COMMISSION
NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

24e rapport d'activité 2003

prévu par l'article 23 de la loi du 6 janvier 1978

ISBN 2-11-005609-6

Sommaire

Avant-propos

Alors que je m'apprête à écrire ces quelques lignes d'avant-propos au rapport d'activité de notre Commission nationale de l'informatique et des libertés pour l'année 2003, je mesure que l'exercice est délicat.

Délicat d'abord puisque depuis quelques semaines j'ai l'honneur de succéder au Président Michel Gentot qui a, durant cinq ans, imprimé sa marque sur nos travaux, faite de hauteur de vue, de finesse dans l'analyse juridique et d'un sens exigeant de l'intérêt général.

Je présente donc ici une édition qui relate des actions entreprises et menées à bien sous son impulsion : c'est pourquoi, cet avant-propos est d'abord, à mes yeux, une manière de lui rendre hommage.

L'exercice est délicat également puisque ce rapport relate les travaux de notre Commission telle qu'elle aura fonctionné depuis l'entrée en vigueur de la loi de 1978 jusqu'à la publication au Journal officiel de la future loi de réforme dans le courant de cette année.

C'est donc, pour moi, l'occasion de rendre aussi un hommage et d'adresser des remerciements à l'ensemble des personnalités qui ont siégé au sein de notre Commission depuis vingt-cinq ans, qui en ont forgé la doctrine et qui lui ont donné sa réputation sur le plan international et je voudrais, bien entendu, ici même, associer l'ensemble du personnel à cet hommage.

L'exercice est délicat, encore, puisque, probablement, jamais depuis la création de notre institution, une année n'aura autant été marquée par des bouleversements technologiques survenus dans le domaine « informatique et libertés » qui exigent que nous soyons capables de réagir « vite et bien ».

On pourra en découvrir quelques exemples à la lecture de ce rapport, certains illustrant des processus parvenus à éclosion, et donc d'application pratique, d'autres qui sont en gestation et recèlent des capacités d'évolution et de transformation fulgurantes.

Je pense, par exemple, à la biométrie qui incontestablement passe de l'âge de l'expérimentation à celui de l'application dans le domaine de la sécurité, au point d'apparaître comme un instrument décisif des politiques de contrôle aux frontières et de lutte contre le terrorisme. Mais à côté de cette dimension régalienne, la CNIL est aussi confrontée à des utilisations plus locales de simples contrôles d'accès.

Je songe aussi à la banalisation de l'internet et de son usage-phare, le courrier électronique, qui s'accompagne d'une explosion des courriels non sollicités – les « spams » – dont on peut se demander s'ils ne constituent pas un poison mortel pour l'espace de libre communication qu'est encore la « toile ».

De même la maturation de technologies telles que celles de la téléphonie mobile ou des puces sans contact génère des questions nouvelles à propos de la liberté d'aller et venir anonymement et des limites de la traçabilité des déplacements.

Au-delà de ces innovations techniques, le développement de l'informatique en réseau conduit à une personnalisation de la relation entre l'administration et l'usager ou entre le commerçant et le client qui est source de services meilleurs mais aussi de risques d'excessive identification des personnes et des comportements.

L'exercice est délicat enfin, car une bonne lecture de ce présent rapport doit se faire ligne après ligne mais aussi entre les lignes.

Comment, en effet, passer sous silence, à l'instant, le grand travail de préparation, de mobilisation de l'ensemble des équipes de la CNIL aux nouvelles responsabilités que lui confiera le législateur dans ces toutes prochaines semaines, entrepris sous la présidence de Michel Gentot et qu'il nous appartient de poursuivre ?

Durant l'année 2003, comme durant l'année en cours, chaque question soumise à notre Commission a fait l'objet d'une double analyse : comment répondre en vertu des principes fondamentaux de la loi de 1978 et de la doctrine élaborée depuis lors ? Mais aussi comment répondrons-nous, dans les mois et années qui viennent, sous l'empire de la directive européenne de 1995 et de la loi qui en assurera la traduction dans notre droit interne ?

Telle sera notre mission inscrite dans la continuité mais sans cesse renouvelée, exigeante, parfois angoissante mais toujours passionnante.

Alex TÜRK

LA CNIL EN CHIFFRES ET EN PRATIQUE

I. LA CNIL AU QUOTIDIEN

Instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) voit sa mission générale résumée dans les premiers mots de son texte fondateur : « *L'informatique doit être au service de chaque citoyen.* [...] *Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Encadrant une technique en pleine expansion, cette loi dite « informatique et libertés » impose à la CNIL un exercice permanent de réflexion quant aux effets de l'utilisation de l'informatique sur la vie privée, les libertés et le fonctionnement des institutions démocratiques. À cet effet, la CNIL a été dotée d'une gamme de pouvoirs qu'elle décline dans la diversité de ses activités.

A. Séances plénières

Pour rendre ses avis, la Commission se réunit régulièrement en formation plénière, autour d'un ordre du jour établi à l'initiative de son président M. Michel Gentot à qui a succédé le 3 février 2004 M. Alex Türk (*cf.* annexe 1 Composition de la CNIL).

À l'occasion de ces séances plénières, la Commission adopte des délibérations qui peuvent être des avis sur des projets de loi ou de décret, des avis sur des traitements ou des fichiers, des suites données à des plaintes ou des demandes de conseil, des textes normatifs, des recommandations (*cf.* annexe 4 Liste des délibérations adoptées en 2003 et deuxième partie de ce rapport Les délibérations 2003 par secteur d'activité).

Au cours des vingt-quatre réunions qui se sont tenues en 2003, la CNIL a adopté soixante-huit délibérations parmi lesquelles il convient de relever :
— une norme simplifiée ;
— un avis défavorable ;
— cinq recommandations ;
— cinq avertissements ;
— neuf dénonciations au parquet ;
— onze avis sur des projets de loi ou de décret.

1) La procédure des normes simplifiées participe du pouvoir réglementaire de la CNIL qui, conformément à l'article 17 de la loi, établit et publie des normes types pour les traitements publics ou privés les plus courants qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés. Cette procédure vise à alléger les formalités préalables à la mise en œuvre de fichiers (*cf. infra* dans ce chapitre, IV). Depuis 1978, la CNIL a édicté quarante-deux normes simplifiées. Celle adoptée en 2003 par la délibération n° 03-067 du 18 décembre concerne la gestion et les négociations des biens immobiliers (*cf.* chapitre 7, III, B).

2) L'avis défavorable émis par la CNIL en 2003 concerne la délibération n° 03-065 du 16 décembre 2003 par laquelle la CNIL n'a pas autorisé la mairie de Levallois-Perret à recourir à la reconnaissance par les empreintes digitales pour contrôler l'accès à un roller-parc (*cf.* chapitre 1, I, D).

3) La mission de conseil à l'égard des responsables de traitements d'informations nominatives définie par le décret d'application du 17 juillet 1978 se traduit en séance plénière par l'adoption de recommandations, qui sans avoir de force contraignante, servent à orienter ou à définir une ligne de conduite dans des secteurs d'activité particuliers.

Depuis 1978, la CNIL a publié une trentaine de recommandations. Celles adoptées en 2003 concernent les domaines suivants :

— La délibération n° 03-012 du 11 mars 2003 est relative à la gestion de fichiers de personnes à risques par les loueurs de véhicules (*cf.* chapitre 7, II, A).

— La délibération n° 03-034 du 19 juin 2003 traite du stockage et de la conservation du numéro de carte bancaire dans le secteur de la vente à distance (*cf.* chapitre 7, I).

— La délibération n° 03-036 du 1er juillet 2003 concerne la sécurité des systèmes de vote électronique (*cf.* chapitre 3, II, A).

— La délibération n° 03-038 du 16 septembre 2003 traite de la collecte et du traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques (*cf.* chapitre 5, I, A).

— La délibération n° 03-053 du 27 novembre 2003 s'attache aux traitements de données à caractère personnel mis en œuvre par les registres du cancer (*cf.* chapitre 8, III, C).

4) Dans le cadre des séances plénières, il arrive également que la CNIL en vertu de l'article 21-3e de la loi du 6 janvier 1978, adresse des avertissements, ou

dénonce des affaires à la justice. Au 31 décembre 2003, ce sont cinquante-quatre avertissements et trente-quatre dénonciations au parquet qui étaient ainsi recensés depuis la création de la CNIL.

Parmi les cinq avertissements prononcés en 2003, quatre d'entre eux ont visé des établissements financiers qui n'ont pas respecté la réglementation relative au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France et à propos duquel la CNIL est très fréquemment saisie de réclamations (*cf. infra* chapitre 7). Le cinquième avertissement a visé une organisation syndicale qui a diffusé sans précautions suffisantes des informations sur internet. Il s'agissait en l'occurrence des propositions de titularisations, promotions ou mutations des surveillants de l'administration pénitentiaire examinées lors des commissions administratives paritaires (délibération n° 03-047 du 23 octobre 2003 portant avertissement à l'Union fédérale autonome pénitentiaire).

5) Les neuf dénonciations au parquet qui sont intervenues en 2003 concernent les affaires suivantes :

— La délibération n° 03-040 du 23 septembre 2003 a dénoncé une opération de collecte illicite et déloyale de données à caractère personnel réalisée à partir d'annuaires sans s'assurer que les personnes auxquelles ces données se rattachaient n'avaient pas exercé leur droit d'opposition (*cf. infra* chapitre 2, I, 2).

— Les délibérations n° 03-057 à n° 03-064 du 9 décembre 2003 ont dénoncé au parquet des infractions au Code des postes et télécommunications commises par plusieurs sociétés qui persistaient à adresser à des personnes physiques des publicités non-sollicitées par voie de télécopie. Or, depuis une loi de juillet 2001, la prospection directe d'un abonné ou utilisateur d'un télécopieur est subordonnée à son consentement préalable. En l'absence, ce type de prospection est interdit en France comme dans l'ensemble des États membres de l'Union européenne et punie d'une amende de 750 euros maximum par message envoyé (*cf. infra* chapitre 2, II, B).

Les séances plénières sont également l'occasion de faire le point sur des sujets de nature à éclairer les membres de la CNIL dans la conduite de leurs missions ; parmi les thèmes évoqués en 2003, on peut relever le *Spam*, l'administration électronique, les développements de l'informatique municipale, l'émergence des puces RFID, les services de géolocalisation sur les routes ou de localisation des enfants via leurs téléphones portables ou encore la question des plates-formes informatiques de confiance.

Compte tenu de la grande variété des dossiers que la CNIL doit traiter, une répartition par secteur d'activité est établie entre les commissaires (*cf.* annexe 2 Répartition par secteur d'activité). Ces attributions ont l'avantage d'instaurer une forme de spécialisation et de faciliter les contacts des commissaires avec les responsables de traitements. Néanmoins, les délibérations de la CNIL sont adoptées selon les principes de la collégialité.

B. Activités hors séances plénières

Pour accomplir leurs missions, les membres de la CNIL s'appuient sur différents services, soit un effectif de quatre-vingt-deux agents (*cf.* annexe 3 Organisation des services et annexe 4 Le budget de la CNIL).

Investie d'une mission générale de réflexion prospective, la CNIL doit se tenir informée des activités industrielles et de services concourant à la mise en œuvre de l'informatique.

À cet effet, la CNIL a créé en son sein divers groupes de travail, notamment sur l'administration électronique, sur le blanchiment d'argent au sein d'établissements de crédit, sur les listes noires. Elle entretient par ailleurs des relations régulières avec de nombreux organismes extérieurs, soit en étant appelée à y siéger officiellement, comme c'est le cas au Conseil consultatif de l'internet, soit par le biais de groupes de travail ou dans le cadre de collaborations sur des sujets précis, par exemple avec l'Agence pour le développement de l'administration électronique (*cf.* annexe 7 Participation de la CNIL à divers organismes extérieurs).

C. Activités européennes et internationales

La coopération européenne et internationale en matière de protection des données personnelles est devenue, sous l'effet conjugué de l'intégration européenne et de la mondialisation des échanges, une réalité quotidienne.

Les autorités européennes de protection des données personnelles constituent, bien évidemment, les principaux correspondants quotidiens de la CNIL à l'étranger. Toutefois, le nombre des autorités de protection des données personnelles hors d'Europe ne cesse de croître, et la CNIL a à cœur de créer des liens avec ces nouveaux homologues.

En 2003, la CNIL a ainsi reçu une quinzaine de délégations étrangères (Lettonie, Japon, Malaisie, Sénégal…) et, à la demande du ministère des Affaires étrangères français, a conduit une mission d'expertise en Croatie afin d'évaluer la situation de cet État sur le plan de la protection des données.

Outre la réception de nombreuses délégations de représentants des pays tiers, une première mission de coopération a été effectuée en Afrique. Dans le cadre de la préparation par le ministre des Droits humains du Burkina Faso du projet de loi sur la protection des données déposée devant le parlement en décembre 2004, le président et un expert de la CNIL ont participé à sa demande en janvier 2003 à des réunions de travail, à une conférence ainsi qu'à de nombreux entretiens à haut niveau dont les médias burkinabés ont rendu compte.

Le réseau constitué par les autorités de protection des données personnelles à travers le monde se renforce progressivement, et démontre chaque jour son utilité face à la mondialisation des échanges et à l'internationalisation des traitements de données personnelles : la coopération dans le traitement de plaintes internationales,

les échanges d'informations relatives aux décisions prises par les autres autorités, la confrontation de doctrines permettent à chaque autorité d'être plus efficaces.

La CNIL a également pris part à de nombreuses conférences, au nombre desquelles, bien sûr, se trouvent les deux conférences des commissaires à la protection des données qui se tiennent annuellement (conférence des commissaires européens à Séville en avril 2003, conférence internationale à Sydney en septembre 2003). À cette dernière occasion, la CNIL a activement contribué à l'élaboration et à l'adoption de cinq résolutions. Ces résolutions concernent les sujets suivants : la radio-identification, les mises à jour automatiques de logiciels, la protection des données et les organisations internationales, les transferts des données des passagers, l'amélioration des pratiques d'information en matière de protection des données et de la vie privée [1].

En outre, comme il est désormais habituel, la CNIL participe deux fois par an au groupe de travail sur les plaintes transfrontalières dont la création a été décidée par la conférence européenne, ainsi qu'au groupe de travail international sur la protection des données dans le secteur des télécommunications.

Toutefois c'est à Bruxelles, au sein des instances européennes instituées dans le domaine de la protection des données, que sont menés les travaux les plus significatifs car les plus normatifs.

1. LE GROUPE DE « L'ARTICLE 29 »

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité nationale. Ce groupe, dit « de l'article 29 », a pour mission de contribuer à l'élaboration des normes européennes par l'adoption de recommandations destinées à l'application homogène de la directive dans l'Union européenne, d'avis sur le niveau de protection dans les pays tiers et de conseils à la Commission sur tout projet de mesure ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles.

Ce groupe, toujours présidé en 2003 par M. Rodota, président de l'autorité italienne de protection des données, a adopté et traité un programme ambitieux.

Indéniablement, le sujet le plus important qui ait été abordé par le groupe a été celui du transfert des données passagers des compagnies aériennes aux autorités américaines [2]. La CNIL a apporté une contribution majeure dans ce dossier, qui a vu une coopération étroite se développer avec l'Allemagne et les autres autorités, notamment italienne et espagnole.

Une autre contribution importante de la CNIL a concerné le développement de la doctrine générale en matière de transferts de données vers les pays tiers, en ce qui concerne notamment l'adoption d'un document sur les règles d'entreprises contraignantes permettant d'encadrer les transferts de données intra-groupes, l'examen

1 Toutes ces résolutions sont en ligne sur le site de la CNIL à l'adresse www.CNIL.fr
2 Ce dossier est traité en détail au chapitre 1, point II — B -1 du présent rapport.

des clauses contractuelles élaborées par *l'International Chamber of Commerce*, mais aussi le lancement d'une discussion qui mènerait à une interprétation commune des dérogations prévues à l'article 26-1 de la directive.

Par ailleurs, le groupe a pu, à partir encore d'une initiative de la CNIL qui a mené ces travaux, adopter une doctrine commune en matière d'administration électronique. Le groupe a également adopté des documents de travail sur la biométrie, sur les plates-formes électroniques et sur la réutilisation des données publiques. Ce dernier document, qui a été adopté en parallèle à l'adoption de la directive sur le sujet, a d'ailleurs été largement inspiré du document adopté deux ans auparavant sur l'initiative de la CNIL dans le cadre du livre vert sur le sujet. Par ailleurs d'autres travaux ont été entamés, notamment sur les données génétiques et les dispositions anti-*spam* de la directive de juillet 2002, qui n'aboutiront à l'adoption de documents de travail qu'au début 2004.

La CNIL siège également au sein de quatre autorités de contrôle communes (ACC) Europol, Schengen, Eurodac et système d'information douanier, dont la mission consiste à garantir la protection des droits des citoyens face aux traitements automatisés à caractère policier et douanier mis en œuvre dans le cadre de chacune des conventions ou règlements applicables.

2. L'AUTORITÉ DE CONTRÔLE COMMUNE EUROPOL

Europol, office européen de police installé à La Haye, a pour mission d'améliorer la prévention et la lutte contre le terrorisme, le trafic illicite de stupéfiants et autres formes graves de criminalité internationale. Cet office gère un système informatisé de données comprenant un système d'informations et des fichiers de travail à des fins d'analyse.

L'autorité de contrôle commune (ACC) Europol a pour tâche de surveiller l'activité d'Europol.

En 2003, l'autorité de contrôle commune (ACC) Europol, présidée par M. Klaus Kalk, membre de la délégation allemande, s'est réunie à cinq reprises en session plénière. Au cours de cette année, l'ACC a opéré un suivi attentif des questions qui avaient particulièrement retenu son attention durant l'année 2002 : l'accord conclu entre Europol et les États-Unis à la suite des événements du 11 septembre 2001 d'une part, le projet danois visant à modifier la convention Europol d'autre part. L'ACC Europol a rendu un nouvel avis sur ce projet, compte tenu des modifications apportées au texte postérieurement à son avis de 2002 (*cf.* avis 02-55 et 03-09).

Par ailleurs, l'ACC, en application de la convention Europol du 26 juillet 1995, a rendu des avis sur trois nouveaux projets d'ordre d'ouverture de fichiers d'analyse créés par l'office européen de police, et sur des projets d'accords entre Europol et plusieurs États et instances tiers (Roumanie, Malte, Lettonie, Lituanie, Eurojust). En outre, conformément à la politique consistant à procéder chaque année à un contrôle des systèmes d'informations de l'office, l'ACC s'est rendu à Europol au mois de février 2003 pour effectuer une inspection, qui a donné lieu à un rapport adopté en réunion plénière au mois de juillet 2003.

Les représentants des autorités nationales de protection des données des pays qui doivent rejoindre l'Union européenne le 1er mai 2004 participant désormais en tant qu'observateurs aux réunions de l'ACC, ceux-ci ont été invités à présenter aux délégations des quinze pays de l'Union leurs compétences et leurs pouvoirs au regard des fichiers de police au niveau national.

Enfin, 2003 aura été l'année de la mise en place de nouveaux moyens devant permettre à l'ACC Europol de mieux se faire connaître par le public : l'ACC a en effet publié son premier rapport d'activité (octobre 1998 — octobre 2002) et son site internet est désormais en ligne (www.europoljsb.ue.eu.int).

Le comité des recours, présidé par M. Giuseppe Busia, membre de la délégation italienne, s'est également réuni cinq fois durant l'année 2003, et a rendu une seconde décision en séance publique le 24 septembre 2003 (*cf.* appel n° 02/01).

3. L'AUTORITÉ DE CONTRÔLE COMMUNE SCHENGEN

Le système d'information Schengen (SIS) centralise au niveau européen, sur le fondement des articles 95 à 100 de la convention d'application du 19 juin 1990, deux grands types de signalements concernant, l'un des personnes recherchées ou placées sous surveillance, l'autre des véhicules ou des objets recherchés.

L'autorité de contrôle commune (ACC) Schengen a pour principales tâches d'exercer le contrôle technique du fichier central (C-SIS) installé à Strasbourg et de vérifier le respect par les États participant au système des droits accordés aux personnes par la convention.

Présidée par M. Giovanni Buttarelli, membre de la délégation italienne, puis par M. Ulco Van de Pol, membre de la délégation néerlandaise, l'ACC s'est réunie cinq fois en 2003. Les représentants des autorités nationales de protection des données des dix nouveaux pays devant intégrer l'Union européenne le 1er mai 2004 ont été invités à participer à ces réunions en tant qu'observateurs.

Les sujets qui ont particulièrement retenu l'attention de l'ACC en 2003 furent, comme en 2002, les projets de modification de la convention d'application de l'accord de Schengen du 19 juin 1990 et du système d'information Schengen (SIS). L'ACC a notamment participé le 7 octobre 2003 à l'audition organisée par la commission des libertés et des droits des citoyens, de la justice et des affaires intérieures du Parlement européen concernant le SIS II. L'une des préoccupations majeures de l'autorité concerne l'introduction dans le futur système de données biométriques, en premier lieu les empreintes digitales et les photographies de personnes signalées dans le SIS. Sur ce sujet, l'ACC estime que des précisions complémentaires doivent être apportées, s'agissant notamment des conditions juridiques permettant d'enregistrer de telles données sensibles. Au-delà de cette question, les débats qui se poursuivront au sein des autorités européennes en 2004 porteront sur les garanties qui doivent accompagner la mise en place d'un système d'information européen qui concerne les données personnelles de plusieurs millions de personnes, consulté pour des motifs divers.

L'ACC s'est en outre prononcée sur la possibilité pour les autorités chargées de procéder à l'immatriculation des véhicules de consulter le SIS, sur les modalités de participation de la Grande-Bretagne et de l'Irlande à Schengen, sur l'accès aux signalements enregistrés dans le SIS par le ministère des Affaires étrangères autrichien, et, à la demande de l'autorité grecque, sur l'interprétation des articles 112 et 113 de la convention (durée de conservation des signalements enregistrés sur le fondement de l'article 96).

Par ailleurs, un contrôle du C-SIS (système central installé à Strasbourg) s'est déroulé au mois de mars 2003, et le rapport définitif d'inspection — faisant notamment état de recommandations à caractère technique — a été adopté par l'ACC au mois de septembre 2003. En outre, l'ACC a décidé de demander aux autorités nationales de protection des données des pays participant au système d'information Schengen de vérifier les modalités d'application de l'article 96 de la convention (« non-admission ») par les autorités gouvernementales concernées, en particulier le respect des dispositions aux termes desquelles les signalements enregistrés dans le SIS résultent d'une décision prise par les autorités administratives ou les juridictions compétentes. La mission de vérification a été entamée par la CNIL auprès du ministère de l'Intérieur français en 2003 et devrait s'achever en 2004.

Enfin, l'ACC Schengen, à l'image de ce qu'a fait l'ACC Europol, s'est attachée à mettre en place de nouveaux supports de communication : un site internet (www.schengen-jsa.dataprotection.org) et une lettre d'information dont la publication devrait être périodique.

4. L'AUTORITÉ DE CONTRÔLE COMMUNE EURODAC

Le système Eurodac, installé à Luxembourg, a pour objet de centraliser les empreintes digitales des demandeurs du statut de réfugié et des ressortissants étrangers appréhendés en situation irrégulière, soit à l'occasion du franchissement d'une frontière extérieure de l'Union européenne, soit sur le territoire d'un des États membres.

L'autorité de contrôle commune (ACC) Eurodac, présidée par M. Alex Türk, membre de la délégation française, s'est réunie le 23 janvier 2004.

Cette réunion a permis aux délégations d'obtenir des données et des statistiques concernant le fonctionnement d'Eurodac, entré en fonction depuis le 15 janvier 2003, et d'échanger des informations portant sur les implications du système pour les États de l'Union européenne au regard de la protection des données.

Compte tenu de la nomination du contrôleur européen de la protection des données — M. Peter Hustinx — en application de l'article 286.2 du traité (*cf.* décision du Parlement européen et du Conseil du 22 décembre 2003), l'ACC a été dissoute à la fin de la réunion, conformément à l'article 20.11 du règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système Eurodac.

5. LE SYSTÈME D'INFORMATION DES DOUANES

Cette base de données centralisée vise à prévenir, rechercher et poursuivre les infractions aux réglementations douanière et agricole, que celles-ci soient fixées au niveau communautaire ou qu'elles restent de la compétence des États comme en matière de trafic illicite de stupéfiants, d'interdictions ou de restrictions d'importation, d'exportation ou de transit de marchandises ou de blanchiment de capitaux. Elle est régie par le règlement communautaire du 13 mars 1997 n° 515/97 et par la convention du 26 juillet 1995 sur l'emploi de l'informatique dans le domaine des douanes. Des informations nominatives ne peuvent y être introduites par un État ou par la Commission européenne que sur des personnes à l'égard desquelles, des indices réels portent à croire qu'elles ont commis, sont en train de commettre ou commettront des infractions dans ces domaines. Le traitement est soumis, dans chaque pays, aux lois nationales de protection des données.

Le SID est opérationnel depuis mars 2003. Cependant, il n'est pas encore utilisé dans plusieurs pays de l'Union européenne, notamment en France. La direction générale des douanes et droits indirects, à laquelle échoit la responsabilité du traitement en France, n'a demandé qu'en mars 2004 à être autorisée par la CNIL à mettre en œuvre le SID. La Commission sera donc appelée à se prononcer sur ce traitement au cours du second trimestre de 2004.

La CNIL n'en participe pas moins à l'autorité de contrôle commune, qui est chargée de surveiller le fonctionnement du système d'information des douanes, en concertation avec les autorités de contrôle nationales et le contrôleur européen à la protection des données. Cette instance, qui réunit des représentants de toutes les autorités de contrôles indépendantes des États signataires de la convention de 1997, a déjà adopté son règlement intérieur, auditionné des représentants de l'Office européen de lutte anti-fraude (OLAF) qui est chargé de la gestion technique de la base de données et programmé plusieurs visites d'information ou d'inspection en 2004. Elle devrait rendre public son premier rapport d'activité fin 2005.

II. LES SAISINES

Les articles 6, 21, 22 et 39 de la loi du 6 janvier 1978 confient à la CNIL la mission d'informer les personnes de leurs droits et obligations, de tenir à leur disposition le registre des traitements déclarés (« fichier des fichiers »), de recevoir les réclamations, pétitions et plaintes, ainsi que d'exercer, à la demande des requérants, le droit d'accès aux fichiers intéressant la sécurité publique et la sûreté de l'État.

À ce titre, la CNIL répond aux demandes de conseils juridiques ou techniques qui lui sont adressées, instruit les plaintes dont elle est saisie, procède aux vérifications nécessaires dans le cadre du droit d'accès indirect et délivre à toute personne qui en fait la demande un extrait de la liste des traitements qui lui sont déclarés.

En 2003, la CNIL a reçu 6 136 saisines qui se répartissent en :
— 3 567 plaintes ;
— 1 163 demandes de droit d'accès indirect (*cf.* chapitre 1er, III) ;
— 1 102 demandes de conseil ;
— 304 demandes d'extraits du « fichier des fichiers ».

Saisines	2000	2001	2002	**2003**	Variation 2002/2003
Demandes de droit d'accès indirect	817	836	1 264	**1 163**	– 7 %
Plaintes	3 543	3 668	5 186	**3 567**	– 31 %
Demandes de conseil	1 049	973	1 126	**1 102**	– 2 %
Demandes d'extrait du fichier des fichiers	208	252	333	**304**	– 8 %
Totaux	**5 617**	**5 729**	**7 909**	**6 136**	**– 22 %**

Après plusieurs années de forte progression des saisines auprès de la CNIL, en particulier des plaintes et des demandes de droit d'accès indirect, les chiffres 2003 révèlent un repli de 22 % du nombre total des saisines.

Il convient cependant de relever que le nombre des plaintes, après avoir connu une véritable explosion en 2002 (+42 %), est en baisse du fait de la nette réduction des plaintes émanant de personnes recevant des télécopies publicitaires non désirées. Cela s'explique par le fait que la CNIL, ayant anticipé sur le nouveau cadre juridique à venir par le décret du 1er août 2003, a écrit à la quasi-totalité des sociétés mises en cause dans ces plaintes afin de leur demander de mettre un terme à leurs pratiques dans la mesure où elles n'avaient pas recueilli l'accord des personnes prospectées (*cf. infra* chapitre 2). Ainsi, sur les 5 186 plaintes répertoriées en 2002, 2 280 concernaient des plaintes motivées par la réception de télécopies publicitaires intempestives, tandis que sur les 3 567 plaintes recensées en 2003, seules 705 relevaient de cette problématique. Au final, hors le secteur de la prospection commerciale par fax, le nombre de plaintes dont la CNIL est saisie se maintient en 2003.

L'objet le plus fréquent des plaintes concerne l'exercice des droits, et tout particulièrement du droit d'opposition à figurer dans un traitement ou à faire l'objet de prospection commerciale. Les secteurs d'activité qui ont suscité en 2003 le nombre le plus important de plaintes sont, par ordre décroissant : prospection commerciale, banque, travail, télécommunications.

Les demandes de conseil portent le plus souvent sur les formalités préalables à la mise en œuvre des fichiers. En 2003, les secteurs d'activité qui ont suscité le nombre le plus important de demandes de conseil sont, par ordre décroissant : travail, santé, collectivités locales, fiscalité.

III. LES CONTRÔLES

En 2003, la Commission a effectué trente et une missions de contrôle [1]. Ce nombre, en constante augmentation depuis 2000, est à rapprocher des 324 missions de contrôle ou de vérifications sur place qui ont été effectuées par la Commission depuis son installation.

Si la Commission a jusqu'à présent peu fait usage de cette modalité particulière de contrôle, cette progression constitue, après la création en 2001 du service des contrôles, une des premières traductions du souhait de la Commission d'anticiper la prochaine loi « informatique et libertés » dont l'un des traits les plus marquants consiste à alléger le contrôle *a priori* (les formalités préalables) et à accentuer le contrôle *a posteriori* (les missions de vérification sur place) : le projet de loi transposant la directive européenne 95/46, tel qu'il résulte de son adoption en première lecture par le Sénat le 1er avril 2003, reconnaît à la Commission de nouveaux pouvoirs de sanctions en cas de non-respect de la loi, en particulier un pouvoir de sanction pécuniaire, d'injonction de cesser le traitement ou de retrait de l'autorisation accordée selon que ce dernier est soumis au régime de déclaration ou d'autorisation.

Au-delà de ces aspects purement quantitatifs, plusieurs innovations amorcées en 2003 — tenant tant à l'objet qu'au déroulement des missions de contrôle — méritent d'être soulignées.

En premier lieu, la CNIL a décidé de procéder plus fréquemment à des missions de contrôle sans information préalable de l'organisme concerné. Cette intervention « inopinée » de la Commission s'avère particulièrement utile lorsque le responsable du traitement peut facilement remédier au manquement à la loi porté à la connaissance de la CNIL, sans porter atteinte de manière importante au bon fonctionnement général de l'application mise en œuvre (ex. : effacement d'informations faisant apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes par exemple).

En second lieu, s'inscrivant dans le cadre de la définition prochaine d'une nouvelle politique de contrôles, des séries de missions de contrôle ont été effectuées afin de mieux connaître les évolutions et les conséquences de l'informatisation de secteurs d'activités spécifiques, alors que la pratique la plus courante consistait jusqu'alors à décider de manière ponctuelle, au coup par coup, d'une mission de contrôle. Il s'agit de :

Missions de contrôles auprès de communes

La Commission a dressé un premier état des lieux de l'informatisation des mairies à partir d'un échantillon de dix communes de plus de 15 000 habitants (Aix-en-Provence, Carpentras, Clichy-sous-Bois, Goussainville, Hautmont, La Rochelle,

1 Ce chiffre ne tient pas compte des visites d'information organisées notamment dans le cadre de l'instruction de dossiers de formalités préalables ou de demandes de conseil.

Le Mans, Tarascon, Vaulx-en-Velin et Villeparisis), afin d'évaluer les modalités d'application de la loi du 6 janvier 1978 et de mesurer les difficultés rencontrées par les responsables locaux. Ces missions ont donné lieu à un rapport d'étape adopté en séance plénière le 9 décembre 2003 et ont permis de modifier sur certains points le guide *Collectivités locales* diffusé par la CNIL.

Missions de contrôle auprès d'organismes procédant au recouvrement de créances pour le compte de tiers

Huit missions de contrôle se sont déroulées auprès de sociétés de recouvrement de créances. Ces missions ont été décidées dans le cadre de l'élaboration du rapport « listes noires » [1]. Elles ont permis d'établir un certain nombre de constats, qui ont conduit la Commission à rappeler aux organismes concernés les principes de la loi du 6 janvier 1978.

Missions de contrôle auprès de registres du cancer

La Commission a procédé à deux missions de contrôle auprès du registre des tumeurs digestives du Calvados à Caen et du registre général du cancer de l'Isère à Grenoble. Ces missions, suivies de l'envoi à l'ensemble des responsables des registres du cancer d'un questionnaire sur la sécurité et l'information des personnes, ont débouché sur l'adoption, le 27 novembre 2003, d'une nouvelle recommandation relative aux traitements de données à caractère personnel mis en œuvre par les registres du cancer [2].

Missions de contrôle auprès d'entités publiques et privées pour évaluer l'application des recommandations de la CNIL en matière de « cybersurveillance »

Les missions de contrôle opérées auprès de quatre organismes ont permis d'adapter au vu des constats effectués le rapport « cybersurveillance » adopté le 5 février 2002.

Au nombre des contrôles opérés par la CNIL en 2003, on retiendra également les missions ayant pour fondement des plaintes adressées à la Commission aux termes desquelles des données relevant de l'article 31 de la loi, en particulier des informations relatives aux origines raciales, étaient collectées et enregistrées à l'insu des personnes par des organismes publics et privés exerçant leur activité dans le secteur immobilier. Dans un cas, les constats opérés ont abouti à la suppression des documents établis à partir desdites informations ; dans trois autres cas, la Commission a rappelé aux organismes concernés les principes de la loi « informatique et libertés », notamment les obligations déclaratives qui en découlent.

D'autres missions de contrôle avaient pour objet de vérifier la nature des informations et justificatifs exigés lors de la location d'un bien immobilier ou

1 *Cf. infra.*

2 Une première recommandation avait été adoptée par la CNIL sur ce sujet le 19 février 1985.

l'existence d'une « liste noire » de clients jugés indésirables par un établissement sportif. Dans ces cas, les constats opérés ont permis à la CNIL de rappeler aux responsables des traitements informatiques ou fichiers le cadre légal à respecter.

IV. LES FORMALITÉS PRÉALABLES À LA MISE EN ŒUVRE DES FICHIERS

Pour la période du 1er janvier au 31 décembre 2003, la CNIL a enregistré 65 921 nouveaux traitements de données nominatives et 3 431 déclarations de modification de traitements déjà enregistrés : ce sont ainsi 69 352 dossiers de formalités préalables qui ont été traités durant cette période.

Ces chiffres reflètent une augmentation de 21 % du nombre de formalités préalables à la mise en œuvre de fichiers réalisées auprès de la CNIL pour l'année 2003.

Formalités préalables	2000	2001	2002	**2003**	Variation 2002/2003
Déclarations simplifiées	33 657	29 755	33 261	**42 015**	+ 26 %
Demandes d'avis	3 149	3 351	3 733	**5 520**	+ 47 %
Déclarations ordinaires	9 563	9 247	9 320	**9 588**	+ 2 %
Déclarations de sites internet	6 114	7 389	7 366	**8 232**	+ 11 %
Demandes d'autorisation chapitre V*bis*	287	288	384	**507**	+ 32 %
Demandes d'autorisation chapitre V*ter*	73	59	64	**59**	– 7 %
Déclarations de modification	2 607	3 061	2 915	**3 431**	+ 17 %
Totaux	55 450	53 150	57 043	**69 352**	**+ 21 %**

Au 31 décembre 2003, la CNIL avait enregistré 941 076 traitements automatisés de données nominatives depuis 1978.

V. L'INFORMATION DU PUBLIC

Conformément à ses missions, la CNIL consacre une partie de son activité à des actions d'information des personnes sur leurs droits et sur leurs obligations.

A. Le site internet

Créé en 1997, le site www.CNIL.fr est devenu au fil des années un instrument privilégié de la politique de diffusion des informations de la CNIL. Reconnu pour son originalité et son caractère pédagogique, notamment du fait de sa rubrique phare « Vos traces » qui démontre les formes de « pistage » sur internet, le site de la CNIL a fait peau neuve au début de l'année 2004 afin de valoriser sa richesse éditoriale et de répondre à une audience toujours en hausse.

La CNIL recense en moyenne 50 000 pages visionnées par jour, pour 2000 à 3 000 visites quotidiennes.

Le nouveau site de la CNIL, en ligne depuis le 10 mars 2004, a pour objectif principal de rendre la CNIL plus accessible en apportant une information claire et précise au grand public et en permettant aux usagers d'accomplir plus facilement leurs démarches auprès de l'institution.

Outil de référence en matière de protection des données personnelles, le site de la CNIL offre une place de choix à l'actualité de l'institution, elle-même relayée par une lettre mensuelle d'information, baptisée *Lettre InfoCNIL* lancée en septembre 2003 et qui compte près de 5 000 abonnés. Une tribune, un agenda et des informations régulières sur les séances plénières permettent de faire connaître, au fur et à mesure, l'activité de la CNIL.

Pour donner plus d'écho à certaines de ses décisions ou de ses actions, la CNIL publie des communiqués de presse. Les sujets abordés dans ce cadre en 2003 ont concerné par exemple le dispositif de surveillance épidémiologique du sida, l'utilisation des données personnelles par les banques, l'annuaire universel ou encore les fichiers des abonnés aux télévisions payantes.

Le nouveau site web de la CNIL est organisé autour de cinq grandes rubriques auxquelles s'ajoute un espace à l'attention des juniors.

B. Les publications

Au-delà de la parution annuelle de son rapport d'activité, la CNIL a renforcé sa politique éditoriale autour de deux collections : les guides pratiques et les rapports thématiques.

Au titre de la collection « Guides », la CNIL a publié en 2003 un nouveau fascicule : le guide *Protection des données et refus de crédit*. Élaboré par le service des plaintes et des requêtes générales de la CNIL, ce guide pratique a été conçu pour répondre aux questions que peuvent se poser les personnes à qui a été opposé par un établissement de crédit ou une banque un refus de crédit. Ce guide s'ajoute au guide *Santé*.

Dans la collection « Rapports », la CNIL a publié deux volumes :

— Le rapport *Listes noires*, qui traite du fichage des « mauvais payeurs » et des « fraudeurs » au regard de la protection des données personnelles.

— Le rapport *La cybersurveillance sur les lieux de travail*, qui s'attache aux technologies de l'information et de la communication sur les lieux de travail et à l'équilibre à trouver entre les intérêts des employeurs et le nécessaire respect des droits et libertés des employés, et en particulier de leur vie privée (La Documentation française, mars 2004).

Ces guides et rapports sont disponibles en téléchargement sur le site de la CNIL dans la bibliothèque de ses publications.

C. Les colloques et salons

Directement sollicitée par de nombreux organismes, sociétés ou institutions pour conduire des actions de formation et de sensibilisation à la loi « informatique et libertés » (323 demandes au titre de l'année 2003), la CNIL participe également à des colloques, des salons ou des conférences.

À titre d'exemple, la CNIL a pris part en 2003 à deux salons, le salon des collectivités locales et le Medec. Au final, c'est à près de 220 manifestations, réunions ou colloques auxquels la Commission a collaboré au cours de cette même année, pour l'essentiel en tant qu'intervenant.

Première partie

AU CŒUR DE L'ACTIVITÉ 2003

Chapitre 1

L'IMPÉRATIF DE SÉCURITÉ ET SES CONTREPARTIES

En 2003, les questions de sécurité intérieure ont encore longuement retenu l'attention de la CNIL. Dans la politique de lutte contre la délinquance menée par le gouvernement français, l'utilisation des fichiers demeure un axe important, comme en témoignent par exemple la création d'un fichier des délinquants sexuels ou l'extension du fichier national des empreintes génétiques dont la CNIL a eu à nouveau à connaître dans sa version réglementaire.

Plus généralement, le recours à la biométrie caractérise l'évolution des instruments de la sécurité publique, en particulier pour les contrôles de l'immigration. Toutefois, si les autorités américaines partagent cette approche puisqu'elles s'apprêtent à imposer au reste du monde l'insertion de données biométriques dans les passeports, elles y ajoutent une exigence à laquelle *de facto* sinon *de jure* les Européens ont dû déjà se soumettre : le transfert des données des passagers des compagnies aériennes. À l'unisson de ses homologues européens, la CNIL a jugé illégal ce transfert pour lequel la recherche d'un cadre juridique est en cours.

I. LA PROPAGATION DE LA BIOMÉTRIE

Dans son rapport *Méthodes scientifiques d'identification des personnes à partir des données biométriques et techniques de mise en œuvre* [1], Christian Cabal, député, souligne que les techniques de biométrie se diversifient, s'automatisent et s'élargissent à de nouveaux domaines d'application, au-delà des applications militaires et

1 Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, n° 938 Assemblée nationale, n° 355 Sénat, juin 2003.

policières. Il n'en reste pas moins que, aux dires mêmes du rapporteur, *« l'utilisation de la biométrie apparaît comme un élément utile voire indispensable aux autorités publiques de l'État ou des États, dans la nécessité qui est la leur, conformément aux lois qui régissent nos sociétés, de savoir si tel individu est bien celui qu'il prétend être et s'il est habilité à entreprendre un certain nombre d'actions correspondant à notre vie sociale en général »* (*cf.* p. 153).

Utile ou indispensable ? Il y a une nuance que la CNIL est amenée à examiner quand elle est saisie de projets (macroscopiques ou microscopiques) relatifs à l'utilisation de la biométrie à des fins de sécurité.

On peut rappeler que les techniques biométriques concernent l'ADN, l'empreinte digitale, le visage, la rétine, l'iris, le contour de la main, la voix ou d'autres procédés moins usuels comme l'écriture manuscrite, les odeurs, etc. Le champ d'application de ces techniques s'étend sans cesse grâce aux progrès réalisés dans la qualité et la miniaturisation des appareils de capture, ainsi que dans l'augmentation de puissance des microprocesseurs.

A. Le relevé d'empreintes digitales des étrangers

Dans le cadre du renforcement de la politique de contrôle de l'entrée des étrangers en France, la loi du 24 novembre 2003 relative à l'immigration a réformé de façon substantielle les procédures de vérification des identités lors de la délivrance des visas et lors du contrôle aux frontières, en généralisant le recours aux techniques biométriques.

La loi du 24 avril 1997 avait déjà prévu la possibilité de relever, de conserver et de traiter sous forme informatique les empreintes digitales des demandeurs de titres de séjour ainsi que celles des étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement du territoire [1]. Ces dispositions, introduites dans l'ordonnance du 2 novembre 1945 (article 8-3), n'ont reçu aucune application à ce jour.

L'article 8-3 autorise également les agents expressément habilités du ministère de l'Intérieur ou de la gendarmerie à consulter, « dans les conditions fixées par la loi du 6 janvier 1978 », le fichier automatisé des empreintes digitales (FAED), géré par le ministère de l'Intérieur, afin d'identifier les étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement qui n'auraient pas présenté les pièces justificatives nécessaires. Cette consultation n'a pas non plus, semble-t-il, été mise en œuvre.

Les nouvelles dispositions introduites en 2003 étendent la possibilité de prise d'empreintes digitales et de leur traitement aux étrangers qui ayant été contrôlés à l'occasion du franchissement de la frontière, ne sont pas munis des documents et

1 Le Conseil constitutionnel, saisi d'un recours notamment contre ces dispositions, n'a pas considéré que la prise d'empreintes digitales des étrangers, non ressortissants des États membres de l'Union européenne, qui sollicitent la délivrance d'un titre de séjour, sont en situation irrégulière ou font l'objet d'une mesure d'éloignement, constituait une *« atteinte excessive à la liberté individuelle de nature à méconnaître la Constitution »* (décision du 22 avril 1997).

visas d'entrée nécessaires ou ne remplissent pas les conditions d'entrée sur le territoire prévues à l'article 5 de la convention de Schengen du 19 juin 1990.

La loi de 2003 a également inséré un nouvel article 8-4 dans l'ordonnance du 2 novembre 1945 aux termes duquel les empreintes digitales et les photographies des étrangers non ressortissants de l'Union européenne qui sollicitent la délivrance, auprès d'un consulat ou à la frontière, d'un visa afin de séjourner dans un État membre de l'Union européenne, pourront être relevées, mémorisées et faire l'objet d'un traitement automatisé dans les conditions fixées par la loi du 6 janvier 1978.

Il s'agit de limiter les récidives dans les tentatives d'entrer sur le territoire avec des documents frauduleux et sous différentes identités et de faire des rapprochements *a posteriori* pour identifier une personne à laquelle un visa aurait été délivré et qui se maintiendrait en France illégalement sous une autre identité ou en masquant son origine.

La prise d'empreintes s'intègre par ailleurs dans le cadre des travaux en cours sur le plan communautaire visant à systématiser l'introduction de données biométriques dans les passeports, les visas et les titres de séjour. Le Conseil européen de Laeken, en décembre 2001, a également demandé au Conseil des ministres et aux États membres de prendre les dispositions nécessaires pour la mise en place d'un système commun d'information sur les visas, qui permettrait de recenser dans une base unique les demandes et les refus de visas, afin notamment de lutter contre la fraude, d'améliorer la coopération consulaire, de déterminer plus aisément, aux postes de contrôle aux frontières extérieures ou lors des contrôles d'immigration ou de police, les usurpations d'identité, de faciliter l'application de la convention de Dublin sur le droit d'asile et de vérifier l'identité des personnes en situation irrégulière. À cet effet, certaines lignes directrices ont déjà été définies, parmi lesquelles l'intégration dans la base des photographies numérisées et d'autres données biométriques.

Consultée sur les articles 8-3 et 8-4 du projet de loi par le ministère de l'Intérieur, la CNIL a, dans son avis du 24 avril 2003, posé en particulier le principe que la mémorisation et le traitement de données issues des empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données qui pourraient ainsi être constituées, n'étaient admissibles que dans la mesure où ils seraient justifiés par des exigences impérieuses en matière de sécurité ou d'ordre public. Rappelant ainsi sa doctrine sur l'utilisation des techniques biométriques [1], la Commission a souligné à nouveau qu'elle estimait en revanche légitime le recours, pour s'assurer de l'identité d'une personne, à des dispositifs de reconnaissance de données biométriques dès lors que celles-ci sont conservées sur un support (ex. : cartes à puce) en possession de la personne ou sur un appareil (ex. : téléphone portable, ordinateur…) dont elle a l'usage exclusif.

La Commission a également considéré que la loi devait clairement indiquer les finalités pour lesquelles il pourrait être procédé à des traitements automatisés d'empreintes digitales des étrangers. La loi du 26 novembre 2003 précise ainsi qu'il

1 *Cf.* rapport annuel d'activité 2001 p. 101 et ss.

sera possible de procéder au relevé, à la mémorisation et au traitement des empreintes digitales ainsi que de la photographie des demandeurs de visas *« afin de mieux garantir le droit au séjour des personnes en situation régulière et de lutter contre l'entrée et le séjour irréguliers des étrangers en France »*, et ce dans les conditions fixées par la loi du 6 janvier 1978.

La Commission a aussi estimé que, compte tenu de l'ampleur des bases de données qui pourraient ainsi être constituées, des garanties appropriées devraient être prises pour assurer le respect des droits et libertés individuelles, s'agissant en particulier de l'accès à de telles bases, de la durée de conservation et de la mise à jour des données.

Ainsi l'accès aux traitements d'empreintes digitales, eu égard à la sensibilité des données qui y seraient conservées, devrait être strictement réservé à un nombre limité de personnes expressément habilitées à cet effet et des mesures particulières de sécurité devraient être adoptées pour éviter toute utilisation détournée des informations, compte tenu non seulement de la dimension des fichiers mais aussi de la répartition mondiale des postes consulaires.

Se référant d'autre part aux différents avis rendus en particulier sur le traitement de gestion, par le ministère de l'Intérieur, des dossiers des ressortissants étrangers (AGDREF) [1] et sur le traitement de délivrance des visas (RMV2) [2] mis en œuvre par le ministère des Affaires étrangères, la Commission a rappelé que, compte tenu des conséquences graves que pourrait entraîner à l'égard des personnes concernées la conservation dans les traitements d'empreintes digitales, d'informations incomplètes ou périmées, s'agissant par exemple de personnes ayant acquis la nationalité française ou ayant régularisé leur situation en France, les durées de conservation des informations et les procédures de mise à jour et d'apurement de celles-ci devraient être précisément définies et rigoureusement appliquées.

La Commission a en conséquence recommandé que la loi renvoie explicitement à un décret en Conseil d'État, pris après avis de la CNIL, les modalités d'application de chacun des deux articles, afin de préciser notamment les modalités d'habilitation des personnes pouvant accéder aux informations, la durée de conservation et les conditions de mise à jour des informations enregistrées et l'exercice de leur droit d'accès par les personnes concernées. Cette recommandation a été suivie par le législateur. La CNIL n'a pas encore été saisie à ce jour du projet de décret.

1 L'application AGDREF, créée par un décret du 29 mars 1993 pris après avis favorable de la CNIL (délibération du 7 mai 1991), a notamment pour finalités d'améliorer les procédures relatives au règlement de la situation administrative des ressortissants étrangers et d'assurer la fabrication des titres de séjour et des récépissés de demande de délivrance ou de renouvellement des titres, des autorisations provisoires de séjour accordées aux demandeurs d'asile. L'application ne comporte pas a priori aujourd'hui de données biométriques. Il convient toutefois de noter que les titres de séjour doivent comporter la photographie du titulaire. Lors de l'avis rendu en 1991 sur ce traitement la CNIL avait demandé que le fichier fasse l'objet de mises à jour et d'apurements réguliers. Or, tel ne semble pas être le cas.

2 L'application RMV2, créée par un arrêté du 22 août 2001, pris après avis favorable de la CNIL (délibération du 15 mai 2001), a pour objet de faciliter l'instruction des demandes de délivrance de visas par les consulats et les sections consulaires des ambassades, en procédant notamment aux échanges d'informations nécessaires avec le ministère de l'Intérieur et les autorités centrales des États Schengen. Les informations enregistrées dans les différents fichiers composant cette application ne comportent aucune donnée biométrique.

Compte tenu des initiatives en cours sur le sujet au plan européen, la Commission examinera avec une particulière attention les modalités de mise en œuvre de ces nouvelles dispositions et notamment, leur articulation avec les systèmes d'information européens déjà en vigueur, tel EURODAC, ou en cours tel le système d'information sur les visas VIS.

B. Le nouveau cadre du fichier national des empreintes génétiques

L'article 29 de la loi du 18 mars 2003 pour la sécurité intérieure a modifié les articles 706-54 à 706-56 du Code de procédure pénale relatifs au fichier national automatisé des empreintes génétiques (FNAEG) afin d'étendre son champ d'application tant du point de vue des personnes dont l'empreinte génétique peut être enregistrée que de celui des infractions pouvant justifier un prélèvement.

Au mois d'août 2003, le ministère de la Justice a transmis pour avis à la Commission le texte du projet de décret d'application de l'article 706-54 du Code procédure pénale dans sa nouvelle rédaction. Ce texte a pour objet de préciser les nouvelles conditions d'alimentation et de consultation du FNAEG ainsi que la durée de conservation des informations nominatives appelées à y être enregistrées.

Après avoir relevé que l'extension très importante du champ d'application du fichier nécessitait des garanties sérieuses pour prévenir tout enregistrement abusif de données personnelles et tout détournement de finalité, la Commission a, par une délibération n° 03-043 du 7 octobre 2003, rendu un avis favorable assorti d'un certain nombre d'observations et de demandes sur le texte qui lui était présenté.

1. L'ÉVOLUTION DU FNAEG

Créé par l'article 28 de la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, le FNAEG était, à l'origine, conçu pour faciliter l'identification et la recherche des auteurs des infractions sexuelles limitativement énumérées à l'article 706-47 du Code de procédure pénale. En conséquence, il centralisait uniquement les empreintes génétiques des personnes condamnées pour de telles infractions, ainsi que celles effectuées à partir de prélèvements effectués sur les lieux d'une infraction et correspondant à des personnes non identifiées.

L'article 706-54 du Code de procédure pénale prévoyait en outre la possibilité de comparer, à la demande d'un magistrat, les empreintes génétiques des personnes à l'encontre desquelles il existerait des indices graves et concordants de nature à motiver leur mise en examen pour l'une des infractions visées à l'article 706-47 du Code de procédure pénale avec celles figurant déjà au fichier, sans toutefois qu'elles puissent y être conservées.

L'article 56 de la loi du 15 novembre 2001 relative à la sécurité quotidienne a étendu à des crimes et délits n'ayant pas une nature sexuelle la liste des infractions pouvant donner lieu à enregistrement dans le FNAEG des traces ou des empreintes génétiques de leurs auteurs définitivement condamnés.

À l'occasion de cette réforme, le législateur a érigé en infraction pénale le fait, pour une personne définitivement condamnée pour l'une des infractions visées, de refuser de se soumettre à un prélèvement et a harmonisé la définition des personnes dont l'empreinte génétique peut faire l'objet d'un rapprochement avec les données déjà inscrites au FNAEG avec les dispositions de l'article 80-1 du Code de procédure pénale sur la mise en examen telles qu'elles résultaient des modifications apportées à ce texte par la loi du 15 juin 2000 renforçant la présomption d'innocence et les droits des victimes.

L'article 29 de la loi du 18 mars 2003 pour la sécurité intérieure, qui vient modifier pour la seconde fois les dispositions du Code de procédure pénale relative au FNAEG, a principalement élargi, d'une part, la liste des personnes dont l'empreinte génétique est susceptible de faire l'objet d'un enregistrement dans ce fichier et, d'autre part, celle des infractions pouvant donner lieu à enregistrement dans le fichier de traces ou de prélèvements biologiques des personnes concernées [1].

Cette modification a également pour effet, ainsi que la Commission l'avait demandé au ministère de la Justice dès la création du FNAEG, d'inscrire dans la loi la garantie selon laquelle les empreintes génétiques ne seront réalisées que sur la partie non codante de l'ADN. La Commission a toutefois estimé utile de faire également figurer cette précision dans le projet de décret d'application de ces dispositions, ce qui n'a soulevé aucune objection.

2. LES GARANTIES DEMANDÉES PAR LA CNIL

a) Sur l'extension du champ d'application du fichier

La loi du 18 mars 2003 et le projet de décret d'application prévu par son article 29 élargissent sensiblement la liste des personnes dont les empreintes génétiques pourront faire l'objet d'un enregistrement dans le FNAEG.

Il sera ainsi possible d'inscrire au FNAEG l'empreinte génétique de personnes non identifiées, à savoir les personnes disparues pour lesquelles des échantillons biologiques ont été recueillis dans le cadre d'une enquête pour recherche des causes d'une disparition inquiétante et celle résultant des traces biologiques de personnes inconnues, recueillies dans le cadre d'une enquête de flagrance, préliminaire ou d'une instruction concernant l'une des infractions visées par l'article 706-55 du Code de procédure pénale, ainsi que les échantillons biologiques prélevés sur des cadavres non identifiés et les traces biologiques issues de personnes inconnues dans le cadre d'une enquête sur les causes de la mort ou sur une disparition inquiétante et suspecte.

1 En plus de certaines infractions de nature sexuelle, pourront désormais donner lieu à prélèvement d'échantillon ou de traces biologiques les crimes contre l'humanité et les crimes et délits d'atteintes volontaires à la vie de la personne et à l'intégrité des personnes, de trafic de stupéfiants, d'atteintes aux libertés de la personne, de traite des êtres humains, de proxénétisme, d'exploitation de la mendicité et de mise en péril des mineurs ; certains crimes et délits contre les biens ; les atteintes aux intérêts fondamentaux de la nation, les actes de terrorisme, la fausse monnaie et l'association de malfaiteurs ; les crimes et délits en matière de législation sur les armes, ainsi que les infractions de recel ou de blanchiment du produit de l'une de ces infractions.

Les données concernant deux nouvelles catégories de personnes peuvent être enregistrées :
— celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale. Le prélèvement, dans cette hypothèse, ne peut intervenir que dans le cadre d'une enquête préliminaire ou de flagrance ou d'une instruction et sur décision de l'officier de police judiciaire agissant soit d'office, soit sur demande du procureur de la République ou du juge d'instruction compétent ;
— les ascendants ou descendants d'une personne disparue, dans le cadre d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte. Dans ce cas, le prélèvement ne peut se faire qu'avec l'accord des personnes concernées.

Cette dernière catégorie de personnes, n'étant pas expressément prévue par l'article 706-54 du Code de procédure pénale dans sa nouvelle rédaction, la Commission a estimé que l'inscription dans le FNAEG de l'empreinte génétique des ascendants ou descendants d'une personne disparue faisait naître le risque d'une confusion entre deux finalités différentes : la recherche des personnes disparues et la recherche des auteurs d'infractions.

Elle a donc considéré, tout en prenant acte de la proposition du ministère de la Justice de renforcer l'information des personnes concernées sur ce point par l'ajout d'une mention expresse au procès-verbal, que le FNAEG devrait être structuré de telle façon que les informations concernant cette catégorie particulière de personnes soient gérées de façon distincte lorsqu'elles ont limité l'utilisation de leur empreinte génétique aux seules fins de recherche de la personne disparue concernée.

b) Sur la nature des informations nominatives traitées

Le projet de décret prévoyait que les empreintes génétiques résultant de l'analyse de prélèvements ou de traces biologiques sont accompagnées, dans tous les cas, du numéro de procédure, des informations relatives à l'autorité judiciaire ou à l'officier de police judiciaire ayant demandé l'enregistrement au fichier, de la date de la demande d'enregistrement dans le fichier ou de la date de condamnation, du nom de la personne ayant réalisé le prélèvement, ainsi que de la nature de l'affaire justifiant le prélèvement.

Cette information ne pourra, s'agissant des personnes définitivement condamnées ou de celles mises en cause dans une affaire relative à une des infractions visées à l'article 706-55 du Code de procédure pénale, être exploitée qu'en vue d'un traitement à des fins statistiques.

Toutefois, le FNAEG étant un fichier d'identification et non un fichier d'antécédents judiciaires, la Commission a sur ce point demandé au ministère de la Justice que le décret précise expressément que l'information relative à la nature de l'affaire n'apparaît pas en cas de consultation du fichier, et ne peut servir de critère de recherche nominative.

c) Sur la durée de conservation des informations

Le projet de décret soumis initialement à la Commission prévoyait que les informations enregistrées dans le FNAEG seraient conservées pour une durée maximale de quarante années (fixée antérieurement au quatre-vingtième anniversaire de l'individu concerné), que les traces concernent les personnes définitivement condamnées ou celles seulement mises en cause.

Il était également prévu que les empreintes génétiques prélevées ou utilisées aux fins d'identification de cadavres non identifiés ou de recherche de personnes disparues soient effacées après identification définitive de la personne décédée ou dès réception d'un avis de découverte dans le dernier cas.

Interrogée sur le caractère uniforme de cette durée maximale de conservation des informations, au regard notamment de la présence dans le fichier d'empreintes génétiques de personnes seulement mises en cause, voire d'ascendants ou de descendants de personnes disparues, le ministère de la Justice a indiqué que, par cohérence avec ce que prévoit notamment le décret du 8 avril 1987 relatif au fichier automatisé des empreintes digitales, pris après avis de la CNIL (*cf. 7*e rapport d'activité de la Commission, p. 108 et ss.), il était envisagé de réduire ce délai de conservation à vingt-cinq années, à l'exception toutefois des informations relatives aux auteurs d'infractions de nature sexuelle ayant bénéficié d'une décision de classement sans suite, de non-lieu, de relaxe ou d'acquittement exclusivement fondée, en application de l'article 122-1, premier alinéa, du Code pénal, sur l'existence d'un trouble mental.

La Commission, tout en soulignant que cette proposition pouvait poser la question de l'application en l'espèce du principe traditionnel du droit pénal selon lequel l'intention criminelle est un élément constitutif de l'infraction, a pris acte de la proposition du ministère de la Justice.

Elle a toutefois demandé, prenant une nouvelle fois en compte le fait, que le FNAEG est un fichier d'identification et non un fichier d'antécédents, que la durée maximale de conservation des informations puisse, à l'instar des modalités de fonctionnement d'autres fichiers de police judiciaire, tels le STIC et JUDEX, être modulée en fonction de la gravité et de la nature de l'infraction concernée, s'agissant tant des personnes condamnées que de celles uniquement mises en cause.

d) Sur la procédure d'effacement

Le projet de décret fixait les nouvelles modalités pratiques de la procédure d'effacement des informations inscrites au FNAEG, dont le principe a été posé par la loi du 18 mars 2003.

Cette disposition prévoit notamment que l'intéressé disposera désormais, en cas de refus d'effacement des informations le concernant émanant du procureur de la République compétent, d'une possibilité de recours devant le juge des libertés et de la détention, puis devant le président de la chambre de l'instruction en cas de nouveau refus.

Toutefois, le projet de décret ne donnant aucune précision supplémentaire pouvant faciliter l'application des dispositions du Code de procédure pénale, telles qu'elles résultent de la loi du 18 mars 2003, la Commission a demandé que la circulaire d'application du décret lui soit soumise.

Bien plus, elle a demandé que les informations figurant au FNAEG soient effacées de façon automatique dans le cas spécifique où une personne, mise en cause dans une procédure relative à une des infractions visées à l'article 706-55 du Code de procédure pénale, viendrait à être mise totalement hors de cause, notamment dans l'hypothèse où le véritable auteur des faits concernés serait identifié au cours de la procédure.

e) Sur les destinataires

La loi du 18 mars 2003 a déterminé de façon limitative les catégories de personnes habilitées à recevoir communication d'informations issues du FNAEG, à savoir les magistrats concernés par la procédure et les officiers de police judiciaire lorsqu'ils font procéder au rapprochement de l'empreinte génétique d'une personne mise en cause dans une procédure relative à une des infractions visées à l'article 706-55 du Code de procédure pénale ou lorsqu'ils souhaitent, préalablement à un prélèvement biologique, vérifier au vu de son seul état civil que l'empreinte génétique de la personne n'est pas déjà enregistrée dans le fichier.

Chaque utilisateur disposera d'un code d'accès personnel et les consultations du FNAEG continueront de faire l'objet d'un suivi informatique.

Le projet de décret fixait la liste des destinataires pouvant accéder directement au fichier, qui sont d'une part les personnels de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire de la police nationale et ceux de la gendarmerie nationale, spécialement affectés dans le service mettant en œuvre le traitement et dûment habilités et, d'autre part, les personnels dûment habilités qui sont affectés au service central de préservation des prélèvements biologiques.

Dans la mesure où la possibilité d'accéder au fichier, pour les officiers de police judiciaire agissant au titre de l'article 706-56 I du Code de procédure pénale, est déjà prévue par la loi, la Commission a estimé, dans un souci de clarté, que cette catégorie de destinataires devait également figurer dans le décret d'application, cet ajout permettant ainsi de préciser la nature des informations accessibles.

La Commission a, à cet égard, demandé au ministère de la Justice que lui soient indiquées les modalités techniques d'interrogation du fichier.

Elle a également demandé que cette disposition soit complétée à cette occasion par le rappel que ces personnels ne peuvent accéder au FNAEG que dans le cadre et les limites des procédures qu'ils diligentent.

À la date de rédaction de ce rapport, le décret d'application n'avait pas encore été publié.

C. La reconnaissance du contour de la main dans les prisons

À la suite de plusieurs évasions par substitution de personnes ayant eu lieu l'été 2002 à l'occasion de visites à des détenus, le ministère de la Justice a souhaité mettre en place, dans l'ensemble des établissements pénitentiaires, un dispositif destiné à vérifier l'identité des détenus par reconnaissance biométrique de la morphologie de la main, notamment lors de l'accès au parloir et lors des déplacements à l'intérieur des bâtiments de détention.

La Commission a été saisie de ce dispositif.

La Commission s'est déjà prononcée favorablement sur plusieurs applications de contrôle d'accès reposant sur cette technique biométrique (*cf.* 22e rapport d'activité, p. 157). Elle a réaffirmé, à cette occasion, sa préférence pour de tels systèmes qui font appel à un élément d'identification qui, à la différence des empreintes digitales ou des éléments du corps humain pouvant servir à obtenir une empreinte génétique, ne peut être relevé à l'insu de la personne et ne laisse pas de « trace ».

Afin d'apprécier les modalités de fonctionnement de ce dispositif, une délégation de la Commission s'est rendue à la maison d'arrêt de la Santé qui l'expérimente.

Ce dispositif repose sur un système de reconnaissance automatique du contour de la main, couplé à une base centralisée, et associé à une carte d'identité à piste magnétique comportant la photographie du détenu. À l'arrivée d'un détenu dans un établissement carcéral, le personnel du greffe pénitentiaire procède au relevé de son identité (nom, prénom et numéro d'écrou), ainsi qu'à la numérisation de sa photographie et de celle des mesures du volume de sa main.

Cet enregistrement permet à la fois d'alimenter une base de données dédiée et propre à chaque établissement et de créer la carte d'identité du détenu. La carte sert à vérifier l'identité des détenus, lors de leurs déplacements à l'intérieur de l'établissement.

La base dans laquelle sont enregistrées les informations relatives au détenu est reliée à une ou plusieurs bornes situées à l'intérieur de l'établissement. La vérification d'identité se déroule de la façon suivante : le détenu présente sa carte d'identité au surveillant qui la place dans le lecteur magnétique de la borne. Le numéro d'écrou, enregistré sur la piste magnétique, permet d'interroger la base centrale, située au greffe de l'établissement, après que le détenu a placé sa main sur le lecteur biométrique situé dans la borne. Le système procède alors à la comparaison de la morphologie de la main du détenu concerné avec le gabarit enregistré dans la base.

Si la mesure de la main est identique à celle enregistrée dans la base centrale, les informations relatives à l'identité du détenu, ainsi que sa photographie s'affichent à l'écran ; au contraire, si la comparaison du gabarit et de la mesure ponctuelle ne correspondent pas, l'absence d'affichage de l'identité du détenu et de sa photographie laisse supposer une tentative d'usurpation d'identité et alerte le surveillant.

À l'issue de l'examen en séance du projet d'arrêté portant création de ce dispositif, la Commission a, par sa délibération n° 03-27 du 22 mai 2003, émis un avis favorable à sa mise en œuvre. L'arrêté du 10 juin 2003 portant création d'un système de reconnaissance biométrique de l'identité des détenus, a été publié au *Journal officiel* du 26 juin 2003.

D. Empreintes digitales et sécurité locale

Le cas du « roller-parc » de Levallois-Perret est un exemple du risque de banalisation de l'usage de la biométrie pour des applications où les exigences de sécurité sans être nulles, ne sont cependant pas impérieuses. Un administré de la ville de Levallois a porté à la connaissance de la CNIL la mise en œuvre, par la mairie, d'un système biométrique faisant appel à la reconnaissance des empreintes digitales pour contrôler les accès au « roller-parc », ouvert en avril 2003.

La Commission, n'ayant pas été saisie de la mise en œuvre de ce traitement d'informations nominatives, a demandé au maire de Levallois-Perret de le lui soumettre pour avis. Une mission d'information sur place a été menée afin d'apprécier les modalités de fonctionnement du système.

Le dispositif en cause reposait sur deux bases de données gérées de manière distincte : d'une part un fichier des abonnés au « roller-parc » comportant leurs coordonnées et un numéro d'ordre chronologique, d'autre part une base de données contenant l'enregistrement des caractéristiques des empreintes d'un doigt de l'abonné.

Les responsables du fichier ont expliqué que le recours à la technique biométrique avait été dicté par la volonté d'utiliser un système n'impliquant pas une gestion trop lourde pour contrôler l'accès au parc et par le souci d'éviter toutes manipulations de cartes oubliées, volées ou perdues et ainsi d'écarter tout risque de fraude.

La Commission, fidèle à sa doctrine élaborée dés 2000 à l'occasion de différents traitements recourant aux biométries, a rendu, le 16 décembre 2003, un avis défavorable à la mise en œuvre du traitement estimant qu'il n'apparaissait ni adéquat ni proportionné au regard de l'objectif poursuivi par la mairie. En effet, la constitution de bases de données d'empreintes digitales n'était pas en l'espèce justifiée par un impératif de sécurité et d'identification des personnes.

La ville de Levallois-Perret a informé la Commission qu'elle s'engageait à remplacer le traitement biométrique par un nouveau système d'identification qui sera soumis à l'avis de la Commission.

E. Vers une doctrine européenne ?

En 2003, les autres autorités nationales de protection des données de l'Union européenne ont été aussi confrontées à de nombreux traitements de données biométriques. C'est dans ce contexte que le groupe de l'article 29 a adopté le 1er août 2003 un document de travail sur la biométrie, publié en annexe à ce rapport. Ce faisant, le groupe répondait à l'une de ses missions visant à contribuer à l'application efficace et homogène des dispositions nationales adoptées en vertu de la directive, notamment à l'occasion de problématiques résultant de l'apparition de nouvelles technologies. Dans ce document, le groupe propose des orientations uniformes au niveau européen quant à l'application des règles de protection des données aux systèmes biométriques, tant à l'intention des professionnels de cette industrie qu'à celui de leurs utilisateurs.

Ce document, dont les préconisations centrales s'accordent parfaitement avec les idées fortes de la doctrine, que la CNIL a élaborée sur le sujet, apprécie l'application de chacun des principes de la directive 95/46 aux applications biométriques, et tout particulièrement des principes de finalité et de proportionnalité du traitement de ces données. De fait, le critère de proportionnalité a été déterminant dans presque toutes les décisions relatives au traitement de données biométriques prises jusqu'ici par les autorités de protection des données. À titre d'exemple, c'est en vertu de ce principe que le document préconise qu'il soit plutôt fait recours, à des fins de contrôle d'accès ou de contrôle des horaires, à des systèmes biométriques se référant à des caractéristiques physiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les empreintes digitales) ou à des systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), dans la mesure où ces systèmes créent manifestement moins de risques, au regard de la protection des libertés et des droits fondamentaux de la personne. Toutefois, le groupe admet que la mise en œuvre de telles bases de données centralisées est possible au regard des principes de finalité et de proportionnalité lorsqu'un impératif particulier de sécurité le justifie.

À l'heure actuelle, cependant, une tendance préoccupante se dessine : la baisse des coûts, l'innovation technologique, la pression du marché et les commodités d'usages risquent d'aboutir à la prolifération des fichiers d'empreintes digitales. Or ce risque en génère un autre : celui d'une relative désensibilisation du public vis-à-vis de ces questions, du fait d'une banalisation du recours aux données biométriques pour toutes sortes de finalités. Cette tendance ne peut être que confortée par le contexte sécuritaire international, qui a contribué à hisser la biométrie en haut de la liste des priorités de travail pour les autorités de protection des données personnelles européennes.

En 2003, trois événements importants ont confirmé le bien-fondé de cette anticipation. En premier lieu, les États-Unis ont adopté une législation qui nécessite la présence d'éléments d'identifiants biométriques dans les passeports des citoyens des États bénéficiant d'une exemption de visa à partir du 26 octobre 2004. En second lieu, les ministres de l'Intérieur du G8, réunis à Paris le 5 mai 2003, ont décidé la création d'un « groupe de travail d'experts de haut niveau » pour émettre des recommandations sur les technologies biométriques, susceptibles d'être employées dans les passeports et les visas. En troisième lieu, enfin, le Conseil européen de Thessalonique des 19 et 20 juin 2003 a confirmé la nécessité de *« dégager au sein de l'Union européenne une approche cohérente en ce qui concerne les identificateurs ou les données biométriques, qui permettrait d'appliquer des solutions harmonisées pour les documents des ressortissants de pays tiers, les passeports des citoyens de l'Union et les systèmes d'information (VIS et SIS II) »* et a invité la Commission *« à élaborer les propositions appropriées, en commençant par la question des visas ».*

Ainsi, outre le fait que le groupe de l'article 29 a prévu de revoir son document de travail à la lumière des développements technologiques et de l'expérience

que les autorités auront acquise sur ces questions, on ne doute pas qu'il aura de nouvelles occasions répétées de traiter des questions de biométrie, en particulier dans le cadre de contrôles aux frontières.

II. LE RENFORCEMENT DU CONTRÔLE DES PERSONNES

A. Sur le territoire national

1. LA SURVEILLANCE DES DÉLINQUANTS SEXUELS

Différentes affaires judiciaires portant sur des infractions de nature sexuelle commises par des récidivistes ont suscité l'émoi en 2003 et ont fait naître la volonté d'assurer un meilleur suivi des délinquants sexuels à leur sortie de prison.

C'est la raison pour laquelle le rapporteur au Sénat du projet de loi portant adaptation de la justice aux évolutions de la criminalité a présenté, lors de sa première lecture en octobre 2003, un amendement visant à créer un fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) destiné à garder en mémoire l'adresse ou les changements d'adresse des intéressés.

La loi a été définitivement adoptée le 5 février 2004 et, après examen par le Conseil constitutionnel, publiée au *Journal officiel* du 10 mars 2004.

La Commission n'a pas été consultée sur la décision de créer ce fichier puisqu'elle a été opérée par amendement. Elle n'en a pas moins délibéré à plusieurs reprises et fait connaître son avis aux parlementaires.

a) Les caractéristiques du FIJAIS

Ce fichier, qui sera tenu par les services du casier judiciaire national automatisé, sous l'autorité du ministre de la Justice et le contrôle d'un magistrat, a pour finalité, aux termes de l'article 706-53-1 du Code de procédure pénale, de *« prévenir le renouvellement des infractions mentionnées à l'article 706-47* [du Code de procédure pénale [1]] *et de faciliter l'identification de leurs auteurs »*.

Seront enregistrées dans le FIJAIS l'identité et l'adresse ou les adresses successives et, le cas échéant, des résidences des personnes — mineures ou majeures au moment des faits — qui ont fait l'objet de l'une des décisions juridictionnelles énumé-

1 Meurtre ou assassinat d'un mineur précédé ou accompagné de viol, de tortures ou d'actes de barbarie ; viol simple ou aggravé ; agressions sexuelles simples ou aggravées autres que le viol et sa tentative ; relations de nature sexuelle avec un mineur se livrant à la prostitution ; fait simple ou aggravé de favoriser la corruption d'un mineur ; fixation, enregistrement ou transmission à des fins de diffusion de l'image ou de la représentation à caractère pornographique d'un mineur ; fait de fabriquer, transporter ou diffuser un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou fait de faire commerce de ces messages ; atteinte sexuelle sans violence, ni contrainte, ni menace, ni surprise commise par un majeur sur un mineur.

rées à l'article 706-53-2 du Code de procédure pénale [1], ainsi que la décision judiciaire ayant justifié l'inscription, que cette dernière soit ou non définitive [2], et la nature de l'infraction. Les décisions de condamnation et celles prises en vertu de l'ordonnance du 2 février 1945 seront enregistrées au fichier dès leur prononcé.

Le procureur de la République ou le juge d'instruction compétent fera inscrire directement ces informations dans le fichier ; la dernière adresse de la personne concernée pourra être inscrite directement dans le fichier par les officiers de police judiciaire habilités à cette fin lorsqu'ils en recevront sa justification ou acquerront la connaissance de sa nouvelle adresse. Dans les deux cas, cette inscription se fera par l'intermédiaire d'un moyen de télécommunication sécurisé.

Toute personne inscrite au FIJAIS devra en effet, à titre de mesure de sûreté, justifier de son adresse une fois par an et déclarer, au plus tard dans un délai de quinze jours, ses changements d'adresse soit en adressant un courrier au gestionnaire du fichier, soit en se présentant au commissariat de police ou à la brigade de gendarmerie de son domicile. Si l'intéressé a été condamné de façon définitive pour un crime ou un délit puni de dix ans d'emprisonnement, il devra justifier, en personne et tous les six mois, de son adresse, sauf dispense prévue par l'article 706-53-10.

Ces informations devront être directement accessibles, par l'intermédiaire de systèmes de télécommunication sécurisés, aux magistrats, officiers de police judiciaire (dans le cadre de procédures concernant une infraction mentionnée à l'article 706-47 du Code de procédure pénale), préfets et administrations de l'État, pour l'examen des demandes d'agrément concernant des activités ou professions impliquant un contact avec des mineurs.

L'intéressé sera informé par l'autorité judiciaire de son inscription au fichier soit par notification à personne, soit par lettre recommandée adressée à sa dernière adresse déclarée, pourra obtenir communication de l'intégralité des informations le concernant, avec interdiction de lui délivrer une copie du relevé dont il lui sera seulement donné lecture [3], et éventuellement faire rectifier ou supprimer une mention le concernant selon la procédure prévue aujourd'hui pour rectifier les bulletins du casier judiciaire.

Enfin, il est prévu qu'un décret en Conseil d'État, pris après avis de la CNIL, déterminera les modalités et conditions d'application de ces nouvelles dispositions.

1 Condamnation, y compris par défaut si elle n'a pas été frappée d'opposition ou déclaration de culpabilité assortie d'une dispense ou d'un ajournement de la peine ; décision prononcée en vertu des articles 8 (placement, mise sous protection judiciaire, remise aux parents ou à un tuteur, admonestation, dispense de peine, relaxe), 15 (remise aux parents ou à un tuteur, placement), 15-1 (confiscation, interdiction de paraître, interdiction de rencontrer la victime ou les coauteurs ou complices, mesure d'aide ou de réparation, obligation de suivre un stage de formation civique), 16 (remise aux parents ou à un tuteur, placement), 16 bis (mise sous protection judiciaire) et 28 (mesures de protection ou de surveillance à l'occasion d'une modification du placement ou de la garde) de l'ordonnance du 2 février 1945 relative à l'enfance délinquante ; composition pénale prévue par l'article 41-2 du Code de procédure pénale dont l'exécution a été constatée par le procureur de la République ; décision de non-lieu, de relaxe ou d'acquittement fondée sur l'abolition du discernement ou du contrôle des actes de l'intéressé au moment des faits ; décision de même nature prononcée par une juridiction étrangère.

1 Cette précision a été ajoutée lors des débats parlementaires intervenus après l'adoption de l'amendement sénatorial créant le FIJAIS.

3 Cette règle, protectrice de l'intéressé, est identique à celle édictée par l'article 777-2 du Code de procédure pénale s'agissant du casier judiciaire.

La Commission a souhaité faire connaître ses observations au rapporteur du projet de loi à l'Assemblée nationale, lors d'une audition intervenue le 5 novembre 2003.

Celles-ci ont plus particulièrement porté sur trois points :
— le caractère automatique de l'inscription et la durée uniforme de la durée de conservation des informations nominatives enregistrées, fixée à quarante ans, sans que soient pris en considération, notamment, la nature de l'infraction commise, l'âge de son auteur au moment des faits et la gravité de la mesure ou de la décision prononcée à son encontre ;
— l'extrême sensibilité des informations enregistrées dans le fichier, qui appelle des garanties voisines de celles qui entourent le fonctionnement du casier judiciaire national automatisé, aussi bien pour l'alimentation du fichier que pour sa consultation et son accès ;
— la possibilité pour les préfets d'avoir accès à ce fichier pour *« l'examen des demandes d'agrément concernant des activités ou professions impliquant un contact avec des mineurs »*, la Commission considérant que cet accès à des fins purement administratives ne s'inscrivait pas dans la finalité judiciaire de ce fichier et faisait en tout état de cause double emploi avec la possibilité pour ces autorités d'obtenir communication du bulletin n° 2 de leur casier judiciaire.

b) Les modifications intervenues au cours des débats parlementaires

Si les modifications apportées à ces dispositions du texte postérieurement à l'adoption de l'amendement sénatorial ayant créé le fichier ne répondent que partiellement aux observations formulées par la Commission, des garanties nouvelles au regard de l'esprit et de la lettre de la loi du 6 janvier 1978 ont cependant été apportées.

S'agissant ainsi des conditions d'alimentation et de mise à jour du fichier, l'inscription au FIJAIS de l'auteur d'un des délits prévus par l'article 706-47 du Code de procédure pénale perd son caractère automatique dans le texte définitif de la loi, alors qu'à l'origine aucune distinction n'était opérée selon la gravité de l'infraction concernée. L'inscription au FIJAIS des décisions concernant les auteurs de délits punis de moins de cinq années d'emprisonnement ne peut désormais être ordonnée que sur décision expresse de la juridiction ou du procureur de la République.

La loi prévoit également, afin d'éviter toute erreur susceptible de nuire à une personne ne figurant pas dans le FIJAIS, qu'en cas de consultation du fichier, les informations qui y sont enregistrées ne sont accessibles *« qu'après vérification, lorsqu'elle est possible, de l'identité de la personne concernée* [...] *au vu du répertoire national d'identification »*.

Ensuite, les dispositions de l'article 706-53-4 du Code de procédure pénale prévoient désormais que la durée de conservation des informations enregistrées au fichier sera modulée — ainsi que la Commission en avait exprimé le souhait — selon la gravité de l'infraction : trente années s'il s'agit d'un crime ou d'un délit puni d'au moins dix ans d'emprisonnement, vingt ans dans les autres cas.

Dès que la décision judiciaire rendue à son encontre aura été effacée du bulletin n° 1 de son casier judiciaire, l'intéressé pourra en outre demander au procureur de la République d'ordonner la rectification ou l'effacement des informations le concernant dont la conservation, compte tenu de la finalité du fichier, n'apparaît plus nécessaire au regard de la nature de l'infraction, de l'âge de la personne lors de la commission, du temps écoulé depuis lors et de la personnalité actuelle de l'intéressé ; en cas de refus, la loi prévoit une possibilité de recours devant le juge des libertés et de la détention, puis devant le président de la chambre de l'instruction.

En outre, les informations inscrites dans le fichier, qu'elles concernent un auteur majeur ou mineur au moment de la commission des faits, en seront désormais retirées en cas d'intervention d'une décision définitive de non-lieu, de relaxe ou d'acquittement, sauf lorsque cette décision est fondée sur l'existence, au moment de la commission de l'infraction, d'un trouble psychologique ou neuropsychique ayant aboli le discernement de l'auteur des faits ou le contrôle de ses actes.

S'agissant des destinataires, les préfets et administrations de l'État ne pourront interroger le FIJAIS pour l'examen des demandes d'agrément concernant des activités ou professions impliquant un contact avec des mineurs que sur le seul critère de l'identité de la personne concernée.

Enfin, à l'instar des dispositions concernant le casier judiciaire national automatisé, la loi prohibe, d'une part, tout rapprochement et toute interconnexion du FIJAIS avec un autre fichier qui ne dépendrait pas du ministère de la Justice et, d'autre part, toute mention des informations inscrites au FIJAIS dans un autre fichier du même type.

Saisi de deux recours contre ce texte, le Conseil constitutionnel n'a, dans sa décision du 2 mars 2004, invalidé aucune des dispositions relatives au FIJAIS, ni émis de réserve d'interprétation les concernant et a décidé, en insistant sur les garanties, que « *ces dispositions sont de nature à assurer, entre le respect de la vie privée et de la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* ».

Il appartiendra à la Commission, lors de l'examen du décret prévu par l'article 706-53-12 du Code de procédure pénale de s'assurer tout particulièrement que la confidentialité des informations inscrites au fichier, et tout spécialement celle de l'adresse des intéressés, est assurée par des mesures de sécurité appropriées évitant toute divulgation de ces informations et tout risque d'utilisation détournée.

2. LA CONSERVATION DES DONNÉES DE CONNEXION

Selon la police et les services de sécurité, l'exploitation des données de connexion aux réseaux de télécommunications et à internet (Qui a appelé qui ? D'où ? Combien de temps ? Etc.) est un enjeu majeur pour les enquêtes relatives au terrorisme et à la grande criminalité. Le gisement d'informations existe. Il a été constitué par les opérateurs de télécommunications pour leurs propres besoins commerciaux et financiers. Peut-il être utilisé à des fins radicalement différentes, si légitimes

soient-elles ? À quelles conditions ? Ces questions sont posées au législateur et à la CNIL depuis plusieurs années. Le dossier a avancé en 2003 sans être encore conclu.

a) Historique du dossier

Au cours de l'année 2003, la Commission a été saisie pour avis par le ministère de la Justice du projet de décret relatif à la conservation des données relatives à une communication par les opérateurs de communications électroniques et portant modification du Code des postes et télécommunications. Ce décret doit être pris pour l'application de l'article L. 32-3-1 du Code des postes et télécommunications introduit par l'article 29 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (LSQ) et complété par la loi n° 2003-2390 du 18 mars 2003 relative à la sécurité intérieure. Cet article traite de la conservation par les opérateurs de communications électroniques des données de connexion, c'est-à-dire les informations qui sont produites ou nécessitées par l'utilisation de réseaux de communications électroniques, qu'il s'agisse des communications téléphoniques ou des connexions au réseau internet. La loi du 15 novembre 2001 prévoyait que cette disposition — figurant dans son chapitre V relatif aux dispositions renforçant la lutte contre le terrorisme — n'était adoptée que pour une durée allant jusqu'au 31 décembre 2003. La loi du 18 mars 2003 a, par la suite, pérennisé ce dispositif.

L'article L. 32-3-1 du Code des postes et télécommunications, dans son état actuel, en même temps qu'il pose un principe général d'anonymisation ou d'effacement instantané de ces données, distingue celles qui peuvent être conservées à des fins de facturation (pendant un an), celles qui peuvent être conservées à des fins de sécurité du réseau des opérateurs, et enfin celles qui ne sont conservées qu'aux fins exclusives d'enquêtes judiciaires pendant une période maximale d'un an.

Les informations traitées dans ce cadre ne visent qu'à permettre l'identification des personnes utilisatrices des services fournis par les opérateurs et à recueillir les caractéristiques techniques des communications assurées par ces derniers.

Compte tenu des enjeux, la Commission, avant même d'être saisie pour avis du projet de décret, avait lancé une vaste opération de consultation des opérateurs de communications électroniques. En outre, au cours de l'année 2003, la Commission avait été saisie d'une demande de conseil de l'Association des fournisseurs d'accès et de services internet (AFA) relative à la possibilité pour un fournisseur d'accès d'exiger, de manière systématique, la communication du numéro appelant d'un internaute qui utiliserait ses services. Selon l'AFA, l'enregistrement de cette donnée serait un moyen efficace pour prévenir le développement d'appels cachés par une personne utilisant de manière frauduleuse les identifiants de connexion (nom de compte, mot de passe) d'un abonné et permettre au fournisseur d'accès de s'assurer que l'utilisateur d'une offre commerciale est bien le bénéficiaire identifié auprès du fournisseur d'accès. En l'absence du décret visé à l'article 29 de la LSQ, la Commission a estimé que le fait de subordonner l'obtention d'un service d'accès à internet à la levée du secret permanent dont peut bénéficier la ligne téléphonique d'une personne est disproportionné. En effet, une telle solution reviendrait, en l'état actuel, à imposer

à l'abonné de ne plus utiliser que le mode du secret appel par appel, ce qui aurait pour effet d'amoindrir la protection des personnes concernées.

Le dispositif dont le décret vise à préciser les modalités d'application était, à l'origine, prévu en 2001 par le projet de loi sur la société de l'information qui n'a jamais été examiné par le Parlement, mais sur lequel la Commission avait été consultée et avait rendu un avis (délibération n° 01-018 du 3 mai 2001). Cet avis avait été l'occasion pour la Commission de souligner *« le caractère inédit du dispositif retenu »* qui déroge au principe de finalité puisqu'il fait obligation aux opérateurs de communications électroniques de conserver, aux fins exclusives de faciliter le travail des autorités policières et judiciaires, des données qui se rapportent à l'ensemble des personnes utilisant leurs services et dont la conservation ne présente aucune utilité pour eux. La Commission a, dès lors, estimé indispensable que son avis rappelle le contexte général dans lequel il s'inscrit et qui, en dépit de son apparente technicité, dépasse largement les spécificités de la technologie en mettant en cause les principes essentiels de la protection des données à caractère personnel.

Il convient par ailleurs de noter qu'au-delà de l'avis juridique de la CNIL sur la rédaction de ce projet de décret, la délibération vise aussi à permettre aux opérateurs de communications électroniques d'apprécier la portée précise du dispositif prévu par ce décret.

b) L'avis de la CNIL

LES CATÉGORIES DE DONNÉES VISÉES PAR LE DÉCRET

La délibération n° 03-056 du 9 décembre 2003 s'attache en premier lieu à définir les limites du décret qui est soumis à l'avis de la Commission. Il est, en effet, apparu indispensable de préciser le champ d'application du décret qui ne doit concerner que les seules données techniques relatives à une communication électronique, c'est-à-dire les données qui sont automatiquement générées et collectées par l'opérateur à l'occasion de celle-ci. La Commission a donc été amenée à préciser que les données relatives à l'utilisateur lui-même (ses nom, prénom, adresse, mode de paiement, etc.) n'ont pas à être visées par le décret. On peut illustrer cette position en prenant l'exemple d'une personne qui s'abonnerait à un fournisseur d'accès et qui lui fournirait, en vue du paiement de son contrat d'abonnement, des données relatives à son nom, prénom, adresse, numéro de compte bancaire, etc. mais qui ne se connecterait jamais à internet. Le fournisseur d'accès ne disposera donc d'aucune donnée de connexion (la personne ne s'est jamais connectée) mais traitera bien les données relatives à l'utilisateur lui-même afin de lui facturer son abonnement, de lui envoyer des informations par voie postale, de le prospecter, etc.

On voit ici très clairement le partage entre les données dites « de connexion » (des données à caractère techniques liées à l'utilisation d'un réseau de communication) et, même lorsque ces données techniques peuvent permettre directement l'identification d'un utilisateur, les données « clients » qui sont celles traitées classiquement dans le cadre d'un abonnement.

La délibération relève, dès lors, que le décret dont la Commission a été saisie ne doit traiter que de la question de la conservation des *« données techniques relatives à une communication »* (alinéa 1er de l'article R. 9-1 nouveau du Code des postes et télécommunications introduit par l'article 2 du projet de décret) et non de la conservation des données dites « clients ». Aussi, sans préjuger de l'importance de cette dernière question, la Commission n'avait donc pas à se prononcer, dans le cadre de l'avis sur le décret dont elle a été saisie, sur la conservation par les opérateurs de communications électroniques des données qui ne concernent pas directement une communication.

En second lieu, pour celles des données dont la mention dans le décret ne peut être contestée, la délibération de la CNIL en précise la détermination et la définition. Ces dernières devant être conservées en dérogation au principe général d'effacement ou d'anonymisation, il convient qu'elles soient précisément définies, ce que ne faisait pas le projet de décret, puisqu'il s'agit d'une obligation qui pèse sur les opérateurs.

L'APPLICATION DES PRINCIPES RELATIFS À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AU RÉGIME DÉROGATOIRE MIS EN ŒUVRE PAR LE DÉCRET

L'application de la loi « informatique et libertés » aux opérations de conservation et de traitement des données visées par le décret a conduit la Commission à rappeler, d'une part, l'application du principe de finalité qui interdit à un opérateur d'utiliser une donnée conservée dans le cadre d'une finalité spécifique pour une autre finalité et, d'autre part, les conditions dans lesquelles les autorités, notamment judiciaires, peuvent avoir accès aux informations détenues par les opérateurs de communications électroniques. Surtout, il est souligné que c'est à la lumière des principes généraux relatifs à la protection des données personnelles que la Commission a examiné le projet de décret, quand bien même certaines d'entre elles seraient conservées sur la base d'un régime dérogatoire à ces principes.

S'agissant des catégories de données conservées pour les besoins de la facturation et du paiement des prestations de communications électroniques, la Commission a relevé que le choix fait par le législateur de renvoyer à un décret le soin de fixer la liste limitative des catégories de données qui peuvent être conservées par les opérateurs par exception au principe général d'effacement ou d'anonymisation des données relatives à une communication, empêche les opérateurs de conserver — notamment à des fins de preuve en matière de contestation de la facturation ou du paiement des prestations — une donnée qui ne serait pas à l'origine prévue par le décret mais dont la conservation pourrait être rendue nécessaire par l'évolution technique de leurs services. Cette possibilité d'évolution est d'ailleurs implicitement prévue par la directive du 12 juillet 2002 qui, à la différence de la directive du 15 décembre 1997 qu'elle abroge et remplace, ne précise plus limitativement les données pouvant être conservées au titre des données de connexion, dites « données relatives au trafic », mais se contente de les définir de manière générique en tant que *« données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation »*.

À défaut d'une modification du cadre législatif, la délibération recommande aux pouvoirs publics de porter une attention toute particulière aux futurs besoins des opérateurs afin de permettre, le cas échéant, une évolution du dispositif, soit par voie réglementaire, soit par des procédures simplifiées.

La liste des données visées par le décret a été établie à la suite d'une concertation entre les opérateurs de communications électroniques — qui ont fait part des données qui leur paraissent nécessaires pour justifier leur facturation — et la direction générale de l'industrie, des technologies de l'information et des postes (DIGITIP). La liste présentée dans le décret reflète ces besoins. Pour autant, les données relatives au numéro appelé et à la durée d'une connexion à internet ne sont pas prévues dans le cadre de l'article R. 9-1-1 issu du projet de décret. La Commission a préconisé que ces informations — indispensables, par exemple, lorsqu'un opérateur téléphonique doit justifier le montant d'une facture — soient présentes au titre des données qui peuvent être traitées par les opérateurs.

Enfin, la Commission a rappelé que la durée de conservation de ces données est fixée par la loi à un an à compter du jour du paiement et écarte, ainsi, les règles applicables en matière de prescription commerciale (dix ans) ou fiscale (de trois à six ans).

Concernant les catégories de données conservées en vue d'assurer la sécurité des réseaux des opérateurs de communications électroniques et sur leur durée de conservation, l'article 20 de la loi du 18 mars 2003 pour la sécurité intérieure a introduit la possibilité pour ces opérateurs de conserver, en dérogation au principe d'effacement ou d'anonymisation précité, certaines données en vue d'assurer la sécurité de leurs réseaux. Le décret fixe la liste de ces données et leur durée de conservation qui ne peut être supérieure à trois mois. Ces dispositions n'ont pas appelé d'observations particulières de la part de la Commission.

La partie du projet de décret concernant les catégories de données conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et sur leur durée de conservation est le point central sur lequel la Commission a eu à se prononcer, notamment au regard de la durée de conservation des données concernées. Concernant la liste des données, la délibération vise à ce que certaines d'entre elles soient interprétées de manière restrictive afin de respecter le dispositif législatif qui impose que les informations conservées au titre du décret ne se rapportent qu'à l'identification des personnes utilisatrices des services fournis par les opérateurs et aux caractéristiques techniques des communications assurées par ces derniers, et non aux informations consultées ou au contenu des informations échangées.

Enfin, et surtout, la Commission a estimé que la durée de conservation des données au titre de la recherche, de la constatation et de la poursuite des infractions pénales ne devait pas être supérieure à trois mois. Elle a considéré, en effet, qu'aucun élément de fait ou de droit n'était de nature à modifier la position qu'elle avait prise lors de son avis relatif au projet de loi sur la société de l'information. Cette position est confortée sur le plan international par la déclaration des commissaires européens à la protection des données adoptée lors de la conférence internationale de

Cardiff (9-11 septembre 2002) relative à la conservation systématique et obligatoire des données de trafic des télécommunications qui concluait que *« la conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable »*.

À travers son avis, la Commission a proposé un point d'équilibre à atteindre en matière de conservation des données issues de l'utilisation de moyens de communications électroniques entre, d'une part, les mesures — légitimes — permettant aux autorités policières et judiciaires d'exercer leurs missions dans les meilleures conditions possibles et, d'autre part, les principes devant s'appliquer à la protection des données à caractère personnel dans une société démocratique.

B. Au passage des frontières

Au-delà de la lutte contre l'immigration clandestine, dans le cadre de laquelle les États de l'Union européenne ont mis en place des outils de coopération et d'échange d'informations tel que le système EURODAC, c'est la lutte contre le terrorisme international qui justifie de plus en plus le renforcement des moyens de contrôle au passage des frontières. Le développement de ces moyens de contrôle ne doit toutefois pas s'effectuer au détriment de la protection des libertés individuelles et des droits fondamentaux, y compris le respect de la vie privée et la protection des données. La recherche de cet équilibre apparaît difficile dans un contexte international en raison de l'existence d'intérêts et de législations différents, comme en témoignent les négociations amorcées depuis plus d'un an entre les États-Unis et l'Union européenne au sujet du transfert des données passagers vers les autorités américaines.

1. L'OBLIGATION DE TRANSFERT DES DONNÉES PASSAGERS VERS LES ÉTATS-UNIS

Dans le cadre de la lutte contre le terrorisme et les actes criminels, les États-Unis ont adopté, le 19 novembre 2001, une législation sur la sécurité de l'aviation et du transport *(The Aviation and Transportation Security Act)* et le 5 mai 2002, une loi renforçant les conditions d'entrée sur le territoire américain *(Enhanced Border Security and Visa Entry Reform Act)*. Ainsi, depuis le 5 mars 2003, ces mesures imposent aux compagnies aériennes de communiquer aux services des douanes et de sécurité américains des informations personnelles relatives à leurs passagers à destination des États-Unis, sous peine de contrôles renforcés, d'amendes et du refus du droit d'atterrir.

Les informations concernées sont celles collectées par les compagnies aériennes et les agences de voyage auprès des passagers dans le cadre des services de réservation. Stockées dans les bases de données des systèmes de réservation, elles sont échangées entre les entreprises intervenantes à partir du moment de la réservation jusqu'à la réalisation des prestations demandées par les passagers. Les données présentes dans ces bases prennent la forme d'enregistrements

d'informations standardisés au plan international dénommés « PNR » *(Passenger Name Record)*.

Le PNR peut ainsi contenir, en fonction des prestations offertes par les compagnies et demandées par le client, des renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, l'itinéraire du déplacement qui peut comporter plusieurs étapes, les indications des vols concernés (numéro des vols successifs, dates, heures, classe économique, business, etc.), le groupe de personnes pour lesquelles une même réservation est faite, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les services demandés à bord tels que le numéro de place affecté à l'avance, les repas (végétarien, asiatique, casher, etc.) et les services liés à la santé (diabétique, aveugle, sourd, assistance médicale etc.).

S'agissant d'informations associées à l'identité des passagers, leur traitement et leur communication à des tiers, en l'espèce les autorités américaines, sont encadrés par la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

La communication de données collectées à des fins commerciales à une autorité publique d'un pays tiers en raison d'une obligation légale est sans précédent. En outre, cela constitue une exception à l'article 6 b) de la directive précitée selon lequel les données sont collectées pour des finalités déterminées et qu'elles ne sauraient être traitées ultérieurement de manière incompatible avec ces finalités. Par ailleurs, l'Union européenne a jusqu'à présent toujours considéré que les États-Unis n'offraient pas un niveau de protection adéquat des données à caractère personnel.

Dès lors, le transfert d'informations exigé par les États-Unis apparaît, en l'état, illégal au regard de la législation européenne et nécessite que les parties en présence déterminent une base juridique adéquate de nature à permettre sa mise en œuvre. L'article 25 paragraphe 6, de la directive 95/46/CE prévoit un tel cas de figure, en ce qu'il dispose que la Commission européenne peut constater qu'un pays tiers assure un niveau de protection adéquat en raison de ses engagements internationaux.

La détermination de cet accord international a donné lieu à des discussions entre la Commission européenne et les autorités américaines tout au long de l'année 2003 ainsi qu'à de nombreuses réactions de la part des autorités de protection des données.

2. LA POSITION DE LA CNIL ET DES AUTORITÉS DE PROTECTION DES DONNÉES

Les compagnies aériennes européennes, partagées entre les menaces américaines et le fait de procéder à des traitements illégaux au regard de la législation européenne, se sont naturellement adressées aux autorités en charge de la protection des données à caractère personnel de leurs États afin de connaître leur position sur la mise en œuvre d'un tel dispositif. La CNIL et l'ensemble de ses homologues euro-

péens se sont en conséquence exprimés le 24 octobre 2002 au travers d'un avis du groupe des commissaires européens en charge de la protection des données (G29), institué par l'article 29 de la directive européenne 95/46/CE.

Le groupe de l'article 29 indique dans cet avis que la transmission des données contenues dans le PNR aux autorités américaines constitue un détournement de finalité du traitement informatique dans la mesure où elles ont été collectées à des fins commerciales et non pour des raisons de sécurité. Il précise également que certaines informations figurant dans le dossier de réservation d'un passager sont de nature à révéler à un tiers des données susceptibles de porter atteinte à la vie privée des personnes concernées, *a fortiori* lorsqu'il s'agit d'informations susceptibles de faire apparaître les origines raciales ou les opinions politiques, philosophiques, religieuses ou les mœurs. En outre, le groupe de l'article 29 rappelle que la transmission de données personnelles vers un pays tiers ne peut s'effectuer qu'à condition que celui-ci offre un niveau adéquat de protection de ces informations, ce qui n'est pas le cas des États-Unis. En conclusion, le groupe de l'article 29 estime qu'il convient d'entamer des négociations à l'initiative des États membres et le cas échéant par la Commission européenne, en vue d'un accord international.

Pour sa part, la CNIL a clairement indiqué aux compagnies aériennes que la transmission de ces données personnelles était illégale au regard tant de la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 que de la législation européenne en matière de protection des données personnelles, précisant également qu'en tout état de cause, il lui apparaissait nécessaire que les personnes concernées soient informées dès la collecte de l'objet spécifique du traitement aux États-Unis, ainsi que des destinataires des données.

C'est dans ce contexte que la Commission européenne et les services des douanes américaines, suite à plusieurs entretiens, ont effectué le 18 février 2003 une déclaration commune prenant acte de certaines garanties offertes par les autorités américaines. Toutefois, le 13 mars, le Parlement européen a adopté une résolution dénonçant cet « accord » dans laquelle il soulignait que les exigences américaines constituaient une violation des règles européennes en matière de protection des données à caractère personnel et invitait en conséquence la Commission européenne à engager de nouvelles négociations.

Les autorités américaines ont alors communiqué le 22 mai 2003 de nouvelles dispositions *(Undertakings of the United States Bureau of Customs and Border Protection and the United states transportation security administration)* résultant des négociations réouvertes avec la Commission et faisant état de l'ensemble des engagements pris par les États-Unis.

En réaction, le groupe de l'article 29 a émis un avis le 13 juin 2003 dans lequel il a précisé les garanties supplémentaires devant compléter les engagements américains issus de ces nouvelles dispositions afin que les données relatives aux passagers des vols aériens transférées vers les États-Unis puissent être considérées comme bénéficiant d'un niveau adéquat de protection.

Par ailleurs, le 12 septembre 2003 à Sydney, lors de la vingt-cinquième conférence internationale des commissaires à la protection des données et à la vie

privée, ceux-ci ont adopté une résolution relative aux transferts des données passagers. Ils ont ainsi constaté que ces mesures étaient susceptibles de porter atteinte aux libertés fondamentales et d'entrer en conflit avec les principes internationaux de protection des données. Ils ont également affirmé, d'une part, que les États devaient, dans le cadre de la lutte contre le terrorisme, définir leurs actions en assurant le plein respect des principes fondamentaux de la protection des données, d'autre part, que *« lorsqu'un transfert international et régulier de données personnelles s'avère nécessaire, il devrait intervenir dans un cadre prenant en compte la protection des données, par exemple sur le fondement d'un accord international fixant les exigences adéquates de protection des données, incluant la définition d'une finalité claire et déterminée, une collecte des données adéquates et non excessives, une durée de conservation des données limitée, l'information des personnes concernées, la garantie des droits des personnes concernées et un contrôle indépendant »*.

Les réactions unanimes des autorités en charge de la protection des données à caractère personnel, tant au niveau national, européen qu'international ont conduit la Commission européenne à relancer les négociations avec les États-Unis en vue d'obtenir des garanties supplémentaires et à s'interroger sur la nécessité de définir une politique globale de l'Union européenne relative à l'utilisation des données passagers pour la sécurité aérienne et aux frontières.

3. VERS UNE POLITIQUE GLOBALE DE L'UNION EUROPÉENNE

La Commission européenne a adopté le 16 décembre 2003 une communication faisant état d'une proposition pour une approche globale de l'Union européenne sur l'utilisation des données passagers pour la sécurité aérienne et aux frontières. Elle y expose notamment les résultats de ses discussions avec les États-Unis au vue desquelles elle propose d'établir un régime juridique stable sous la forme d'un accord bilatéral destiné à fonder en droit l'obligation des compagnies aériennes de transmettre les données.

Elle indique également que cet accord bilatéral doit être associé à une décision reconnaissant le niveau adéquat de la protection assuré par les autorités américaines en charge du contrôle aux frontières, en annexe de laquelle les engagements de ces autorités devront figurer. Enfin la Commission propose, pour faire face aux demandes de même nature d'autres pays, de promouvoir un accord multilatéral au sein de l'Organisation internationale de l'aviation civile (OACI).

S'agissant du résultat des discussions avec la partie américaine, la Commission précise dans le cadre de cette communication qu'elle a obtenu que la liste des données transférées soit réduite de trente-huit à trente-quatre champs, que les données sensibles soient transmises puis détruites, et que l'utilisation des données soit limitée à la lutte contre le terrorisme et d'autres formes de criminalité grave à caractère international. Elle indique par ailleurs que la conservation des données transférées n'excédera pas la durée de l'accord envisagé, soit trois ans et demi au terme desquels il sera réexaminé et que l'application par les États-Unis de leurs engagements est soumise à un examen annuel. Enfin, la Commission signale qu'elle

envisage de créer un organisme européen chargé de collecter les dossiers de passagers à partir des systèmes de réservation et de les transmettre aux autorités concernées après avoir filtré certaines informations.

À la suite de cette communication, le G29 a de nouveau rendu un avis le 29 janvier 2004 dans lequel il rappelle les principes devant être respectés afin d'assurer une protection appropriée des données personnelles des passagers aériens destinées à être transférées aux autorités américaines. Il précise également que, malgré quelques progrès, les termes de l'accord devant résulter des discussions avec les États-Unis ne permettent pas en l'état de considérer qu'un niveau adéquat de protection des données avait été atteint.

Au moment de la rédaction du présent rapport annuel, la position des États membres ainsi que celle du Parlement européen, très circonspect sur l'ensemble de l'affaire, sont attendues sur les différents textes proposés. La Commission européenne a, pour sa part, indiqué qu'elle souhaitait que l'ensemble des textes soit adopté avant la fin du mois d'avril 2004. La détermination d'un cadre juridique de nature à garantir une protection adéquate des données apparaît d'autant plus urgente que la plupart des compagnies aériennes communiquent actuellement les données de leurs passagers à destination des États-Unis, sous peine de les voir soumis à des contrôles renforcés et peut-être subir une interdiction du territoire américain.

III. LE DROIT D'ACCÈS AUX FICHIERS DE POLICE

En application des articles 39 et 45 de la loi du 6 janvier 1978, toute personne a le droit de demander à la CNIL d'entreprendre des vérifications relatives aux renseignements la concernant pouvant figurer dans des traitements automatisés et des fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Aucun fichier de cette nature n'échappe à de telles vérifications. Celles-ci sont effectuées par les membres de la Commission appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes.

A. Données générales

Depuis sa création, la CNIL a reçu 8 686 demandes de droit d'accès indirect qui ont donné lieu à plus de 14 500 investigations. Le nombre des requêtes de 2003 est toujours élevé. Ces demandes de droit d'accès indirect conduisent à plus de 2 500 vérifications, une même requête pouvant concerner plusieurs traitements (par exemple pour les fichiers de police consultés lors d'une assermentation, le fichier du système de traitement des infractions constatées — STIC—, les fichiers de sécurité publique des commissariats et le fichier JUDEX de la gendarmerie nationale).

Évolution des demandes de droit d'accès indirect reçues à la CNIL depuis 1995

	1995	1996	1997	1998	1999	2000	2001	2002	2003
Requêtes reçues	243	320	385	401	671	817	836	1 264	1 163

L'analyse des demandes montre que, de plus en plus, les requérants saisissent la CNIL à la suite d'un refus d'embauche (par exemple dans les sociétés de gardiennage et de sécurité) ou d'un licenciement résultant d'une enquête administrative défavorable ou encore du non-renouvellement d'une autorisation de port d'arme (notamment pour les agents de sécurité employés par la RATP ou par la police ferroviaire).

À cet égard, il doit être rappelé que depuis les lois du 15 novembre 2001 et du 18 mars 2003 sur la sécurité intérieure, les enquêtes administratives réalisées pour l'accès à certaines catégories d'emplois publics ou privés relevant notamment du domaine de la sécurité ou de la défense, peuvent donner lieu à des consultations de fichiers de police judiciaire tels que le STIC ou JUDEX.

Les autres demandes peuvent résulter d'un refus de délivrance de visa ou d'un titre de séjour du fait d'une inscription dans le système d'information Schengen ou dans un fichier d'opposition, d'une interpellation par les services de police ou de la gendarmerie, d'articles de presse ou d'émissions télévisées sur les fichiers des renseignements généraux, de police ou encore d'informations diffusées sur des sites internet décrivant les modalités de droit d'accès aux fichiers de police.

Au cours de l'année 2003, 1 962 vérifications ont été effectuées dont 95 % opérées dans les fichiers du ministère de l'Intérieur.

Ces 1 962 vérifications concernent des saisines reçues au cours des années 2000, 2001, 2002 et 2003 car la recherche d'une éventuelle fiche peut nécessiter plusieurs mois et plusieurs investigations notamment pour le contrôle des mises à jour et des suppressions.

Ministère de l'Intérieur	**1 861**
— Renseignements généraux (RG)	686
— Police judiciaire (PJ)	435
— Sécurité publique (SP)	92
— Direction de la surveillance du territoire (DST)	46
— Système d'information Schengen (SIS)	599
— Direction de la sûreté et de la protection du secret du CEA (DSPS)	3
Ministère de la Défense	**101**
— Gendarmerie nationale (GEND)	51
— Direction de la protection et de la sécurité de la défense (DPSD)	26
— Direction générale de la sécurité extérieure (DGSE)	24
Total	**1 962**

B. Les fichiers autres que ceux des renseignements généraux et de Schengen

Le résultat des investigations menées en 2003 à l'exclusion de celles relatives aux fichiers des renseignements généraux (686) et du système d'information Schengen (599) soit 677 investigations menées est le suivant :

Fichiers	PJ	SP	DST	DSPS	GEND	DPSD	DGSE	Total
Pas de fiche	204	72	36	2	27	16	22	379
Fiche sans suppression	178	19	10	1	23	8	2	241
Suppression totale ou partielle	50	1	–	–	1	2	–	54
Mise à jour	3	–	–	–	–	–	–	3
Total	435	92	46	3	51	26	24	**677**

Les délais d'instruction de ces saisines sont généralement longs, dans la mesure où les vérifications portent non seulement sur les données informatisées mais aussi sur tous les dossiers « papier » qui ont été à l'origine de l'enregistrement (compte rendu d'enquête, procès-verbal d'audition…) et qui sont détenus dans les directions départementales et régionales des services de police. Ceci nécessite de la part des services concernés du ministère de l'Intérieur et du ministère de la Défense un travail de regroupement des différentes pièces conservées tant au niveau local que central. Ce qui prend du temps…

Les investigations dans ces fichiers et en particulier dans le système de traitement des infractions constatées (STIC) ont conduit la CNIL à faire procéder dans 23 % des cas (53 saisines sur les 231 requérants fichés à la police judiciaire) à des mises à jour ou même à la suppression des signalements erronés, manifestement non justifiés ou dont le délai de conservation était expiré.

Ainsi, une personne était encore signalée dans une affaire d'escroquerie datant de vingt ans et dans laquelle elle n'était que témoin.

Un requérant était signalé dans le STIC comme mis en cause dans une affaire d'usage de stupéfiant. En réalité, il avait été entendu dans le cadre de la mise en examen d'un ami pour usage et cession de produits stupéfiants dans la mesure où il partageait le même appartement que l'auteur des faits.

Une personne était signalée comme mise en cause dans une affaire d'enlèvement de mineur qui avait trouvé refuge (une nuit) chez lui alors que le mineur s'y était rendu de plein gré.

Une personne s'était vue refuser sa candidature à un concours de recrutement de gardien de la paix au motif qu'elle était inscrite dans le STIC en qualité de « mise en cause » dans une affaire de vol alors qu'elle était mineure au moment des faits. Compte tenu de la suppression de cette inscription, à la demande de la CNIL, la direction générale de la police nationale en a informé le préfet afin que sa candidature soit réexaminée.

Une personne âgée était signalée en tant que mise en cause dans une affaire de vol à main armée avec séquestration alors qu'elle était en réalité la victime.

Un requérant était signalé dans une affaire de mœurs de 1994 alors qu'il faisait de l'assistance éducative en milieu défavorisé. Après enquête et instruction, le requérant avait été totalement innocenté.

Il faut noter que la procédure de communication des fiches STIC aux personnes concernées, avec l'accord du ministère de l'Intérieur et du procureur de la République, qui est prévue par le décret du 5 juillet 2001 créant le STIC, n'a toujours pas été mise en œuvre.

C. Les fichiers des renseignements généraux

Le décret du 14 octobre 1991 a fixé les modalités d'exercice du droit d'accès aux fichiers des renseignements généraux. Les membres désignés par la CNIL pour mener ces investigations peuvent, en accord avec le ministre de l'Intérieur, constater que certaines informations ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique et qu'il y a lieu, en conséquence de les communiquer au requérant.

En pratique, trois situations peuvent se présenter :

1) Si les renseignements généraux ne détiennent aucune information nominative concernant un requérant, la CNIL en informe alors ce dernier, en accord avec le ministre de l'Intérieur.

2) Si les renseignements généraux détiennent des informations nominatives concernant un requérant qui ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique, celles-ci lui sont communiquées, en accord avec le ministre de l'Intérieur. Dans l'hypothèse d'une communication totale ou partielle du dossier, le requérant a la possibilité de rédiger une note d'observation ; la Commission transmet au ministre de l'Intérieur cette note d'observation pour demander d'éventuelles suppressions ou mises à jour des données ou qu'elle soit insérée dans le dossier détenu par les services des RG.

3) Si la communication de tout ou partie des informations peut nuire à la sûreté de l'État, la défense et la sécurité publique, le magistrat de la CNIL procède à l'examen du dossier et s'il y a lieu exerce le droit de rectification ou d'effacement des données inexactes ou des données dont la collecte est interdite par la loi. Le président de la CNIL adresse ensuite au requérant une lettre lui indiquant qu'il a été procédé aux vérifications conformément aux termes de l'article 39 de la loi du 6 janvier 1978. Cette lettre mentionne que la procédure administrative est close et indique les voies de recours contentieux qui sont ouvertes au requérant.

Il convient de préciser que, pour les renseignements généraux, les recherches portent à la fois sur le fichier informatique d'indexation et sur le dossier individuel, sur les extraits des dossiers collectifs contenant des données nominatives sur les demandeurs, ainsi que sur les dossiers conservés dans les sections spécialisées de la direction centrale des renseignements généraux.

En outre, lorsqu'un document de synthèse citant des personnes physiques est établi par les services des renseignements généraux, une mention de ce document est faite dans le registre d'indexation des personnes physiques et, si possible, dans les dossiers individuels des personnes concernées.

En 2003, sur les 1 163 saisines reçues à la CNIL, seulement 84 (soit 7 %) concernaient uniquement les fichiers des renseignements généraux. La plupart des saisines visaient plusieurs fichiers.

Bilan des 686 investigations menées en 2003 dans les fichiers des renseignements généraux

	Investigations aux fichiers des RG	% sur le nombre de requérants
Requérants non fichés aux RG	443	65 %
Requérants fichés aux RG	243	35 %
Total	**686**	**100 %**

Sur les 243 requérants fichés, les dossiers ont été communiqués dans les proportions suivantes

	Requérants fichés aux RG	% sur le nombre de fichés aux RG
Dossiers jugés non communicables	26	11 %
Communication refusée par le ministre de l'Intérieur	–	–
Communication acceptée par le ministre de l'Intérieur *Dont :* — communication totale — communication partielle	217 217	89 %
Total	**243**	**100 %**

Il doit être relevé que, de même que les années précédentes, le ministre de l'Intérieur n'a refusé aucune des propositions de communication de dossier faites par les magistrats de la CNIL.

La procédure de communication des dossiers, initialement fixée par un protocole du 12 février 1992 arrêté avec le ministre de l'Intérieur, a fait l'objet d'une circulaire complémentaire du 2 juin 1993. Depuis dette date, la consultation des pièces communicables du dossier s'effectue au siège de la CNIL lorsque les requérants sont domiciliés dans la région Ile-de-France ou lorsque, domiciliés dans une autre région, ils font l'objet d'une fiche dans les services des renseignements généraux de la préfecture de police de Paris. Dans tous les autres cas la communication est organisée au siège de la préfecture du département dans lequel est domicilié le requérant.

Parmi les 217 communications qui ont été effectuées en 2003 :
— 51 ont eu lieu au siège de la CNIL ;
— 166 ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé.

À la suite de ces communications, seuls huit requérants ont adressé une note d'observation qui a été insérée dans le dossier des renseignements généraux les concernant ou qui a donné lieu à des suppressions.

Par ailleurs, il a été procédé à la suppression totale de vingt-deux dossiers et la suppression partielle de cinq dossiers.

Évolution des investigations aux renseignements généraux depuis 1995

Année	1995	1996	1997	1998	1999	2000	2001	2002	2003
Nombre de demandes traitées	197	252	352	282	270	365	576	1 012	686*
Absence de fiche	113	145	213	169	173	261	415	776	443
% sur le total	57 %	58 %	60 %	60 %	64 %	71 %	72 %	76 %	65 %
Nombre de requérants fichés aux RG	84	107	139	113	97	104	161	236	243
% sur le total	43 %	42 %	40 %	40 %	36 %	29 %	28 %	23 %	35 %
Dossiers non communicables	25	33	57	23	15	18	35	36	26
% sur le nombre de fichés	30 %	31 %	41 %	20 %	15 %	17 %	22 %	15 %	11 %
Communication acceptée par le ministre de l'Intérieur	59	74	82	90	82	86	126	200	217
% sur le nombre de fichés	70 %	69 %	59 %	80 %	85 %	83 %	78 %	85 %	89 %
— totale	44	63	75	84	79	85	126	199	217
— partielle	15	11	7	6	3	1	–	1	–

* La baisse du nombre d'investigations auprès des renseignements généraux s'explique en raison du nombre croissant des saisines qui visent plusieurs fichiers et qui nécessitent de plus longues investigations auprès des directions des ministères.

D. Les investigations au système d'information Schengen

Depuis l'entrée en vigueur du décret n° 95-577 du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS, la CNIL a traité 2 454 (dont 599 au cours de l'année 2003) demandes de droit d'accès, conformément à l'article 6 de ce décret et des articles 109 et 114 de la convention Schengen.

Évolution du nombre de demandes de droit d'accès au N-SIS par année

	Nombre	Total cumulé
1995	22	22
1996	20	42
1997	21	63
1998	78	141
1999	359	500
2000	397	897
2001	297	1 194
2002	661	1 855
2003	599	2 454

Parmi les 2 454 demandes de droit d'accès indirect au système d'information Schengen, 747 personnes étaient signalées.

Ces 747 signalements proviennent par ordre décroissant des pays suivants

Pays signalant	Nombre de signalements	% par rapport au nombre de signalements
Allemagne	335	44,5 %
France	280	37,0 %
Italie	82	11,0 %
Espagne	29	3,5 %
Grèce	12	2,0 %
Pays-Bas	5	1,0 %
Belgique	2	0,5 %
Autriche	2	0,5 %
Total	**747**	**100 %**

Suite aux démarches entreprises par la CNIL, 308 signalements ont été supprimés du N-SIS (soit 41 %) dont 233 par l'Allemagne, 51 par la France, 13 par l'Italie, 6 par l'Espagne, 3 par les Pays-Bas, 1 par la Belgique, 1 par la Grèce.

Dès lors qu'aucun signalement n'est enregistré dans le système d'information Schengen et que le requérant qui s'est vu refuser la délivrance d'un visa par le ministère des Affaires étrangères n'est pas un ressortissant de l'espace Schengen, c'est-à-dire de la nationalité de l'un des pays ayant ratifié la convention de Schengen, la CNIL poursuit ses investigations en saisissant le ministère des Affaires étrangères afin de connaître le motif de refus de visa et en particulier l'inscription éventuelle du requérant dans un fichier d'attention.

Ces fichiers gérés par le ministère des Affaires étrangères et en particulier par les postes consulaires sont désormais intégrés dans le nouveau système informatique de délivrance des visas (RMV2), créé par un arrêté du 22 août 2001 pris après avis favorable de la CNIL.

Aux termes de l'article 6 de cet arrêté, le droit d'accès aux informations contenues dans le RMV2 est mixte. Ainsi, les informations enregistrées lors de la demande de visa bénéficient d'un accès direct qui peut être exercé auprès du consulat ou de l'ambassade où la demande a été déposée. En revanche les informations figurant dans les fichiers d'attention (fichier central comme fichiers locaux), susceptibles de porter atteinte à la sûreté de l'État, la défense et la sécurité publique, font l'objet d'un droit d'accès indirect.

À la demande de la CNIL, le ministère des Affaires étrangères s'est engagé à prendre toutes mesures de nature à faciliter l'exercice de ce droit et à permettre aux commissaires en charge du droit d'accès indirect de vérifier le contenu des fichiers d'attention. Cette procédure n'a pas encore pu être mise en œuvre.

Chapitre 2

LE DROIT À LA TRANQUILLITÉ

« Ma boîte à lettres est pleine sans que j'ai rien demandé : comment l'éviter ? » La prospection commerciale a toujours constitué une source de plaintes importantes à la CNIL. Désormais, les campagnes massives de fax et de messages électroniques ont pris la relève et suscitent des réactions de plus en plus violentes des intéressés qui se sentent harcelés et supportent mal ce débordement dans leur sphère privée. S'il est rare que le marketing porte atteinte à l'identité humaine, aux droits de l'homme, aux libertés individuelles ou publiques visés par l'article premier de la loi du 6 janvier 1978, il touche de plein fouet la vie privée, à laquelle l'informatique ne doit pas porter atteinte. Une composante majeure du respect de la vie privée s'affirme au travers d'un droit à la tranquillité, énoncé par plusieurs directives européennes et décliné par le droit français, tant pour le fax que pour le publipostage électronique non sollicité ou *Spam*. Il consiste à renforcer les droits des personnes physiques puisque le principe posé est celui du droit de consentir aux sollicitations par fax ou messages électroniques et non plus seulement de s'y opposer. C'est la consécration du *Opt In* sur l'*Opt Out*.

La CNIL a logiquement tiré les conséquences d'un renforcement des droits des personnes en menant une politique offensive de dénonciations au parquet, accompagnée d'une action de sensibilisation des procureurs concernés. Il lui paraît essentiel d'obtenir des condamnations de sociétés menant des opérations illégales de prospection directe, qu'il s'agisse d'utilisation d'annuaires d'anciens élèves, d'envois de fax ou des fameux *Spams*, qui focalisent désormais l'attention des pouvoirs publics ainsi que de la Commission européenne, et qui sont l'occasion de nombreux échanges au plan international. Ces condamnations permettraient de faire cesser le sentiment d'impunité des sociétés ou individus recourant à ces pratiques. Dans un second temps, s'agissant du *Spam*, il faudra développer des mécanismes de coopération internationale puisque, faut-il le rappeler, l'immense majorité de ces messages provient d'outre-atlantique.

I. ÊTRE OU NE PAS ÊTRE… DANS L'ANNUAIRE

Les annuaires sont un sujet important de la protection des données à caractère personnel puisque leur vocation est précisément de diffuser des informations sur les personnes qui y sont inscrites. La Commission avait déjà énoncé, dans sa recommandation du 8 juillet 1997, les règles devant s'appliquer aux annuaires téléphoniques. Le décret du 1er août 2003, en permettant l'édition d'annuaires universels ou la fourniture de services universels de renseignements, réactualise cette problématique. Par ailleurs, sur ce sujet, l'année 2003 aura permis à la Commission, saisie de plaintes, de rappeler les conditions d'utilisation au regard de la loi « informatique et libertés » des données présentes dans des annuaires spécifiques.

A. Le décret du 1er août 2003 relatif aux annuaires universels

Le 6 août 2003, est paru au *Journal officiel* le décret organisant le marché des annuaires et services de renseignements téléphoniques qui comprennent désormais les abonnés à la téléphonie mobile et les abonnés à la téléphonie fixe dont l'opérateur est autre que France Télécom. Le nouveau schéma pose le principe de la libre concurrence dans l'édition d'annuaires universels ou de la fourniture de services universels de renseignements téléphoniques et impose à chacun des opérateurs de télécommunications de fournir la liste de ses abonnés à tout éditeur d'annuaire universel ou fournisseur de service universel de renseignements téléphoniques. La loi du 31 décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom a supprimé l'obligation faite par le décret à France Télécom d'éditer un annuaire universel sous forme imprimée et électronique et de fournir un service universel de renseignement pour y substituer un mécanisme de désignation par le ministre chargé des Télécommunications parmi les opérateurs à l'issue d'appels à candidature.

Sous réserve de l'exercice du droit d'opposition par les personnes concernées, les listes d'abonnés ou d'utilisateurs transmises par les opérateurs sont constituées des noms, prénoms et, le cas échéant, des raisons sociales ou dénominations sociales, adresses et numéros de téléphone, des données relatives aux autres utilisateurs d'une ligne fixe si ces derniers en font la demande et, éventuellement, des professions ou activité des personnes.

Surtout, ce décret précise les droits reconnus aux utilisateurs quant à la protection des données à caractère personnel les concernant.

Afin de permettre une application aussi rapide que possible et une compréhension uniforme de certaines des dispositions du décret, la Commission a conduit un groupe de travail comprenant les représentants des opérateurs téléphoniques et les représentants de l'autorité de régulation des télécommunications (ART). Ce groupe de travail a permis de dégager des solutions favorisant une application cohérente de ce décret.

Toutefois, la modification du cadre législatif a retardé la mise en œuvre de ce décret.

Rappelons qu'à l'occasion de son avis sur le projet de décret qui lui était soumis en 2002, la CNIL avait estimé à propos des abonnés à la téléphonie *« qu'il serait plus conforme à l'esprit de protection des données personnelles et de la vie privée des personnes concernées de retenir un dispositif prévoyant que seules les personnes qui en auraient manifesté expressément la volonté puissent être inscrites dans un annuaire ou voir leur numéro de téléphone communiqué par un service de renseignements »* (délibération n° 02-014 du 14 mars 2002). Si cette solution ne devait pas être choisie, la CNIL préconisait la gratuité de la liste rouge.

Le gouvernement n'a pas, lors de la rédaction du décret, retenu le principe du consentement puisque le décret du 1er août 2003 prévoit un mécanisme d'opposition à faire valoir dans un délai de six mois une fois l'abonné informé par son opérateur et instaure le principe de la gratuité de la liste rouge faisant droit, ici, à l'une des « positions historiques » de la CNIL.

Néanmoins, face aux risques d'un basculement trop brutal dans les annuaires universels d'une majorité d'abonnés qui, par inadvertance ou par ignorance, n'auraient pas exercé leurs droits d'opposition, l'Assemblée nationale a voté une disposition qui renverse le choix effectué par le décret pour privilégier la position de l'*Opt In* défendue par la CNIL dès 2002 au profit des abonnés à la téléphonie mobile. Cette disposition a été introduite lors de la discussion du projet de loi relatif aux communications électroniques qui réorganise le Code des postes et télécommunications pour créer, notamment, une section relative à la « Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques » et une section relative aux « Annuaires et services de renseignement ».

C'est dans le cadre de cette dernière section qu'un amendement a été adopté qui précise : *« Les abonnés à la téléphonie mobile doivent exprimer leur consentement préalable à ce que les données à caractère personnel les concernant figurent dans les listes d'abonnés ou d'utilisateurs établies par leur opérateur »*. Si cette disposition était définitivement adoptée, elle devrait entraîner une modification substantielle du décret du 1er août 2003.

B. L'utilisation abusive d'annuaires dénoncée

La Commission avait été saisie, au cours de l'année 2002, de deux plaintes concernant l'utilisation par des sociétés de recrutement ou de services financiers d'annuaires d'anciens élèves de grandes écoles, sans que ces sociétés puissent se prévaloir d'aucun accord avec les associations d'anciens élèves dont elles utilisent l'annuaire. Ce faisant, ces sociétés étaient amenées à collecter des données d'élèves ayant pu, lors de leur inscription dans l'annuaire de leur école, exprimer leur opposition à voir les données à caractère personnel les concernant traitées par des tiers. La Commission avait alors considéré cette pratique comme une collecte déloyale au sens de l'article 25 de la loi du 6 janvier 1978 (*cf.* 23e rapport annuel, p. 64).

Suite à l'instruction de ces saisines, la Commission avait décidé, d'une part, d'adresser un avertissement à l'une de ces sociétés en se fondant sur la collecte déloyale d'informations et sur le silence gardé par cette société malgré de nombreuses relances et, d'autre part, de mettre en demeure l'autre société de se conformer aux dispositions de la loi du 6 janvier 1978.

La société avertie s'est alors engagée à ne plus démarcher les anciens élèves de l'école à l'origine de la saisine et, d'une manière générale, à informer les écoles ou associations d'anciens élèves, lors de l'acquisition des annuaires qu'elles éditent, de l'utilisation à des fins de prospection commerciale qui en sera faite afin de respecter les droits des personnes qui y sont inscrites. La Commission avait, dès lors, procédé à la clôture de la saisine.

La seconde société, quant à elle, contestait la position de la Commission en arguant notamment du fait qu'elle avait contacté l'ensemble des personnes figurant dans sa base de données afin de leur permettre d'exercer leurs droits d'opposition ou de modification. À aucun moment, elle ne s'est cependant engagée à modifier sa méthode de collecte.

En avril 2003, la Commission a alors décidé d'adresser un ultime courrier à cette société l'invitant fermement à régulariser sa situation actuelle — au regard du mode de collecte initiale — en apportant dans un délai de quinze jours, les éléments précis et probants relatifs aux conditions de réalisation de l'opération relative au recueil du consentement de toutes les personnes dont la société traite les données. En parallèle, la Commission exigeait de cette société le respect du droit des personnes dont elle envisagerait, à l'avenir, de traiter les données.

Face au silence de la société mise en cause, la Commission a estimé devoir faire application de l'article 21-4 de la loi du 6 janvier 1978 en dénonçant au parquet sur le fondement des articles 43 de la loi du 6 janvier 1978 et 226-18 du Code pénal la société AlinéA.

II. FAX INDÉSIRABLES

Nombre de plaintes adressées à la Commission dans le secteur du marketing direct en 2003, comme les années précédentes, se rapportent encore à la prospection par voie de télécopie, car ce mode de prospection est très intrusif pour les personnes démarchées. Mais désormais, la CNIL n'est plus désarmée. L'évolution récente du droit applicable à la prospection par voie de télécopie ainsi que les nombreuses plaintes dont elle a été saisie en 2003 ont conduit la Commission à porter huit affaires devant la justice.

A. Le droit applicable à la prospection par voie de télécopie

Les ordonnances des 25 juillet et 23 août 2001, qui ont transposé en droit français plusieurs directives européennes [1], ont posé un principe simple : la prospection directe par télécopie est interdite en France (comme dans l'ensemble des États membres de l'Union européenne) sauf à l'égard des personnes qui auraient spécialement exprimé leur consentement à être ainsi démarchées (nouvel article L. 33-4-1 du Code des postes et télécommunications et nouvel article L. 121-20-5 du Code de la consommation).

S'agissant des sanctions relatives au non-respect de ce principe, il aura fallu attendre la publication au *Journal officiel* du 6 août 2003 du décret n° 2003-752 du 1er août 2003, relatif à l'annuaire universel et aux services universels de renseignements. Ce décret prévoit en effet que le fait d'adresser une télécopie à caractère publicitaire à une personne physique qui n'a pas exprimé son consentement à la recevoir est puni de l'amende prévue pour les contraventions de la quatrième classe (750 euros par télécopie).

Le décret du 1er août 2003 a ainsi modifié l'article R. 10-1 du Code des postes et télécommunications, dont l'alinéa 2 prévoit désormais que *« la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 est punie pour chaque communication de l'amende prévue pour les contraventions de la quatrième classe ».*

Enfin, il convient de souligner que l'article 12 du projet de loi relatif à la confiance dans l'économie numérique, adopté en deuxième lecture par l'Assemblée nationale le 8 janvier 2004, modifie l'article L. 33-4-1 du Code des postes et télécommunications. Cet article interdit *« la prospection directe au moyen d'automates d'appel ou de télécopieurs* [...] *utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen ».*

B. Le bilan des plaintes pour l'année 2003

Dans les deux tiers des cas, les personnes prospectées par voie de télécopie qui saisissent la CNIL sont des personnes morales (des sociétés privées, des associations, des collectivités locales...). Ces réclamations permettent certes à la CNIL de disposer d'une « photographie » de la situation dans le domaine du marketing direct, toutefois la Commission ne peut que se déclarer incompétente s'agissant de personnes morales.

En revanche, lorsqu'une personne physique reçoit des télécopies publicitaires sans avoir exprimé son consentement préalable à les recevoir, la CNIL est compétente pour agir. Ces plaignants, personnes physiques, saisissent la CNIL en lui

1 Directive 97/66 du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et directive 97/7 du 20 mai 1997 concernant la protection des consommateurs en matière de contrat à distance.

adressant les télécopies publicitaires qu'elles reçoivent chaque jour, parfois même la nuit [1].

À quelques exceptions près, les personnes physiques sollicitées par voie de télécopie le sont dans le cadre de leur activité professionnelle : ce sont des artisans, des gérants d'entreprises, des médecins, des avocats, des pharmaciens, des agriculteurs, des prêtres, des trésoriers d'associations, des proviseurs de lycée… qui manifestent leur indignation face à l'intrusion dans leur activité professionnelle de ce mode de prospection. Des médecins, par exemple, témoignent de leur impossibilité à recevoir les résultats d'analyses médicales de leurs patients par télécopie, leur télécopieur étant occupé par la réception de publicités. Les artisans, quant à eux, font valoir l'impossibilité d'utiliser leur télécopieur, outil de travail quotidien, également constamment occupé. Enfin, tous s'insurgent du coût du papier et de l'encre que ce mode de prospection fait peser sur eux.

L'année 2002 avait été marquée par un nombre très élevé de plaintes adressées à la CNIL par des personnes, morales et physiques, qui recevaient des télécopies non sollicitées à caractère publicitaire (2 298 plaintes). En 2003, ce chiffre a considérablement baissé (-69 %) puisque la Commission a reçu 708 plaintes. Cette baisse, dont on ne peut que se réjouir, s'explique, notamment, par le fait que, dès l'adoption des ordonnances de l'été 2001, et sans attendre que le décret d'application prévoyant les sanctions pénales soit pris par le Gouvernement, la CNIL a adressé de très nombreux courriers aux sociétés émettrices de télécopies publicitaires afin de les enjoindre de mettre un terme à leurs pratiques de marketing par télécopie dans la mesure où elles seraient contraires au principe posé par les ordonnances de 2001.

La Commission a ainsi reçu des réponses de sociétés qui l'informaient, alors que le décret du 1er août 2003 n'était pas publié, de leur décision de cesser ces pratiques.

C. Huit affaires portées devant la justice

Depuis le 6 août 2003, date de publication du décret du 1er août 2003 au *Journal officiel*, les services de la Commission ont analysé chacune des plaintes qui lui ont été adressées par des personnes physiques et ont ainsi pu identifier dix-neuf sociétés les plus souvent mises en cause. Il s'agit donc de sociétés qui, malgré l'interdiction pénalement sanctionnée, persistent à adresser des télécopies publicitaires sans avoir préalablement recueilli le consentement de ces personnes.

Si ces sociétés offrent aux destinataires de leurs télécopies publicitaires la possibilité de s'opposer *a posteriori*, soit en leur proposant la radiation de leurs fichiers de leur numéro de télécopieur, soit en leur proposant de s'inscrire sur une « liste d'opposition », de telles pratiques sont aujourd'hui sans fondement pour les personnes physiques, le législateur ayant opté pour le recueil de leur consentement.

1 On peut observer que les plaintes, qu'elles proviennent de personnes morales ou de personnes physiques, sont généralement dirigées contre les mêmes sociétés.

De surcroît, on observera que les modalités d'exercice de ce droit d'opposition sont coûteuses, complexes et rarement efficaces. En effet, les personnes démarchées sont généralement informées par le biais d'une mention figurant sur la télécopie qu'elles peuvent s'opposer à recevoir de nouvelles télécopies en appelant un numéro de téléphone surtaxé (08…), généralement tarifé 0,34 euro la minute. Les personnes qui saisissent la CNIL indiquent, dans leur très grande majorité, qu'elles n'ont pas exercé leur droit d'opposition du fait de ce caractère payant, qu'elles jugent très excessif.

Les dix-neuf sociétés « identifiées » par la Commission ont reçu un courrier leur rappelant la réglementation en vigueur et leur demandant de mettre un terme aux opérations de prospection par voie de télécopie à destination de personnes physiques qui n'ont pas au préalable exprimé leur consentement à être ainsi démarchées.

Huit sociétés n'ont apporté aucune réponse aux demandes de la Commission.

Aussi, lors de sa séance plénière du 9 décembre 2003, la CNIL a adopté huit délibérations portant dénonciation aux parquets compétents du fait, pour ces huit sociétés, d'avoir adressé des télécopies à caractère publicitaire à des personnes physiques qui n'avaient pas au préalable consenti à être ainsi démarchées, fait susceptible de constituer l'infraction visée par l'article R. 10-1 modifié du Code des postes et télécommunications.

III. FACE AU *SPAM*

L'opération « Boîte à *Spams* » menée par la CNIL à l'été 2002 (*cf.* 22e rapport annuel, p. 45) a clairement démontré qu'il n'existait pas de réponse unique pour endiguer la pratique du *spamming*. Combattre efficacement le *Spam* suppose la mise en œuvre d'une série d'actions à plusieurs niveaux : une application effective d'une législation « anti-*Spam* », une politique de sensibilisation des internautes, le développement de solutions techniques, l'adoption de codes de bonne conduite et une forte coopération internationale.

A. L'intervention de la loi

1. LA SITUATION EN FRANCE : LE PROJET DE LOI POUR LA CONFIANCE DANS L'ÉCONOMIE NUMÉRIQUE

Ce projet de loi assure la transposition de certaines dispositions de la directive européenne du 12 juillet 2002 « Vie privée et communications électroniques » [1] qui subordonnent l'utilisation de courriers électroniques dans les opérations de prospection directe au consentement préalable des personnes concernées.

1 Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

En effet, au sein de l'Union européenne, le cadre juridique applicable à la prospection par voie électronique est fixé par la directive du 12 juillet 2002 dont la date limite de transposition a été fixée au 31 octobre 2003. Les États-membres ayant transposé cette directive en 2003 sont la Belgique (loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information complétée par un arrêté royal du 4 avril 2003 visant à réglementer l'envoi de publicités par courrier électronique), le Danemark en modifiant en juin 2003 l'article 6 de la loi sur les pratiques commerciales du 17 juillet 2000, l'Irlande (règlement du 6 novembre 2003), l'Italie avec l'adoption en décembre 2003 du Nouveau Code de protection des données (section 130 du Code), l'Espagne avec la loi sur les télécommunications de novembre 2003 modifiant la loi sur la société de l'information du 27 juin 2002 et le Royaume-Uni avec l'entrée en vigueur le 11 décembre 2003 de *« The Privacy and Electronic Communications Regulations »*.

a) Points en discussion

La CNIL, saisie pour avis de l'avant-projet de loi [1], a régulièrement fait valoir sa position sur ce texte lors d'auditions organisées par chacune des assemblées [2] (*cf.* 23e rapport annuel, p. 71 et p. 178). Il n'est pas utile de revenir sur tous les aspects de cette position qui a été exposée dans le précédent rapport annuel. On se bornera à quelques points qui ont fait débat entre les deux assemblées au cours des deux lectures intervenues en 2003 et de celle faite à l'Assemblée nationale au tout début de 2004.

Ainsi en est-il de la question de la nécessité ou non de définir ce qu'est le consentement à recevoir des messages de prospection directe. Comme l'avait préconisé la CNIL, l'Assemblée nationale a réintroduit la définition du consentement préalable qui avait été supprimée par le Sénat en reprenant la définition issue de la directive de l'article 2 de la directive du 24 octobre 1995 mais en l'adaptant au cadre des opérations de prospection directe. Selon le nouvel alinéa 2 de l'article L. 33-4-1 du Code des postes et des télécommunications, *« on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe »*. La CNIL a notamment fait valoir en faveur du maintien de cette définition que se voyant confier le soin d'instruire les plaintes liées au non-respect du nouveau dispositif, il lui paraissait nécessaire de disposer d'un texte non susceptible de faire l'objet d'interprétations qui seraient de nature à compliquer sa tâche d'instruction des plaintes.

S'agissant de l'instauration d'un régime transitoire ayant pour objet de ne pas rendre inutilisables les fichiers existants, la Commission relève avec satisfaction que l'Assemblée nationale n'a pas retenu un amendement prévoyant un mécanisme de consentement présumé. Ainsi, dans les six mois suivant la date de publication de la loi, les informations relatives aux clients ou prospects pourront être utilisées afin

1 Délibération n° 02-093 du 28 novembre 2002 portant avis sur l'avant projet de loi sur l'économie numérique.

2 Adoption du projet de loi en première lecture par l'Assemblée nationale le 26 février 2003 et par le Sénat le 25 juin 2003.

d'offrir à ces derniers la faculté d'exprimer leur consentement. À l'expiration de ce délai, ces personnes sont présumées avoir refusé l'utilisation ultérieure de leurs coordonnées personnelles si elles n'ont pas manifesté expressément leur consentement à celle-ci. Ce régime transitoire vise uniquement les cas dans lesquels le consentement de la personne est requis. La précision apportée sur le fait que le consentement doit être explicitement donné, le silence des personnes valant refus, apparaît pleinement satisfaisant pour la CNIL.

En outre, le projet de loi prévoit que la CNIL et la DGCCRF (direction générale de la concurrence, de la consommation et de la répression des fraudes) seront habilitées à intervenir pour assurer le respect de la législation relative à la publicité par voie électronique. Sur ce point, un travail de concertation a été engagé avec la DGGCRF visant à définir des modalités concrètes de cette coopération.

Il est aussi précisé que l'intervention de la CNIL est expressément limitée aux plaintes émanant des personnes physiques, et que la réception de plaintes, par voie électronique, de personnes physiques victimes de publipostage électronique non sollicité n'est plus une obligation mais une simple faculté offerte à la Commission.

La CNIL relève également que dans le texte adopté par l'Assemblée nationale le recueil du consentement préalable est exigé uniquement pour les opérations de prospection de nature commerciale. Cette évolution ne fait pas obstacle à l'application des principes généraux régissant la protection des données aux opérations de prospection qui ne seraient pas de nature commerciale, comme le démarchage politique, associatif, religieux ou caritatif (par exemple, la collecte de dons).

b) Personnes morales, personnes physiques

S'agissant de la question relative à l'application du principe du consentement préalable aux personnes morales, la CNIL s'était félicitée de la position retenue dans l'avant-projet de loi qui posait le principe du consentement préalable au bénéfice des personnes morales et des personnes physiques. Ce choix permettait en effet d'éviter la délicate opération qui consisterait à distinguer les adresses de courriers électroniques des personnes physiques de celles des personnes morales. Cette position n'a pas été suivie par les parlementaires. L'Assemblée nationale, qui a d'ailleurs abandonné le critère fondé sur l'inscription ou non au Registre du commerce et des sociétés concernant le courrier électronique, a exclu les personnes morales, quel que soit le vecteur de prospection (automates d'appel, télécopie, courrier électronique), du bénéfice du consentement préalable. Elle a ainsi modifié le schéma issu des ordonnances de juillet et août 2001 qui prévoyait le principe du consentement préalable au bénéfice des personnes physiques ou morales en matière de prospection par automates d'appel et télécopie.

Concernant la question de la distinction entre les adresses de courriers électroniques utilisées par des personnes physiques ou morales, la CNIL a, lors de sa séance plénière du 1er juillet 2003, dégagé la position suivante :

— En présence d'adresse « impersonnelles », de type info@..., contact@..., commande@...., service-clientèle@... qui seraient manifestement les coordonnées de

personnes morales, le principe du consentement préalable ne s'applique pas, pas plus que les dispositions de la loi du 6 janvier 1978.

La CNIL se déclare ainsi systématiquement incompétente lorsqu'elle est saisie de plaintes relatives à la réception de courriers électroniques qui sont envoyés à des adresses appartenant à cette catégorie.

— En présence d'une adresse de courrier électronique attribuée par une personne morale à ses employés (adresses de courriels professionnelles) comme par exemple (nom.prenom@nomdedomainedelasociété.fr), le régime du consentement préalable s'applique dans la mesure où ces adresses permettent l'identification de personnes physiques. L'utilisation à des fins privées ou professionnelles de cette adresse importe peu.

La CNIL souhaite que le décret pris pour l'application de la loi reprenne cette interprétation sans avoir à attendre que la jurisprudence règle cette question.

Cette position qui est notamment celle de la législation belge 24 est aussi celle retenue au sein du groupe article 29 dans son avis interprétatif adopté le 27 février 2004 sur les communications de prospection directe non sollicitée selon l'article 13 de la directive 2002/58/CE [1]. Le groupe article 29 a en effet souhaité contribuer à une application uniforme des mesures nationales car le nouveau régime juridique applicable à la prospection par voie électronique soulève incontestablement des difficultés d'interprétation.

2. DROIT COMPARÉ : LE *CAN-SPAM ACT*

L'Union européenne n'a pas été la première à déclencher une lutte active contre le fléau du *Spam* en adoptant une législation spécifique sur le sujet. Ainsi, à titre d'exemple, en 2002 le Japon et la Corée du Sud avaient déjà adopté des lois sur le sujet ; l'Afrique du Sud s'était également dotée d'une loi sur les communications et les transactions électroniques à l'été 2002, traitant du *Spam* dans un de ses chapitres. Le mouvement s'est poursuivi en 2003, en particulier dans des pays d'Amérique latine où des projets de lois sur le sujet ont été déposés auprès des parlements du Brésil, d'Argentine et du Chili. En Australie, le *Spam Bill*, voté le 2 décembre 2003, introduit un régime de consentement préalable pour les messages électroniques commerciaux. Mais indéniablement, l'événement législatif majeur dans le domaine de la lutte contre le *Spam* en 2003 a été l'adoption par le Congrès américain du « *Controlling the Assault of Non-Solicited Pornography and Marketing Act* », dit *Can-Spam Act*, dont les dispositions sont rentrées en application au 1er janvier 2004.

a) L'esprit de la loi américaine

L'activité parlementaire américaine précédant l'adoption du *Can-Spam Act* avait été fournie : outre le fait que de nombreux États avaient d'ores et déjà adopté ou étaient sur le point d'adopter des lois pour leur propre juridiction, de nombreux

1 http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_fr.pdf

projets de loi avaient été déposés au Congrès qui, selon les parlementaires dont elles émanaient, favorisaient soit les intérêts des professionnels de la communication électronique et du marketing direct, soit les intérêts des utilisateurs d'internet.

Ces initiatives procédaient d'une volonté de répondre aux préoccupations des entreprises et des citoyens américains, excédés par le *Spam* et les envois massifs de messages électroniques à connotation jugée immorale. Pour ne mentionner que deux données chiffrées, il a été notamment estimé qu'en 2003, 50 % du trafic de courriers électroniques aux États-Unis n'était constitué que de l'envoi de *Spams* (cette proportion ayant tendance à augmenter), et qu'en 2002, le coût engendré pour les entreprises américaines par les prospections non sollicitées reçus par leurs salariés s'élevait à 9 milliards de dollars. Quant aux fournisseurs d'accès, ils dénoncent unanimement les coûts subis du fait de l'acquisition d'équipements de filtrage, de la saturation de leur bande passante, de la nécessité du recrutement de personnels spécialisés dans la lutte contre les *Spams* et de personnels gérant les réclamations des abonnés, etc.

La démarche du législateur fédéral américain, dans sa volonté de réguler le *Spam*, a été fondamentalement différente de celle du législateur européen. Ainsi, contrairement à la directive « communications électroniques », le *Can-Spam Act* n'évoque à aucun moment des questions de protection des données personnelles ou de *Privacy*. L'objectif premier de la loi n'est pas tant de protéger les personnes recevant des messages non-sollicités que de sanctionner les sociétés responsables de « pratiques déloyales ou trompeuses » *(Unfair or Deceptive Practices)* ayant, par exemple, eu recours à des données de transmission fausses ou de nature à induire en erreur ou ayant envoyé un message électronique sans adresse de réponse valide. De tels actes, qualifiés de « pratiques déloyales ou trompeuses » et constituant comme tels des infractions à la loi sur le commerce fédéral, sont punis par de lourdes peines d'amende, voire d'emprisonnement. Ainsi, les entreprises sont sanctionnées dans la mesure où elles pénalisent celles qui ont un comportement « convenable » et où, par conséquent, leur attitude est néfaste au commerce fédéral.

Cette attitude centrée sur les questions de commerce et (indirectement) de concurrence, et non sur les questions de protection des personnes, a eu un effet majeur dans la loi : elle consacre le principe d'*Opt Out* pour l'envoi de messages commerciaux non sollicités et non un principe d'*Opt In*. Ce choix, contraire à celui effectué dans la directive « communications électroniques », avantage bien évidemment les annonceurs et professionnels du marketing direct, et a été de ce fait énormément contesté par les associations de défense des utilisateurs d'Internet. Dès sa promulgation, la loi a été ainsi brocardée comme le *You Can-Spam Act*, laissant entendre que loin de lutter contre le *Spam*, cette loi ne faisait que légaliser une pratique rejetée par la grande majorité des Américains. De fait, il est certain que la volonté politique de lutte contre le *Spam* avait dû ménager les intérêts de l'industrie de la communication électronique que la très puissante Association du marketing direct (DMA) s'était efficacement chargée de faire valoir durant tout le processus législatif.

Autre élément largement critiqué de la loi, le *Can-Spam Act* prévoit que ses dispositions « préemptent » celles des lois anti-*Spam* des États, c'est-à-dire que celles-ci se trouvent privées d'effet depuis l'entrée en vigueur de la loi fédérale. Cette disposition inactive de ce fait les législations anti-*Spam* des États, et particulièrement celles qui étaient plus favorables aux utilisateurs d'internet. Ainsi, la loi qui était sur le point d'être passée en Californie consacrait un principe d'*Opt In*, imposant aux professionnels du marketing de prouver qu'ils avaient obtenu le « consentement direct » des internautes à l'envoi de communications commerciales. Du fait de cette disposition de préemption de la loi fédérale, ce projet est caduc depuis le 1er janvier 2004.

b) Grandes lignes du nouveau dispositif

Le premier volet de la loi *CAN-SPAM* édicte une interdiction générale d'avoir recours à des messages électroniques commerciaux de nature déloyale ou trompeuse *(Prohibition Against Predatory or Abusive Commercial e-mail)*, et attache à cette interdiction de lourdes sanctions pénales. Il s'agit ici de sanctionner les expéditeurs de messages dont le contenu serait illégal.

Le second volet, intitulé « autre protection des utilisateurs de messages électroniques commerciaux », aborde les cas de figure dans lesquels l'envoi de *Spam* serait illégal pour des raisons autres que le contenu des messages. Il prévoit à ce titre :
— une interdiction absolue d'envoi de messages contenant des informations de transmission fausses ou de nature à induire en erreur ou de messages aux intitulés trompeurs ;
— une obligation d'inclusion d'une adresse de réponse valide ou d'un mécanisme comparable, permettant aux destinataires des messages de s'opposer à l'envoi de messages ultérieurs, et dont la validité doit être acquise durant au moins trente jours suivant l'envoi des messages ;
— une interdiction d'envoi de messages commerciaux après que son destinataire a exercé son droit d'opposition (principe d'*Opt Out*) ;
— une obligation d'inclusion dans le message de mentions indiquant sa nature commerciale ou publicitaire, une mention claire du droit d'opposition des personnes et de la manière dont exercer ce droit en ligne, ainsi que l'adresse postale valide de l'expéditeur ;
— une obligation de prévenir le destinataire dans l'en-tête du message quand son contenu est « orienté sexuellement ».

Le recours à certaines techniques informatiques est également interdit, quand celles-ci peuvent servir de « support » à l'envoi de *Spam*. Ainsi, la loi prévoit qu'il est illégal d'envoyer des messages électroniques à des personnes dont les adresses ont été collectées de manière massive sur des sites web (*email Harvesting*), à la condition toutefois que ces sites web comportent une mention indiquant que leur propriétaire n'autorise pas la vente ou le transfert des adresses figurant sur le site pour l'envoi de messages électroniques.

Une telle construction est juridiquement inutile en Europe, du fait de la condition préalable du recueil du consentement de l'internaute à l'envoi de messages commerciaux. Cependant, ces modes de collecte automatique d'adresses électroniques

ne connaissent pas de frontières et ne feront pas de différence entre un site français et un site américain. Dès lors, il en résulte que les sites européens devront probablement faire figurer les mentions obligatoires exigées par la loi *Can-Spam* sur leur page d'accueil, afin d'éviter que les coordonnées électroniques qui y figurent ne soient reprises par un « *email Harvester* » américain... Ainsi, cette loi américaine, qui n'avait pourtant pas vocation à avoir des effets extraterritoriaux, les aura *de facto* pour des raisons techniques.

Par ailleurs, le recours à des « adresses forgées », obtenues par la génération automatique d'adresses électroniques par ordinateur, est également interdit, ainsi que le système de génération automatique de comptes mail (sur des messageries gratuites, notamment) ayant pour finalité l'envoi massif de messages illégaux en vertu des autres dispositions de la loi.

En complément des dispositions précédentes, la loi interdit bien évidemment à des annonceurs de recourir aux services de tiers réalisant des opérations d'envoi de messages pour leur compte quand ceux-ci ne respectent pas les dispositions de la nouvelle loi et prévoit de nouvelles sanctions à cet effet.

La loi autorise la *Federal Trade Commission* (FTC), les *Attorneys General* (« AGs ») des États ainsi que les fournisseurs d'accès à internet à engager des poursuites à l'encontre des « spammeurs ». Par contre, les destinataires des messages ne sont pas autorisés à obtenir réparation du préjudice subi. Ce choix, qui a bien entendu attiré de nombreuses critiques, illustre encore une fois que le législateur n'a pas donné priorité à la protection de la personne dans l'élaboration de ce texte. En revanche, les peines prévues sont sévères : les AGs peuvent réclamer le prononcé de sanctions pécuniaires allant jusqu'à 250 dollars par message envoyé (le montant total ne pouvant excéder 2 millions de dollars), tandis que les FAI peuvent réclamer jusqu'à 100 dollars par message envoyé (montant maximum : 1 million de dollars).

D'un avis général, le *Can-Spam Act* ne sera pas simple d'application. Le Comité Internet de l'Association nationale des *Attorneys General* a ainsi considéré que la loi contenait tant de lacunes, d'exceptions et de règles de preuve qu'elle ne protégerait aucunement le consommateur. Plus généralement, la critique a été émise selon laquelle à défaut d'une règle d'*Opt In*, et compte tenu du nombre de messages commerciaux non-sollicités reçus chaque jour par les utilisateurs d'internet aux États-Unis, l'exercice de leur droit d'opposition deviendrait un travail à plein temps !

Dépassant une vision purement nationale, plusieurs commentateurs se sont accordés pour regretter que les législateurs européen et américain n'aient pas adopté des règles similaires de lutte contre le *Spam*, en particulier au regard de la déclaration du Congrès selon lequel « *les problèmes associés à l'augmentation rapide et aux abus de messages électroniques commerciaux non sollicités ne peuvent être réglés par la législation fédérale exclusivement. Le développement et l'adoption d'approches technologiques et la poursuite d'efforts de coopération avec d'autres pays seront également nécessaires* ». [1] Il est évident que si le législateur fédéral américain

1 *Can-Spam Act*, Section 2a), *« Congressional Findings and Policy »*, §12.

avait, comme le législateur européen, validé un principe de consentement préalable à la réception de messages électroniques commerciaux, la coopération internationale visant à lutter contre le *Spam* n'aurait pu que gagner en efficacité, d'autant que, est-il besoin de le rappeler, plus de 80 % des *Spams* reçus par les Européens proviennent des États-Unis !

B. Les nouvelles initiatives contre le *Spam*

Depuis la fin de l'opération « Boîte à *Spams* » menée par la CNIL en 2002, on constate la multiplication des initiatives en matière de lutte contre le *Spam* tant au niveau national ou européen que mondial, compte tenu de la progression exponentielle du phénomène au détriment de tous. Il faut être conscient que désormais la lutte contre le *Spam* représente un enjeu aussi important que la lutte contre les virus.

2. LES INITIATIVES PRISES PAR LA CNIL

Dans la continuité de ses actions précédentes, la CNIL s'est fixée deux orientations principales :

— Prolonger son action pédagogique tant à l'égard des internautes que des professionnels par la mise à jour du module pédagogique « Halte au *Spam* ! » et l'élaboration d'un guide pratique, en concertation avec les professionnels, sur l'application des textes dès que la loi pour la confiance dans l'économie numérique sera votée.

— Accentuer le volet répressif en lançant de nouvelles actions en justice et en favorisant la coopération européenne et internationale.

Il s'avère plus que jamais nécessaire pour les autorités de protection des données ou pour les autres autorités compétentes en matière de *Spam* de faire application des textes législatifs afin d'obtenir des condamnations de « spammeurs » et au travers de quelques cas exemplaires, faire cesser le sentiment d'impunité des sociétés et individus recourant à ces pratiques.

Le *Spam*, comme la CNIL a pu le constater, émane certes à 90 % de pays hors Union européenne mais également de France et d'Europe. Il paraît donc indispensable d'agir aux trois niveaux, national, européen et mondial en collaboration étroite avec d'autres autorités et les professionnels.

a) En France

Des contacts réguliers avec les magistrats des parquets et les services de police spécialisés ont été développés à l'occasion des dénonciations d'octobre 2002 en matière de *Spam*. Par ailleurs, la CNIL s'attache à identifier, grâce aux plaintes reçues et avec l'aide des professionnels, deux ou trois sociétés françaises pratiquant du *Spam* pour les dénoncer au parquet. Elle a également soutenu des actions judiciaires intentées par des fournisseurs d'accès à internet.

b) En Europe

La CNIL a pour objectif d'engager une action coordonnée avec les autorités européennes compétentes pour traiter des réclamations des internautes. Elle envisage même de dénoncer concomitamment des « spammeurs » dans chacun des États concernés et faire usage des pouvoirs de sanction. En Europe, ceci est rendu d'autant plus facile que la direction générale de la société de l'information au sein de la Commission européenne a pris des initiatives pour renforcer cette coopération *(cf. infra)* et que certaines autorités de protection, qui disposent de pouvoirs de sanctions autonomes, ont déjà entamé des actions à l'encontre de « spammeurs ». Ainsi, en Italie, le *Garante* (l'autorité de protection des données italienne) prononce et annonce publiquement chaque semaine des sanctions à l'encontre de « spammeurs » basés en Italie (injonction de cessation d'activité, dommages et intérêts aux plaignants, amendes administratives).

En outre, la CNIL a été saisie, au cours de l'année 2003, de plusieurs cas concrets nécessitant la mise en œuvre d'une coopération européenne. C'est ainsi qu'au printemps 2003, une autorité européenne qui avait mis en place une « Boîte à *Spam* », sur le modèle de celle de la CNIL, a identifié, parmi les courriers électroniques transmis par les internautes, des messages adressés par treize organismes français de divers secteurs d'activités (informatique, finance, commerce, loisirs, etc.). Ces messages ont été transmis à la CNIL qui a, après avoir identifié les expéditeurs, adressé un courrier à chacun d'eux pour faire radier les adresses électroniques des fichiers mais également pour leur rappeler la réglementation en vigueur. La Commission a également été saisie à l'été 2003 d'une plainte par une autre autorité européenne. Le « spammeur » visé dans la plainte a indiqué à la Commission qu'il utilisait un logiciel aspirateur d'adresses de courriers électroniques et la CNIL a finalement obtenu qu'il cesse ces pratiques et procède à la radiation de son fichier de toutes les adresses électroniques collectées par ce moyen déloyal.

Dans un autre sens, la CNIL a transmis à l'un de ses homologues européens plusieurs réclamations d'internautes français qui recevaient des *Spams* financiers émis par un établissement situé sur le territoire de cet homologue. Cet établissement ayant indiqué à la Commission qu'il avait décidé de stopper toute prospection par courrier électronique, la Commission a cependant saisi son homologue afin qu'il vérifie si cette promesse avait été tenue et si les adresses électroniques des plaignants avaient bien été radiées de ses fichiers.

L'expérience acquise sur la base de ces différents cas a permis à la CNIL de dégager quelques principes directeurs afin qu'une procédure de coopération plus efficace soit mise en œuvre, à savoir :
— une indispensable rapidité : les opérations de *Spamming* sont généralement de courte durée et leurs expéditeurs sont très volatils. Dès lors, seule une réaction rapide permettra d'identifier les « spammeurs » et de faire cesser ces pratiques (transmission des plaintes dans le mois ou au maximum deux mois après réception) ;
— une instruction préalable à la transmission à l'autorité du pays d'établissement du « spammeur » afin d'une part de s'assurer qu'il s'agit bien de *Spam* et d'autre part

d'avoir un bon niveau d'indice que l'entreprise est établie dans un autre État membre en réunissant des éléments sur l'origine des messages incriminés ;
— une accumulation de plaintes : sauf cas particuliers, seul le traitement de plaintes en nombre mettant en cause une seule et même société apparaît pertinent, notamment en raison de l'ampleur du phénomène du *Spam*.

c) Dans le monde

Dans un second temps, une action de coopération sera envisagée hors d'Europe, c'est-à-dire là où réside la source principale du *Spam*. La CNIL s'est en effet fixée comme principal objectif d'assainir le marché français avant de poursuivre ses efforts au niveau mondial.

Les grandes lignes d'une coopération au niveau mondial ont toutefois été définies et plus particulièrement en direction des États-Unis qui disposent à présent d'une législation fédérale « anti-*Spam* » avec le *Can-Spam Act* de 2003. La CNIL envisage ainsi de prendre contact avec d'une part les procureurs généraux des États-Unis et d'autre part avec la *Federal Trade Commission* dès lors que le projet de loi en cours de discussion au Sénat américain l'autorisant à échanger des informations avec des autorités étrangères aura été adopté.

Des contacts auprès de fournisseurs d'accès et de messagerie internationaux pourront également être pris afin d'obtenir des éléments d'identification des « spammeurs » américains sévissant en Europe, pour permettre à la CNIL d'étayer un dossier qui pourrait être transmis à la justice dans le cadre d'une nouvelle dénonciation au parquet d'entreprise américaine « spammant » des Français. Les opérateurs américains pourront également relancer des actions judiciaires aux États-Unis en intégrant des éléments d'informations fournis par la CNIL. Trois grands fournisseurs sont concernés : Yahoo ! AOL et Microsoft, tous membres en France de l'Association française des fournisseurs d'accès à internet (AFA).

La mise en œuvre de mécanismes de coopération pourra être l'occasion d'échanger des informations concernant les méthodes d'instruction, les « bonnes pratiques », les technologies utilisées pour identifier les « spammeurs », les modules pédagogiques à destination des internautes et des professionnels, les « cas non résolus » (par exemple, comment la justice nationale traite les *Spams* provenant d'un pays étranger).

2. D'AUTRES INITIATIVES CONVERGENTES

a) Une priorité gouvernementale

Le 10 juillet 2003, le Gouvernement a annoncé à l'occasion du Comité interministériel pour la société de l'information la création d'un groupe de concertation et d'action contre le *Spam* dont l'objectif est de favoriser la concertation entre les acteurs publics et privés de la lutte contre le *Spam* et la coordination de leurs actions, en France comme à l'international. L'animation et le pilotage du groupe de contact ont été confiés à la direction du développement des médias (DDM). Ce groupe a été

officiellement installé le 16 janvier 2004, et a entrepris de mettre en place plusieurs groupes de travail thématiques ainsi que de créer un centre de ressources français sur le *Spam* dont les missions incluront notamment le recueil des plaintes des utilisateurs contre les « spammeurs ». La CNIL assurera le pilotage du groupe de travail « plaintes et sanctions » et participera aux groupes « coopération internationale », « réglementation et auto-réglementation ». La CNIL est également associée aux travaux de pilotage pour la mise en place du centre de ressources.

b) L'action de la Commission européenne

Dans le cadre de la transposition de la directive du 12 juillet 2002 « vie privée et communications électroniques », la Commission européenne a présenté le 22 janvier 2004 une communication portant sur les communications commerciales non sollicitées [1]. Cette action a été lancée en juillet 2003, lors d'une conférence de presse donnée par le commissaire européen chargé des entreprises et de la société de l'information qui a annoncé le renforcement de la coopération internationale, des mesures techniques de lutte (filtres, codes de déontologie) et la sensibilisation des consommateurs et des entreprises.

Plusieurs volets sont en effet envisagés par la Commission européenne parmi lesquels la sensibilisation au problème, avec l'organisation d'ateliers sur le *Spam* pour recenser les mesures prises par les États, les entreprises ou toute autre partie intéressée, contre le *Spam* en vue de discuter des différentes méthodes à employer et contrôler l'application par les États-membres de la législation « anti-*Spam* ».

Enfin, la Commission encourage une large coopération au niveau national, européen et mondial. Ainsi, pour faciliter et coordonner les échanges d'information et les meilleures pratiques en matière de traitement des plaintes, la Commission européenne a créé un groupe en ligne informel sur les communications commerciales non-sollicitées, composé des représentants des administrations nationales compétentes et des autorités chargées de la protection des données, ainsi que des services de la Commission.

c) Un sujet planétaire

Le sommet mondial sur la société de l'information qui s'est tenu à Genève en décembre 2003 a inclus dans son plan d'action la question de la coopération internationale dans la lutte contre le *Spam*, l'OCDE a organisé un atelier sur le *Spam* en février 2004 et la prochaine réunion du dialogue transatlantique des consommateurs sera consacrée à la lutte contre le *Spam*.

1 Cette communication intègre notamment les réponses apportées, par les acteurs publics (dont la CNIL) et privés concernés par le problème du *Spam*, à un questionnaire adressé en janvier 2003 par la Commission européenne sur le suivi pratique de l'approche *Opt In* concernant les communications électroniques, non sollicitées à des fins de prospection directe conformément à la directive 2002/58/CE. La communication est accessible à partir de http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/communic_reports/spam/spam_com_2004_28_fr.pdf

Chapitre 3

LES NOUVELLES TECHNOLOGIES DANS LA SPHÈRE PUBLIQUE

L'intégration des technologies de l'administration dans la gestion et la vie publiques est, à l'évidence, un processus continu. Mais la CNIL ne peut manquer de relever les tournants et les phases d'accélération qui précèdent celles plus lentes et plus discrètes de digestion par l'appareil administratif. Ainsi, la notion d'administration électronique prend, en 2003, un relief particulier quand le Gouvernement lance un programme pluriannuel et ouvre une série de chantiers destinés à tirer tout le parti d'internet dans la simplification administrative. Associée étroitement à la préparation de ce programme, la CNIL n'en garde pas moins sa liberté de jugement pour en apprécier les traductions concrètes dès 2004.

S'agissant des procédés de vote électronique, l'année 2003 a vu émerger les premiers textes réglementant et organisant, avec plus ou moins de rigueur, les nouveaux scrutins à distance.

C'est cependant moins une exigence de facilitation des démarches et actes du citoyen qu'une recherche de l'efficacité qui conduit certaines administrations à mettre en place une circulation de données entre les fichiers publics et les fichiers privés. Si commodes que puissent être de tels échanges, parfois contraints, la CNIL doit en marquer les limites au regard du principe de finalité.

I. L'ADMINISTRATION ÉLECTRONIQUE EN MARCHE

Après plusieurs mois de préparation, le Gouvernement a dévoilé, au début de l'année 2004, son programme de développement de l'administration électro-

nique, pour les quatre années à venir. Baptisé ADELE (administration électronique), ce programme précise, dans un plan stratégique, les décisions prises pour favoriser l'essor de l'administration électronique en France. Un plan d'action décrivant les principaux projets qui seront menés d'ici 2007, a également été établi, projets qui se décomposent eux-mêmes en 140 mesures.

Conçus pour simplifier les démarches administratives des usagers mais aussi, dans une certaine mesure, des entreprises comme des collectivités locales, de nouveaux services devraient donc être déployés, tel celui du numéro unique d'appel pour les renseignements administratifs « 3939 allô service public », actuellement testé en région Rhône-Alpes ou encore le service unique de changement d'adresse, le service personnalisé (monservice-public. fr), susceptible de permettre la gestion de ses dossiers administratifs en ligne et la carte de vie quotidienne, expérimentée prochainement dans plusieurs collectivités locales pour faciliter l'accès aux services publics locaux. Figurent également parmi les projets annoncés, la dématérialisation de l'état civil, la future carte nationale d'identité électronique qui pourrait permettre à ses détenteurs de s'authentifier et de signer électroniquement ou encore les évolutions techniques de la carte VITALE susceptible d'être utilisée comme outil d'identification en dehors du secteur de la santé.

Il s'agit également de multiplier les téléservices, en les rendant faciles d'emploi, accessibles à tous et de plus en plus personnalisés. Ceci devrait se traduire par des mesures de simplifications réglementaires mais aussi par des échanges de données entre administrations.

De tels projets, parce qu'ils peuvent nécessiter de nouveaux traitements de données personnelles, le développement d'interconnexions voire la constitution de bases de données centralisées, appellent, sur le plan de la protection des données à caractère personnel, une vigilance particulière. C'est une des raisons pour lesquelles le secrétaire d'État à la Réforme de l'État a souhaité associer la CNIL aux réflexions et travaux conduits sur le sujet de l'administration électronique tout au long de l'année 2003.

L'administration électronique constitue un domaine d'intervention naturel pour la CNIL. Au fil des ans, celle-ci a été appelée à se prononcer sur de nombreux projets d'envergure préfigurant l'administration électronique de demain, qu'il s'agisse des télédéclarations sociales (NET ENTREPRISES), de la télétransmission des feuilles de soins (SESAM VITALE), de la télédéclaration de revenus, du télérèglement de l'impôt, de la télédéclaration de la TVA ou de l'accès en ligne au compte fiscal simplifié (programme COPERNIC). La Commission a également été consultée sur la demande, par internet, de délivrance de certains extraits du casier judiciaire, et des collectivités locales l'ont saisie de la mise en ligne de certains services tels que l'inscription scolaire, la délivrance d'extraits d'actes de naissance, la prise de rendez-vous avec les services municipaux, voire d'applications de cartes à puce. En 2003, la Commission a eu l'occasion de se prononcer sur d'autres applications d'administration électronique tels l'application « I-prof » développée par le ministère de l'Éducation nationale ou encore la consultation par internet des données cadastrales par les notaires.

A. La position générale de la CNIL

1. REGARD SUR LES LIGNES DIRECTRICES DU PROGRAMME DU GOUVERNEMENT

La CNIL a été amenée à se prononcer en octobre 2003 sur les orientations du programme d'administration électronique du Gouvernement. Elle a, à cette occasion, tenu à souligner l'importance donnée, dans le programme, au nécessaire respect des principes de protection des données à caractère personnel — considéré comme un facteur essentiel de confiance pour l'usager — et pris acte que ses recommandations avaient été prises en considération sur de nombreux points.

La Commission a en outre, rendu, le 27 novembre 2003, un avis sur les dispositions du titre relatif au développement de l'administration électronique, contenues dans un avant-projet de loi habilitant le Gouvernement à simplifier le droit par voie d'ordonnances. Ce texte, qui fait suite à une première loi d'habilitation du 3 juillet 2003, autorise le Gouvernement à fixer par voie d'ordonnance les règles nécessaires pour, notamment, assurer la sécurité et la fiabilité des informations échangées entre les usagers et l'administration et pour permettre aux usagers d'effectuer leurs démarches administratives par voie électronique, mettre à disposition des usagers un dispositif leur permettant de stocker sous forme électronique les données administratives les concernant ainsi qu'un service unique de changement d'adresses.

Dès lors qu'il s'agit de rendre un meilleur service aux usagers de l'administration, de rendre celle-ci plus efficace et plus transparente, de simplifier les démarches tout en garantissant les droits et libertés de chacun, la CNIL est, bien entendu, pleinement favorable au développement de l'administration électronique et encourage toutes les initiatives menées en ce sens. Mais pour assurer le succès de l'administration électronique, il importe que les usagers aient pleinement confiance dans les dispositifs qui leur seront proposés. Or, ainsi que le souligne le plan stratégique, cette confiance repose en particulier sur les garanties qui pourront être offertes aux usagers quant à la protection des données à caractère personnel les concernant.

La CNIL pour sa part, met l'accent sur quatre principes qui sont largement pris en compte par le programme gouvernemental de développement de l'administration électronique :
— le principe de proportionnalité ;
— le principe de transparence ;
— le principe de sécurité graduée ;
— le principe de pluralité des identifiants.

a) Le principe de proportionnalité : simplifier sans multiplier les interconnexions

La CNIL approuve pleinement les projets d'administration électronique, dès lors que, tout en respectant le principe fondamental d'égalité des citoyens devant le service public et en préservant la faculté pour le citoyen de recourir aux autres modes d'intervention auprès de l'administration (accueil physique, téléphone, écrit, bornes

interactives...), ils permettent une réelle simplification des formalités et sont ainsi l'occasion de « repenser », quand cela est nécessaire, l'organisation administrative et de réduire la complexité administrative et non de s'en faire complice, comme la CNIL a pu hélas le constater maintes fois.

La « dimension humaine » des relations usagers-administration devant, en tout état de cause, être préservée, l'administration électronique doit donc s'accompagner d'un effort véritable pour, tout à la fois, favoriser une meilleure compréhension des formalités par les usagers en leur fournissant, sur tous supports disponibles et en langage clair, les moyens de déterminer eux-mêmes l'étendue de leurs droits et obligations, et réduire ainsi le nombre d'informations et de pièces justificatives à produire.

Pour autant cette simplification ne doit pas conduire à multiplier, sans garanties et sans justification réelle, les interconnexions de fichiers entre administrations ou encore la création de bases centralisées. Car l'administration électronique, c'est aussi favoriser l'interopérabilité des systèmes d'information, le décloisonnement des fichiers, bref un plus grand partage de l'information qui peut être bien entendu mis en œuvre au bénéfice de l'usager, lui évitant ainsi d'avoir à produire la même pièce auprès de plusieurs services ou administrations.

Aucun principe de protection des données à caractère personnel n'interdit les interconnexions. Mais le respect du principe de proportionnalité justifie que tout projet de mise en relation de fichiers fasse l'objet d'une vigilance particulière et d'un contrôle spécifique de la CNIL, portant en particulier sur l'appréciation de la finalité même de l'interconnexion (nécessité d'un intérêt public important), sur la pertinence des données échangées, les destinataires habilités à connaître des données, l'information claire et explicite des personnes concernées par ces échanges. En outre, si les informations susceptibles d'être rapprochées sont protégées par un secret professionnel, les échanges de données ne peuvent être envisagés que si, au préalable, une disposition législative spécifique est intervenue pour lever celui-ci.

Ainsi, la CNIL admet que des échanges de fichiers puissent être mis en œuvre, dans les conditions précédemment définies, pour répondre à des finalités déterminées. La plupart des interconnexions réalisées, par exemple, dans les domaines social et fiscal ont eu pour objet principal de contrôler *a posteriori* la cohérence entre diverses obligations déclaratives. La CNIL n'a jamais contesté la légitimité de cet objectif mais elle souhaite que la mise en place des interconnexions soit aussi l'occasion d'envisager de réelles simplifications des démarches administratives pour les usagers.

De même, la Commission constate dans différents secteurs, une tendance de plus en plus marquée à la centralisation d'informations et à la constitution de bases de données nationales. Elle entend rester attentive à ces évolutions dont il ne paraît pas certain que les risques aient toujours été complètement pesés.

À cet égard, la CNIL a pris acte de l'engagement du Gouvernement dans le plan stratégique, de maintenir un stockage des données décentralisé au sein de chaque administration. Elle saura toutefois rester attentive aux déclinaisons pratiques des projets visant, par la création de sites portails, à instituer des points d'accès

uniques à des téléservices, comme c'est le cas en particulier des projets monservice-public. fr, service de changement d'adresse ou encore du service de délivrance d'extrait d'actes de naissance.

Par ailleurs, en évoquant la nécessité d'un format ouvert pour les systèmes d'information des administrations de l'État, des établissements publics de l'État et des collectivités territoriales le plan stratégique fait implicitement référence en particulier à l'utilisation des standards XML, choisis comme axe de promotion de l'interopérabilité de ces systèmes d'information. Le recours à ces standards conduit à structurer de façon normalisée le contenu des fichiers et des bases de données facilitant ainsi de fait, les échanges de données entre systèmes d'information. La CNIL considère qu'au-delà des améliorations techniques attendues des conditions d'utilisation de ces systèmes d'information, le recours aux normes XML favorise implicitement le développement des interconnexions et le transfert de données. Elle entend donc suivre avec une particulière attention les travaux conduits en ce domaine.

b) Le principe de transparence : donner au citoyen une plus grande maîtrise sur ses données personnelles

L'administration électronique doit être transparente pour le citoyen. Ainsi doit-il être parfaitement informé des recueils et échanges d'informations effectués sur son compte par les administrations, tout particulièrement si ceux-ci sont réalisés à des fins de contrôle de sa situation administrative.

La CNIL encourage fortement toutes les initiatives visant à renforcer l'exercice effectif des droits de chacun sur ses données et en particulier le droit d'accès. En effet, ce droit est actuellement peu exercé, que ce soit par ignorance, en raison de la lourdeur des démarches à entreprendre ou encore de réticences des administrations à communiquer les informations.

À ce titre, la consultation en ligne par chacun de son dossier administratif présente un intérêt incontestable. Un nombre croissant de services publics offre aujourd'hui ce service, qu'il s'agisse de l'accès à ses décomptes de sécurité sociale, à son compte retraite, à son compte fiscal, voire même à son dossier médical, et la CNIL approuve pleinement ces initiatives, ayant préconisé ce mode d'exercice du droit d'accès dès ses premières recommandations sur le « bon usage » de l'internet.

À cet égard, la CNIL a pris note avec satisfaction que le Gouvernement entendait permettre aux citoyens de mieux exercer les droits qui leur sont reconnus par la loi « informatique et libertés » du 6 janvier 1978 et la loi sur l'accès aux documents administratifs du 17 juillet 1978 en mettant à leur disposition les outils et services appropriés pour consulter plus facilement leurs dossiers administratifs en ligne.

Mais au-delà, il s'agit d'offrir à chacun, la possibilité, sans avoir à se déplacer ou à se justifier, de vérifier l'exactitude de sa situation administrative, de demander et d'obtenir en ligne, sans délai, la mise à jour de ses données, leur rectification voire leur effacement, en bref de disposer d'un véritable droit de regard sur l'utilisation, par l'administration, de ses données personnelles.

L'administration électronique doit ainsi être l'occasion, pour le citoyen, d'une plus grande maîtrise de ses données administratives personnelles. Mais jusqu'où peut aller cette maîtrise ? Pourrait-on disposer du droit de contrôler l'usage de ses données, de consentir à telle ou telle communication de données et de déterminer les administrations qui auraient « droit » à connaître ses données et celles qui devraient en être « privées » ?

La CNIL estime à cet égard que recueillir l'accord de l'usager constitue bien souvent un leurre, cette démarche pouvant lui donner le sentiment qu'il serait seul maître de décider de l'usage de ses données alors que l'administration constitue à l'évidence un champ d'intervention où l'usager peut être contraint par la loi ou les règlements à fournir telle ou telle information**.** En outre, le fait qu'une personne consente à ce qu'une administration transmette des informations la concernant à une autre administration ne vaut pas nécessairement autorisation pour cette dernière à en faire usage.

Dans les cas où la loi rend obligatoire l'échange d'informations entre administrations, que ce soit à des fins d'appréciation de droits ou d'exécution d'obligations en particulier de contrôle (ex. des échanges de fichiers entre les caisses d'allocations familiales et la direction générale des impôts), l'accord de l'usager n'a pas à être requis et n'aurait d'ailleurs aucune portée. Lorsque la fourniture d'une information conditionne l'obtention d'un droit, le demandeur n'a en effet pas d'autre choix que d'« accepter » l'échange d'information entre administrations. Le refus de transmission entraînerait *ipso facto* le rejet de la demande.

En revanche, l'accord explicite de l'usager pour l'échange direct d'informations entre administrations doit être recueilli dès lors qu'il dispose d'un vrai choix et sous réserve que les textes en vigueur le permettent ou tout au moins ne comportent pas de disposition interdisant l'échange.

Ainsi, il apparaît légitime d'envisager des situations dans lesquelles l'intéressé, dès lors qu'il aurait communiqué une information à une administration — par exemple, signalé son changement de situation familiale… —, puisse l'autoriser à la transmettre à d'autres administrations si celles-ci sont habilitées à la détenir, plutôt que d'avoir à produire lui-même cette information auprès de ces dernières.

c) Le principe de sécurité graduée : de l'anonymat à la signature électronique, moduler les exigences de sécurité selon le type de demande

Une première règle s'impose : le respect, dans la mesure du possible, de l'anonymat, toutes les démarches administratives ne nécessitant pas d'identification préalable. Ainsi, il doit être possible de demander en ligne des formulaires qui sont par ailleurs disponibles librement auprès de l'administration ou de consulter un document administratif communicable sans avoir à s'identifier.

Les exigences de sécurité doivent être modulées en fonction du type de démarche administrative entreprise. Le recours systématique à des procédés de signature électronique, qui demandent d'ailleurs à être adaptés au contexte de l'administration, ne constitue donc pas aujourd'hui, pour la CNIL, une condition

préalable à la mise en place des téléprocédures. Tant que le droit, la technique et l'économie des infrastructures à clé publique ne seront pas totalement stabilisés, il pourrait paraître prématuré d'imposer des solutions qui, en tout état de cause, méritent d'être évaluées en fonction de la finalité du téléservice public et du degré de sécurité que l'on en attend.

En revanche, le recours à des procédés de chiffrement destinés à assurer la confidentialité des données transmises constitue un impératif dès lors qu'il s'agit de transmettre par internet des informations sensibles telles que des données de santé ou des données financières. La libéralisation, en France, de l'utilisation des moyens de cryptologie a permis à la CNIL de préciser, voire de renforcer ses exigences en la matière.

En conséquence, la CNIL ne peut qu'être favorable au renforcement de la sécurité des systèmes d'information des administrations, prôné par le Gouvernement, et en particulier à une politique de référencement intersectorielle de sécurité. L'orientation ainsi prise de permettre aux administrations de disposer de systèmes d'information dont le niveau de sécurité soit conforme aux exigences du monde actuel répond aux préoccupations exprimées à plusieurs reprises par la CNIL sur l'insuffisante prise en compte des impératifs de sécurité par les services publics.

La CNIL, compte tenu de ses missions, a demandé à être associée à l'élaboration et au suivi de cette politique.

d) Le principe de pluralité des identifiants : maintenir des identifiants sectoriels

En application de la loi « informatique et libertés », toute utilisation du numéro d'inscription au Répertoire national d'identification des personnes physiques, c'est-à-dire du NIR ou de son équivalent, le numéro de sécurité sociale, doit être autorisée par décret en Conseil d'État, pris après avis de la CNIL. On peut résumer la position actuelle de la CNIL sur cette question des identifiants par la formule : à chaque sphère son identifiant, pas d'utilisation généralisée d'un numéro national d'identification. Et force est d'ailleurs de constater qu'aujourd'hui l'accès aux téléservices publics existants s'effectue selon les dispositifs d'identification spécifiques aux systèmes d'information de chaque service public concerné (et acceptés par la CNIL), que l'usager a l'habitude d'utiliser dans le cadre de ses relations « traditionnelles » avec chacun de ces services.

À cet égard, il convient de prendre acte de l'affirmation, inscrite dans le plan stratégique, selon laquelle il ne peut être question qu'un identifiant unique national des citoyens, et notamment le numéro de sécurité sociale, soit utilisé pour avoir accès aux téléservices. Il faut noter également le choix du Gouvernement, d'une part, de conserver, les identifiants sectoriels propres à chaque sphère, d'autre part de laisser l'usager libre de déterminer les outils d'identification (mot de passe, certificat électronique logiciel, carte à puce, téléphone portable…) qu'il souhaite utiliser pour s'identifier auprès d'un service, dès lors que cet outil assurerait le niveau de sécurité requis.

La CNIL examinera de façon approfondie les différentes options techniques envisagées et en particulier les modalités de gestion des procédures d'identification tant au niveau du site portail (monservice-public.fr) que des téléservices accessibles via ce site. Ce projet vise à personnaliser l'actuel portail internet (Service-Public.fr) en permettant aux administrés d'accéder à des informations ciblées sur leurs centres d'intérêts, ainsi que l'accès à des téléservices nécessitant une identification préalable.

Il importe que les dispositifs d'identification retenus ne conduisent pas, de fait, à une centralisation des données d'identification des usagers. En effet dans la mesure où l'usager, dans un souci de simplification et d'ergonomie, ne devrait, lorsqu'il accède au site portail pour bénéficier de tel ou tel téléservice, avoir à s'identifier qu'une seule fois, ceci suppose :
— soit la détention par l'usager, via le support d'identification en sa possession et dont il aura l'entière maîtrise (par exemple la carte d'identité ou une carte privative ou encore une clé USB...), de l'ensemble des identifiants sectoriels et des données d'authentification qui y sont associées lui permettant de dialoguer avec chaque téléservice ;
— soit l'attribution par le site portail, jouant le rôle d'une autorité de certification, d'un numéro de certificat unique qui constituerait alors, de fait, un nouvel identifiant national unique, dont la correspondance avec chaque identifiant sectoriel serait gérée sur une base centrale, option qui ne semble guère recevable au regard des principes de protection des données ;
— soit encore l'attribution par le site portail de ce numéro de certificat unique mais qui serait ensuite retransmis aux téléservices auxquels se serait inscrit l'usager, chaque téléservice détenant alors la correspondance entre ce numéro et son identifiant propre (ceci impliquerait cependant la détention de données d'identification au moins pendant le temps nécessaire à l'attribution de ce certificat de données d'identification).

2. PREMIÈRES OBSERVATIONS SUR LA CARTE NATIONALE D'IDENTITÉ ÉLECTRONIQUE

a) L'ébauche d'un grand projet

Le ministère de l'Intérieur a lancé en juillet 2001 une mission d'étude sur un vaste projet de refonte des titres d'identité (carte nationale d'identité et passeport) reposant à la fois sur une procédure unique de délivrance des titres et sur le recours, pour la carte d'identité, à la technologie de la carte à puce intégrant des données biométriques. Est en outre envisagée la constitution de bases de données centralisées d'empreintes et de photographies.

Plus précisément, le projet consisterait à remplacer la carte d'identité actuelle, par une carte à microprocesseur comportant la photographie et l'empreinte digitale, afin en particulier de mieux garantir l'identité des personnes par le recours à des procédures de délivrance des titres plus sécurisés, notamment en permettant aux mairies réceptionnant la demande du titre d'interroger directement la mairie de

naissance pour vérifier l'état civil de la personne et procéder à la capture numérique en mairie de la photo et de l'empreinte digitale.

En outre, dans le cadre du programme de développement de l'administration électronique décidé par le Gouvernement, il est prévu que la carte d'identité électronique soit utilisée pour accéder à des téléservices nécessitant une identification.

Compte tenu de son ampleur et de ses caractéristiques, la CNIL a souhaité être informée de l'état d'avancement du projet et des orientations envisagées par le ministère de l'Intérieur afin de lui faire part, en décembre 2003, de ses premières observations.

b) La question d'une base nationale des empreintes digitales

La CNIL a estimé nécessaire de rappeler au ministère de l'Intérieur, par un courrier du 19 décembre 2003, sa doctrine en matière de fichiers biométriques ainsi que les termes des précédents avis rendus sur l'informatisation des titres d'identité.

Il convient en effet de rappeler que la Commission avait, lors d'un avis rendu le 21 octobre 1986, pris acte qu'il ne serait en aucun cas constitué un fichier manuel ou mécanographique ou automatisé au niveau national des empreintes digitales et qu'il ne serait pas procédé à la numérisation des empreintes dans les fichiers départementaux.

Conformément aux dispositions du décret du 22 octobre 1955 instituant la carte nationale d'identité, les empreintes digitales des demandeurs sont donc conservées dans les dossiers manuels détenus par les préfectures et ne font l'objet d'aucun traitement automatisé. Elles ne sont inscrites ni dans la zone de lecture optique de la carte nationale d'identité sécurisée, ni dans le système permettant la fabrication et la gestion informatisée de ce document et ne peuvent être utilisées qu'en vue de la détection des tentatives d'obtention ou d'utilisation frauduleuse d'un titre d'identité ou de l'identification certaine d'une personne dans le cadre d'une procédure judiciaire.

Depuis lors, la Commission, faisant application du principe de proportionnalité, a toujours considéré que la mémorisation et le traitement de données issues des empreintes digitales, compte tenu à la fois des caractéristiques de l'élément d'identification physique retenu, des usages possibles de ces bases de données et des risques d'atteinte à la liberté individuelle en résultant, ne pouvaient être admis que dans la mesure où des exigences impérieuses en matière de sécurité ou d'ordre public le justifiaient.

Or, il est apparu à la Commission que les objectifs présentés à l'appui du projet de constitution d'une base centrale des empreintes digitales des titulaires de titres — faciliter les démarches administratives des usagers en particulier lors des procédures de renouvellement des titres et lutter contre les usurpations d'identité ou les fraudes en la matière — si légitimes soient-ils, ne justifiaient pas la conservation, sur le plan national, de données biométriques telles que les empreintes digitales et que

les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle.

C'est pourquoi la Commission a estimé nécessaire de faire part au ministère de l'Intérieur de sa réserve de principe sur cette orientation et, afin d'approfondir sa réflexion, souhaité disposer d'un argumentaire plus précis.

La Commission a exprimé les mêmes préoccupations sur la conservation, dans une base centralisée, de la photographie et de la signature numérisées des demandeurs de titres.

B. L'examen d'applications en réseau

1. LE SERVEUR DE DONNÉES CADASTRALES

La direction générale des impôts a développé un portail national de consultation des fichiers du cadastre dans le cadre du programme COPERNIC. Son examen a été l'occasion pour la CNIL, d'une part de rappeler que les données du cadastre sont soumises aux principes de la loi du 6 janvier 1978, notamment au principe de finalité qui définit les précautions prises lors de leur délivrance aux usagers, qu'ils soient ou non professionnels, d'autre part d'engager une réflexion sur la présence, dans ces fichiers, d'informations sans lien avec la propriété immobilière et, de surcroît, non mises à jour, telles que le nom du conjoint du propriétaire qui figure sur l'acte notarié, y compris lorsque celui-ci n'est titulaire d'aucun droit réel sur le bien immobilier.

Le serveur professionnel de données cadastrales (SPDC) doit faciliter la consultation d'une partie de la documentation cadastrale et la confection des extraits dits de modèle 1 qui servent à garantir la sécurité juridique des transactions immobilières et sont nécessaires à la rédaction des actes notariés et à l'accomplissement des formalités de publicité foncière. Seules les données d'identification et de localisation des propriétés immobilières et l'identité des titulaires de droits réels sont accessibles via le SPDC, à l'exclusion des données de nature purement fiscale.

Le SPDC est, dans un premier temps, consultable dans les études des notaires équipés d'internet et dans les centres des impôts fonciers (CDIF). Ses utilisateurs sont, non seulement les notaires, leurs collaborateurs et les agents de la direction générale des impôts (DGI) qui ont une compétence foncière ou domaniale, mais aussi, de manière indirecte, le public qui peut se rendre dans un CDIF pour obtenir un extrait cadastral. Avec ce traitement, les données du cadastre deviennent, pour les notaires, accessibles à distance, en temps réel et pour l'ensemble du territoire national, alors qu'ils avaient jusqu'à présent l'obligation d'interroger le CDIF territorialement compétent en fonction de l'emplacement de la propriété bâtie ou non bâtie concernée. La même contrainte géographique disparaît pour les autres usagers qui peuvent ainsi obtenir plus facilement un extrait cadastral.

Les modalités de consultation ont été définies de manière à réduire les risques de détournement de finalité. Notamment, toute consultation suppose de

connaître au moins le département et la commune de localisation de la propriété, ce qui interdit toute interrogation nationale du cadastre sur la seule base du nom d'un propriétaire. De même, les requêtes ne peuvent pas porter sur plusieurs communes à la fois. Il est en revanche possible de demander la liste des biens appartenant à une personne dans une commune donnée, afin de faciliter la rédaction des actes relatifs à une succession ou à une cession d'actifs sociaux immobiliers.

L'accès aux informations s'effectue par l'intermédiaire d'un annuaire qui assure la gestion des droits d'accès à l'ensemble des traitements de l'administration fiscale recourant à la technologie internet, tant pour les agents de la DGI que pour les utilisateurs externes. Les notaires ont également la faculté de créer, sous leur responsabilité, des habilitations pour leurs collaborateurs. Cette habilitation leur sera attribuée en raison de leur rôle actif dans la chaîne de publicité foncière.

L'administration s'étant engagée à développer en 2003 un dispositif de traçabilité des connexions et d'audit de ces données, la Commission a émis un avis favorable pour une période expérimentale d'un an. Les conditions d'utilisation du SPDC par les notaires devront être définies dans une convention signée entre la DGI et le conseil supérieur du notariat, afin notamment d'interdire toute utilisation de l'application pour des opérations de prospection, en relation avec une activité de négociation immobilière.

2. LE SERVEUR « I-PROF »

L'application « I-Prof » développée par le ministère de l'Éducation nationale a pour objectif de permettre aux personnels enseignants [1] d'accéder et d'agir en ligne sur leur dossier administratif personnel et de dialoguer avec leur correspondant de gestion en s'appuyant sur un environnement internet réservé et sécurisé (extranet). Il s'inscrit dans le cadre d'un projet dénommé « bureau virtuel » [2] destiné à promouvoir auprès des personnels de l'éducation nationale l'accès aux technologies de l'information et de la communication. Ce projet a retenu l'attention de la CNIL en raison de son caractère exemplaire tant dans ses objectifs que dans ses modalités de mise en œuvre.

a) La copie du ministère

Ce bouquet de services, dont l'accès et l'alimentation présentent pour l'enseignant un caractère facultatif [3], constitue un point d'entrée unique, personnalisé et sécurisé, qui fédère :

— l'accès aux données professionnelles et administratives le concernant, actuellement disponibles dans les bases de données informatisées de gestion des personnels de l'éducation nationale avec la possibilité de signaler d'éventuelles erreurs ;

1 À terme, l'ensemble des personnels du ministère devrait bénéficier d'un tel outil.

2 À titre d'illustration, le dispositif (@ mel ouvert) destiné à doter les personnels de l'éducation nationale d'une adresse et d'une boîte aux lettres électronique s'inscrit dans le projet « bureau virtuel ».

3 La possibilité d'accès par une procédure papier à tous les actes de gestion est maintenue dans les rectorats et au niveau du ministère.

— la possibilité de compléter les informations le concernant dans la partie « *curriculum vitae* » du dossier et d'éditer ce *curriculum vitae* ;
— l'accès aux téléprocédures de promotion, de mutation, de formation, ainsi qu'aux décisions en résultant ;
— la consultation des textes juridiques de référence et des guides concernant la carrière et le métier d'enseignant ;
— l'accès à une messagerie électronique avec un gestionnaire attitré permettant une information personnalisée en temps réel concernant tout élément de sa vie administrative et professionnelle.

L'application « I-Prof » s'appuie sur des bases de données académiques. Les données enregistrées et accessibles dans le cadre de « I-Prof » se limitent aux données de gestion des dossiers administratifs des enseignants extraites des applications « AGAPE » et « EPP » de gestion des personnels du premier et du second degrés, ainsi qu'à des données librement communiquées par l'enseignant concerné (ex. : expériences professionnelles complémentaires, formations suivies et diplômes obtenus, publications).

Le premier module dit « enseignants » est accessible par un réseau extranet sécurisé à partir de n'importe quel ordinateur. Ainsi, un enseignant peut se connecter à « I-Prof » de son domicile ou à partir des points d'accès à internet disponibles dans chaque établissement.

Le second module dit « gestionnaires et inspecteurs », accessible via des technologies web à partir d'un poste de travail installé dans les locaux des services académiques ou à distance, est réservé, dans la limite de leurs compétences respectives, aux inspecteurs de l'éducation nationale, aux inspecteurs d'académie inspecteurs pédagogiques régionaux, ainsi qu'aux gestionnaires des personnels enseignants concernés (gestionnaires administratifs des personnels enseignants du premier et du second degrés ainsi que des personnels détachés et affectés à l'étranger). « I-prof » permet aux gestionnaires, en sélectionnant des populations ciblées, et en s'intéressant aux situations de chacun des personnels dont ils ont la charge, de les informer et de les conseiller de manière personnalisée sur leur carrière et leurs perspectives. « I-prof » doit ainsi contribuer à une personnalisation des échanges et une gestion plus individualisée des carrières des enseignants.

b) Examen réussi

Pour qu'un tel dispositif s'appuyant notamment sur le réseau internet puisse être utilisé en toute confiance, des mesures de sécurité particulières doivent être envisagées afin de garantir la confidentialité des données personnelles enregistrées. La CNIL s'est ainsi assurée que des procédés d'authentification des utilisateurs et des serveurs, ainsi que de chiffrement et de contrôle d'intégrité des données étaient mis en œuvre dans le cadre de l'application « I-Prof ».

En particulier, l'accès à distance des gestionnaires et inspecteurs aux informations par un poste dit « nomade » est sécurisé par un dispositif s'appuyant sur une « clé USB » — support physique doté d'un port de communication USB permettant la connexion de la clé sur tout ordinateur du marché — contenant un logiciel support

d'un certificat associé à un code PIN que doit composer l'utilisateur pour se connecter à « I-Prof ». Compte tenu de son intérêt, la CNIL a recommandé la généralisation de ce dispositif de « clé USB ».

La transparence constitue également une condition essentielle pour que la confiance dans le dispositif existe et que chacun puisse choisir d'adhérer ou non à cette démarche en connaissance de cause. La CNIL a ainsi rappelé la nécessité d'une parfaite information des personnels enseignants sur les objectifs poursuivis par la mise en œuvre de ce dispositif au caractère facultatif, sur les destinataires des informations enregistrées et sur leur droit de faire compléter ou rectifier les données les concernant.

Le traitement « I-Prof » est, de par sa finalité et son mode de fonctionnement, de nature à simplifier considérablement l'accès des enseignants aux informations administratives qui les concernent et à assurer ainsi la mise à jour régulière de ces données. C'est pourquoi la CNIL ne peut qu'encourager la mise en œuvre de tels dispositifs dans le domaine de la gestion des ressources humaines.

3. BERCY ET LES FRAUDEURS

La CNIL s'est prononcée en 2003 sur deux traitements qui s'inscrivent dans le cadre des projets d'administration électronique du ministère de l'Économie, des Finances et de l'Industrie et ont pour objet d'apporter aux agents de l'administration une aide à la lutte contre la fraude, douanière dans le premier cas, fiscale dans le second.

a) La lutte contre la fraude douanière

Le système informatisé de la douane concourant au dispositif de lutte contre les fraudes (SI LCF) est un important projet de la direction générale des douanes et droits indirects qui ambitionne une refonte complète du système informatique de collecte des données sur la fraude [1]. Il s'agit d'organiser le suivi, dans le cadre d'un document unique, de toutes les phases de traitement d'une affaire, depuis sa découverte — la collecte du renseignement — jusqu'à son dénouement — les procédures contentieuses et de recouvrement, l'établissement de statistiques. La conception de cette base de données nationale prend en compte le contexte général de la lutte contre la fraude douanière, en particulier la nécessité de ne pas remettre en cause la fluidité des trafics licites de marchandises et de développer la coopération internationale entre administrations douanières. Les agents des douanes habilités à un titre ou un autre à intervenir dans un dossier pourront accéder plus aisément au document correspondant, si besoin est, le modifier ou le compléter et être informés des suites réservées à leurs actions. Le travail d'analyse de risque et de définition d'une politique de contrôles ciblés devrait bénéficier de la mise en place du SI LCF. L'examen de ce projet par la CNIL a été l'occasion d'une concertation approfondie avec la douane.

1 CNIL, 1er rapport d'activité 1978-1980, p. 46 et ss et 13e rapport d'activité 1992, p. 167 et ss.

L'hétérogénéité des formes d'utilisation du traitement a conduit la Commission à demander une définition précise de la finalité du traitement. Dans sa dernière formulation, celle-ci distingue les trois objectifs autour desquels s'articulent les différents emplois du SI LCF :
— la recherche de la fraude, qui se traduit notamment par l'enregistrement des risques de fraude, l'importance donnée à l'analyse de risque et au traitement du renseignement, la centralisation des demandes d'enquêtes et l'exploitation informatisée des déclarations de transferts de fonds à destination ou en provenance de l'étranger effectués sans intervention bancaire ;
— la constatation de la fraude, qui explique l'enregistrement dans la base des informations relatives aux fraudes constatées sur la base d'un procès verbal, d'un règlement transactionnel ou d'un autre acte de constatation ;
— la poursuite et la répression de la fraude, qui conduisent à la transmission aux autorités judiciaires des infractions constatées dont la poursuite n'incombe pas à la douane et, dans le cas contraire, au suivi des diligences contentieuses et des actions de recouvrement.

Compte tenu de l'ampleur de la base de données ainsi constituée, la Commission est intervenue pour que les catégories de personnes et de données susceptibles de figurer dans le SI LCF soient définies avec précision et pour que leur durée de conservation soit adéquate, pertinente et non excessive au regard des finalités justifiant leur traitement. Plusieurs notions ont été redéfinies : la notion de « risque de fraude » suppose la présence *« d'une ou plusieurs raisons plausibles de soupçonner l'existence d'une infraction »*, formulation jugée conforme à l'article 5 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; les constatations d'infractions non suivies de suites contentieuses sur décision de la douane ne donneront pas lieu, en principe, à la saisie de données nominatives ; seules les catégories de personnes dont la responsabilité peut être engagée au regard du Code des douanes, dont la liste exhaustive a été dressée, pourront être citées dans les « fiches de constatation réalisée » ; il en résulte qu'est interdite la conservation d'informations sur des personnes qui n'auraient pas eu conscience de coopérer à une opération irrégulière ; le contenu des zones commentaires a été soigneusement défini et sera soumis à un contrôle interne ; de manière générale, l'organisation mise en place par la douane est destinée à empêcher tout fichage de personnes qui serait abusif ou erroné.

La durée de conservation des données varie de cinq à dix ans, selon la gravité de l'infraction. Le projet initial a également été complété afin de renforcer la mise à jour des données saisies, notamment en présence de décisions de relaxe, d'acquittement ou de non-lieu. La durée de conservation des données a été réduite lorsque leur mise à jour s'avère impossible à garantir, en l'absence des circuits d'informations nécessaires. Tel est le cas lorsque l'intervention de la douane se limite à transmettre la procédure au parquet compétent et à d'autres autorités administratives et qu'elle ne participe pas à la phase de poursuite des infractions qu'elle a initialement constatées.

S'agissant des extractions d'informations effectuées au bénéfice de partenaires extérieurs, qu'ils soient français ou étrangers, la Commission a rappelé que le

SI LCF constituait un fichier d'infractions et qu'il convenait de prendre toutes précautions pour éviter qu'il ne serve de casier judiciaire parallèle. Elle a souhaité être informée chaque année de la liste des extractions effectuées à cette fin. La CNIL a également rappelé dans son avis les conditions dans lesquelles des informations peuvent être ponctuellement communiquées à des tiers autorisés. La CNIL a également examiné avec attention le dispositif de journalisation des interrogations de l'application, qui gardera notamment la trace du motif de la consultation.

Le régime du droit d'accès s'inspire de celui qui avait été mis en place avec la douane dès 1980 pour le précédent traitement de lutte contre la fraude : lorsque la douane considère que certaines des informations visées par la requête, ou leur totalité, intéressent la sûreté de l'État, la défense ou la sécurité publique, ou sont couvertes par une règle de secret résultant d'une convention internationale, elle transmet la demande à la CNIL qui délimite, le cas échéant, les informations qui sont communicables de plein droit. L'information des personnes concernées devrait, enfin, être améliorée si la douane suit les recommandations de la CNIL sur ce point.

b) La lutte contre la fraude fiscale

Le traitement TSE de la direction générale des impôts est une base de données destinée à répertorier tous les liens d'intérêt, notamment en capital, ou de type inter-personnel connus de l'administration fiscale entre sociétés et personnes physiques (dirigeants, associés, actionnaires), entre sociétés ou entre personnes physiques déjà présentes dans la base à l'un des précédents titres (liens maritaux et filiaux). Il est cependant précisé que TSE ne comporte aucune information sur les liens d'actionnaires entre personnes physiques et sociétés de capitaux correspondant aux actions de ces sociétés qui sont librement cessibles sur un marché.

Cette application est représentative des projets informatiques actuellement développés dans le cadre du programme COPERNIC de refonte du système d'information fiscal : une base de données unique regroupe, au niveau national, toutes les informations de même nature ; son contenu est mis à la disposition d'un grand nombre d'agents, tant de la DGI que de la direction générale de la comptabilité publique, en fonction de profils d'habilitation définis à raison des fonctions qu'ils exercent ; la sécurisation du système est assurée par la journalisation de toutes les connexions à l'application qui doit permettre, notamment aux chefs de service immédiats des utilisateurs, d'exercer un contrôle sur l'usage effectif de la base.

TSE se présente comme une source d'informations qui peut être consultée en tant que de besoin, au titre de la programmation et de la préparation des contrôles fiscaux, de la réalisation des contrôles sur place et des contrôles sur pièces et des opérations de recouvrement des impôts, droits et taxes, par exemple : pour délimiter le périmètre d'une vérification en facilitant la détection des « ramifications cachées » d'un dossier susceptibles de justifier que soient menés conjointement une vérification de comptabilité et des contrôles IR et ISF ; pour suivre les groupes informels de sociétés qui résultent des liens familiaux existant entre dirigeants ou associés ; pour suivre les sociétés éphémères, c'est-à-dire les sociétés ou successions de sociétés qui changent régulièrement d'adresse pour échapper à tout contrôle ; pour appliquer les

règles de la solidarité fiscale entre les sociétés et leurs dirigeants ou associés pour le paiement de l'impôt.

Les agents des administrations fiscales ne sont destinataires des informations que pour autant qu'elles se rapportent à des contribuables à l'égard desquels ils participent à la programmation du contrôle fiscal ou exercent une mission de contrôle ou de recouvrement d'un impôt, droit ou taxe. Il sera procédé à une exploitation régulière et systématique des journaux des traces de consultation pour détecter d'éventuels détournements de finalité.

Les informations proviennent souvent d'actes ou de déclarations qui ne sont pas transmis à l'administration par les associés, actionnaires ou dirigeants de société concernés, a fortiori par leurs conjoints, mais par les tiers qui les ont rédigés. Aussi, la CNIL a-t-elle souhaité attirer l'attention de la DGI sur le risque que les intéressés ne soient pas informés de l'existence du traitement, ni des conditions d'exercice des droits d'accès et de rectification. En effet, l'administration ne peut pas se soustraire à son obligation d'information.

Les opportunités offertes par les projets d'administration électronique, qui permettent la consultation en ligne dans un environnement sécurisé des informations nominatives détenues par la DGI ou la délivrance de renseignements sur les traitements automatisés mis en œuvre par les administrations fiscales, devraient aussi être mises à profit. Dans l'immédiat, devant l'impossibilité de demander à l'administration d'adresser un courrier à chaque associé, actionnaire ou dirigeant, la Commission recommande qu'à tout le moins, les documents adressés ou remis aux personnes accomplissant les formalités d'enregistrement indiquent qu'il leur appartient d'informer les personnes mentionnées dans les actes ou déclarations des conditions d'exploitation des données les concernant et d'exercice des droits d'accès et de rectification.

4. TÉLÉDÉCLARATIONS ET TÉLÉPAIEMENTS EN MATIÈRE FISCALE

L'année 2003 a marqué une nouvelle étape dans le développement des téléprocédures fiscales. Pour s'en tenir aux services proposés en matière de fiscalité des particuliers, plus de 600 000 déclarations générales de revenus — contre 117 000 en 2002 — et 80 000 déclarations annexes ont été effectuées en ligne au titre de la campagne d'impôt sur le revenu ; plus de 1,9 million de téléconsultations du compte fiscal ont été enregistrées en 2003.

Quelques améliorations ont été apportées aux traitements TéléIR et ADONIS [1] : trois dates limite de souscription par internet, applicables en fonction de la localisation du contribuable et postérieures à la date limite arrêtée pour les déclarations papier, ont été prévues afin d'accorder un délai supplémentaire aux contribuables qui envoient leur déclaration par voie électronique et d'améliorer la qualité du service en répartissant sur une période plus longue les télédéclarations qui, s'étaient concentrées en 2002, dans les heures précédant la date de dépôt : plus de la moitié

1 CNIL, 22e rapport d'activité 2001, p. 129 et ss.

des déclarations ont ainsi été souscrites au cours des trois dernières semaines en 2003 alors que 50 % des déclarations l'avaient été dans les trois derniers jours en 2002.

2003 a été l'année de la suppression de l'obligation d'adresser sur support papier les demandes de rattachement au foyer fiscal. Dorénavant, c'est la totalité des envois parallèles de documents papier qui ont disparu en cas de télédéclaration. Les justificatifs de charges ou de réduction d'impôt doivent cependant être conservés par les contribuables pendant trois ans pour être produits en cas de demande de l'administration.

Par ailleurs, quelques caractéristiques du système méritent d'être rappelées pour leur intérêt. Les téléservices doivent être ouverts à l'ensemble des internautes, quel que soit le matériel dont ils disposent. Ceux qui rencontrent des difficultés peuvent dorénavant s'assurer que la configuration de leur poste permet de déclarer ses revenus en ligne dans de bonnes conditions. Ceux dont l'ordinateur n'est pas équipé du logiciel nécessaire à l'utilisation du service de déclaration en ligne peuvent le télécharger.

Il est possible de remplir sa déclaration à son propre rythme. Il suffit de la préparer hors connexion après avoir téléchargé le formulaire sur son ordinateur. Dès l'envoi en ligne de sa déclaration, le contribuable reçoit un accusé de réception horodaté qui constitue la preuve de l'envoi. Il peut l'imprimer, le télécharger ou le consulter durant l'année dans le dossier fiscal en ligne.

Le certificat électronique dont il convient d'être muni pour l'envoi sécurisé des déclarations de revenus par internet, continue à être délivré en ligne gratuitement par l'administration. Il est transmis après identification du contribuable sur la base de trois informations à caractère personnel dont la connaissance nécessite d'être en possession du formulaire de déclaration des revenus de l'année N et de l'avis d'imposition sur les revenus N-1. Il doit également fournir son adresse électronique et un mot de passe qui sera demandé à chaque connexion. Cette contrainte d'identification préalable de l'internaute justifie que le service ne soit pas accessible aux personnes qui déclarent leurs revenus pour la première fois ou dont la structure du foyer fiscal vient de changer. C'est ainsi que les couples qui ont bénéficié d'une imposition commune en 2002 au titre de la signature d'un pacte civil de solidarité dès l'entrée en vigueur de la loi ont pu utiliser la téléprocédure pour la première fois en 2003.

Le certificat s'installe automatiquement sur le disque dur de l'ordinateur. Il est cependant possible de le copier sur disquette ou Cédérom ou de le transmettre par messagerie, afin de l'utiliser à partir d'un autre ordinateur. Il permet également de consulter certains éléments du compte fiscal électronique du particulier, qui comporte cette année les déclarations de revenus et les avis d'imposition d'IR et de CSG/CRDS des trois dernières années, y compris les avis de dégrèvement et les avis supplémentaires, ainsi que les avis d'imposition 2003 de taxe d'habitation, du moins s'ils correspondent à la résidence principale.

Le portail fiscal permet également, au travers du traitement SATELIT [1], le télérèglement de l'impôt sur le revenu, la taxe d'habitation et la taxe foncière et la

1 CNIL, 21e rapport d'activité 2000, p. 235 et ss.

gestion des contrats de mensualisation et de prélèvement automatique, la modification du montant de son prélèvement et le signalement des changements d'adresse ou des coordonnées bancaires.

En revanche, aucune solution n'a encore été trouvée pour permettre la double signature des déclarations de revenus en cas d'imposition commune qui est prévue par la législation. Il est également indispensable que chaque membre d'un foyer fiscal puisse disposer, à brève échéance, d'un certificat électronique confidentiel et individuel, c'est-à-dire qui ne soit plus fondé sur des informations partagées au sein du foyer fiscal IR, afin que seuls les redevables d'un impôt accèdent aux données correspondantes et que les personnes solidairement redevables au titre de l'IR ou de la TH ne soient pas en mesure d'accéder aux informations relatives aux impositions propres de leur conjoint ou co-occupant. Seule cette mesure permettra aux usagers de bénéficier de l'application ADONIS dans les mêmes conditions que les agents de l'administration. Enfin, les particuliers ne peuvent toujours pas utiliser le certificat électronique délivré par l'administration fiscale pour procéder au télépaiement de leurs impôts, cette opération ne bénéficiant pas actuellement du même niveau de sécurité.

II. PRINCIPES ET PRATIQUES DU VOTE ÉLECTRONIQUE

Après une année 2002 marquée par plusieurs expérimentations de vote électronique [1], la CNIL a estimé nécessaire d'adopter en 2003 une recommandation sur la sécurité des systèmes de vote électronique. Elle s'est également prononcée sur l'organisation, pour la première fois, d'un vote par correspondance électronique avec valeur probante pour une élection politique ainsi que sur les premiers textes relatifs au vote électronique pour les élections consulaires.

A. La recommandation relative à la sécurité des systèmes de vote électronique

La recommandation, de caractère technique, adoptée par la CNIL le 1er juillet 2003, a pour objet de garantir de façon effective le respect des dispositions de la loi de 1978 sur la protection des données personnelles et d'assurer l'anonymat et la confidentialité du vote, la transparence des systèmes informatiques mis en place, tout en prônant une certaine souplesse dans les solutions à adopter en fonction des enjeux électoraux en cause.

Cette recommandation constitue une première approche de la sécurité des dispositifs de vote électronique sur place ou à distance, en particulier par internet, dispositifs encore en pleine évolution. Elle ne concerne pas les dispositifs de vote par

1 *Cf.* Rapport annuel 2002 « La cyberdémocratie en test » pp. 77-86.

codes-barres et les dispositifs de vote par téléphone fixe ou mobile sur lesquels la Commission sera amenée à se prononcer ultérieurement.

1. L'EXIGENCE DE TRANSPARENCE

Le vote manuel a comme principale qualité sa grande simplicité [1] permettant à l'électeur, s'il le souhaite, à tout moment de vérifier facilement la régularité du déroulement d'un scrutin.

Force est de constater qu'il n'en est pas de même pour les systèmes de vote électronique comme la Commission a pu maintes fois le vérifier à l'occasion de l'instruction des dossiers.

a) Urne électronique ou boîte noire ?

Les procédés techniques mis en œuvre dans les systèmes de vote électronique sont souvent d'une grande complexité, à base notamment de techniques de chiffrement, ce qui nécessite généralement, pour les évaluer, le recours à une expertise tierce. Mais cette expertise se limite le plus souvent à quelques aspects du système et ne va rarement sinon jamais au cœur du système lui-même. En outre, la plupart des éditeurs de ces systèmes se réfugient derrière le secret industriel pour ne rien révéler sur le fonctionnement réel de leur produit.

Or, le dispositif technique présente souvent des négligences flagrantes sous certains aspects pourtant essentiels à la préservation de l'anonymat du vote : il en est ainsi de certains procédés de vote à distance pour lesquels l'électeur s'authentifie par un nom et un mot de passe, ceux-ci étant édités par un sous-traitant puis distribués par courrier ordinaire non recommandé, voire transmis en main propre par un service de la mairie mais sans qu'aucune mesure de protection particulière ne soit prise pour les conserver confidentiels.

Aucun des systèmes de vote connus de la CNIL ne prévoient de produire des éléments de preuve en cas de contentieux électoral. Ces éléments de preuve s'entendent sur le fonctionnement du système de vote lui-même lors du déroulement du scrutin, de manière à démontrer de façon convaincante qu'il n'a pas donné lieu à un fonctionnement anormal, que celui-ci soit involontaire ou délibéré.

La fascination de la technologie est telle qu'on lui fait une confiance aveugle alors que près d'un demi-siècle d'informatisation de notre société nous a pourtant appris à être beaucoup plus réservés.

Peuvent être cités deux exemples qui pourraient paraître triviaux dans le cas d'un vote manuel :

- L'authenticité du bulletin de vote déposé dans l'urne

Dans le cas du vote manuel, c'est l'électeur qui glisse son bulletin de vote dans l'urne, et ce, devant témoins. Dans un système de vote électronique, on perd

1 Symbolisée par l'urne transparente.

cette transparence : l'électeur « clique » sur l'écran de la machine à voter sur le candidat de son choix et doit ensuite faire confiance au système pour qu'il transforme ce choix en un vote dématérialisé déposé dans l'urne électronique virtuelle.

- L'authenticité de l'urne dépouillée

Ici aussi, dans le cas d'un vote manuel, tout électeur soupçonneux peut s'assurer visuellement que l'urne utilisée lors du dépouillement du scrutin est bien celle qui a servi de réceptacle aux bulletins de vote. Dans le vote électronique, le président et son assesseur introduisent chacun de son côté leur mot de passe sur l'écran et au bout de quelques secondes, les résultats s'affichent : rien ne vient prouver l'origine de l'urne dépouillée, du moins pour l'électeur « de base ».

b) Les conditions du contrôle démocratique

Le recours à des techniques informatiques sophistiquées ne doit pas conduire à faire échapper les systèmes de vote au contrôle démocratique des membres du bureau de vote, des scrutateurs et des électeurs au profit de techniciens informatiques.

La Commission préconise donc le recours systématique à l'expertise indépendante des systèmes de vote électronique, à une procédure d'agrément par le ministère de l'Intérieur pour les machines à voter définies par le Code électoral, l'accès au code source des logiciels et l'utilisation d'algorithmes de chiffrement publics. Par ailleurs, le système de vote doit pouvoir fournir la traçabilité complète de son fonctionnement interne lors d'un scrutin afin de garantir une base solide aux audits externes, notamment en cas de contentieux électoral.

L'ensemble du dispositif de vote déployé doit permettre aux autorités nationales compétentes, aux membres du bureau de vote et aux délégués des candidats ou à leurs experts délégués d'assurer ainsi une surveillance effective des opérations électorales.

Dès lors, il importe que toutes les mesures soient prises pour leur permettre de vérifier l'effectivité des dispositifs de sécurité prévus pour assurer le secret du vote et, en particulier, les mesures prises respectivement pour :
— garantir la confidentialité du fichier des électeurs ;
— procéder au chiffrement des bulletins de vote et à leur conservation dans un traitement distinct de celui mis en œuvre pour assurer la tenue du fichier des électeurs ;
— assurer la conservation des différents supports d'information pendant et après le déroulement du scrutin.

Toutes les facilités devraient être accordées aux membres du bureau de vote et aux délégués des candidats, s'ils le souhaitent, pour pouvoir assurer une surveillance effective de l'ensemble des opérations électorales et, en particulier, de la préparation du scrutin, du vote, de l'émargement et du dépouillement. Dans le même esprit, la vérification de l'état initial du système avant l'ouverture du scrutin ou le dépouillement doit être publique.

La Commission insiste aussi fortement sur la nécessité de localiser les serveurs et autres moyens informatiques centraux sur le territoire national.

Enfin, les électeurs doivent être clairement informés des modalités de fonctionnement général du système de vote électronique.

2. LES RÈGLES DE FIABILITÉ

La CNIL préconise des mesures fortes comme la séparation des données nominatives de l'électeur et du fichier des votes (l'urne électronique) sur des systèmes informatiques distincts ainsi que le chiffrement du bulletin de vote dématérialisé dès son émission sur le terminal.

a) Secret et authenticité du vote

LA SÉPARATION DES DONNÉES NOMINATIVES DES ÉLECTEURS ET DES VOTES

Le secret du vote doit être garanti par la mise en œuvre de procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote. Ainsi, la gestion du fichier des votes et celle de la liste d'émargement doivent être faites sur des systèmes informatiques distincts, dédiés et isolés. Ces fichiers doivent faire l'objet de mesures de chiffrement.

Pour assurer la confidentialité des votes, les bulletins doivent être chiffrés par un algorithme public réputé « fort » de même que la liaison entre le terminal de vote de l'électeur et le serveur des votes.

L'émargement doit se faire dès la validation du vote de façon à ce qu'un autre vote ne puisse intervenir à partir des éléments d'authentification de l'électeur déjà utilisés. L'émargement comporte un horodatage. La liste d'émargement doit être située sur un système distinct de celui contenant l'urne électronique. Cette liste, aux fins de contrôle de l'émargement, ainsi que le compteur des votes ne doivent être accessibles qu'aux membres du bureau de vote et aux personnes autorisées.

La liste d'émargement doit être enregistrée sur un support scellé, non réinscriptible.

LES PROCÉDÉS D'AUTHENTIFICATION DE L'ÉLECTEUR

Parmi les procédés d'authentification à distance, la CNIL recommande, en l'état actuel de la technique, l'utilisation d'un certificat électronique quand l'importance de l'enjeu le justifie, mais ne rejette pas la méthode du code identifiant et du mot de passe, dès lors que des garanties sont données sur le caractère confidentiel de leur transmission à leurs titulaires. L'usage de la biométrie est possible s'il s'agit de systèmes ne laissant pas de traces ou comportant l'enregistrement des données sur un support individuel détenu par l'électeur sans constitution de fichier.

LES SÉCURITÉS DES MOYENS INFORMATIQUES

Il convient que toutes les mesures physiques (contrôle d'accès, détermination précise des personnes habilitées à intervenir…) et logiques (*firewall*, protection d'ac-

cès aux applicatifs…) soient prises tant au niveau des serveurs du dispositif que sur les postes accessibles au public afin de garantir la sécurité et la confidentialité des données personnelles en particulier contre les intrusions venant de l'extérieur. Les algorithmes de chiffrement, de signature électronique et les fonctions de hachage doivent être des algorithmes publics réputés « forts ».

b) Secret et authenticité des résultats électoraux

LE SCELLEMENT DU DISPOSITIF DE VOTE ÉLECTRONIQUE

Les systèmes de vote électronique expertisés et utilisés doivent faire l'objet d'un scellement c'est-à-dire d'un procédé permettant de déceler toute modification de ce système. Le procédé de scellement doit lui-même être agréé. La vérification du scellement devrait pouvoir se faire à tout moment, y compris durant le déroulement du scrutin et par tout électeur.

Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement/déchiffrement et le contenu de l'urne ne doivent pas être accessibles, de même que la liste d'émargement, sauf aux fins de contrôle de l'effectivité de l'émargement des électeurs.

La Commission préconise que tous les fichiers supports (copies des programmes sources et exécutables, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) soient conservés sous scellés jusqu'à l'épuisement des délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote. Obligation doit être faite, le cas échéant, au prestataire de service de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation des supports. Lorsqu'aucune action contentieuse n'a été engagée avant l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

LES SÉCURITÉS LORS DU DÉPOUILLEMENT

La génération des clés destinées à permettre le déchiffrement et donc le dépouillement des votes à l'issue du scrutin doit être public et se dérouler le jour du dépouillement. Cette procédure devrait être conçue de manière à prouver de façon irréfutable que seuls le président du bureau et ses assesseurs prennent connaissance de ces clés, à l'exclusion de toute autre personne y compris les personnels techniques chargés du déploiement du système de vote.

Le système de vote doit garantir que des résultats partiels (hormis le nombre de votants) ne seront pas accessibles durant le déroulement du vote.

Les décomptes des voix par candidat ou liste de l'élection doivent apparaître lisiblement à l'écran et faire l'objet d'une édition sécurisée pour être portés au procès-verbal de l'élection.

Le système de vote électronique doit être bloqué après le dépouillement de sorte qu'il soit impossible de reprendre ou de modifier les résultats après la clôture du scrutin.

B. Les urnes électroniques en pratique

La Commission a été consultée en 2003 sur de nouvelles applications de vote électronique.

1. LES FRANÇAIS DE L'ÉTRANGER

A ainsi été mis en œuvre, pour la première fois en France, un vote électronique officiel pour des élections politiques. Le ministère des Affaires étrangères a, en effet, mis en place un dispositif de vote électronique par internet afin de permettre aux Français établis aux États-Unis de participer à la désignation de leurs représentants au Conseil supérieur des Français de l'étranger le 1er juin 2003. Ce dispositif coexistait avec un vote par correspondance papier et un vote dans des bureaux de vote installés dans les consulats.

La CNIL a été saisie d'un projet de décret et d'un projet d'arrêté relatifs à l'organisation de ce vote par correspondance électronique. Dans sa délibération n° 03-019 du 24 avril 2003 [1], la Commission n'a pas estimé devoir, en raison des conditions dans lesquelles cette expérimentation a été décidée et organisée, émettre un avis défavorable aux projets de décret et d'arrêté qui lui étaient soumis ; elle a formulé des recommandations sur les modalités de déroulement des opérations électorales, en particulier sur la gestion de l'impression des identifiants et des mots de passe (l'imprimeur ne devant pas accéder en clair à ces codes), sur la nécessité d'un envoi en recommandé à l'électeur de ses codes personnels ou la mise en place d'un système d'authentification certifié, la possibilité d'enregistrer les réclamations des électeurs et un contrôle effectif des dispositifs de sécurité prévus pour assurer le secret du vote par des représentants du ministère ou des experts.

La Commission a considéré que ces recommandations ne préjugeaient pas de sa position à venir sur l'extension du vote électronique à d'autres circonscriptions électorales du Conseil supérieur des Français de l'étranger et sur les textes correspondants.

Le bilan de cette expérience de vote par correspondance électronique met en exergue clairement que les votants ont privilégié le vote par internet à 60,60 % (33,85 % par correspondance sous pli fermé et 5,56 % dans les bureaux de vote). Cette nouvelle faculté de vote montre son potentiel dans le cas d'un électorat dispersé. En revanche, la participation au scrutin a baissé par rapport à 1997 (14,47 % de votants contre 15,10 % en 1997 [2]). Le vote électronique par internet s'avère donc, en l'état, sans effet sur la participation et sans impact sur le civisme des électeurs.

1 Délibération n° 03-019 du 24 avril 2003 relative aux projets de décret et d'un projet d'arrêté, présentés par le ministère des Affaires étrangères, relatifs au vote par correspondance électronique des électeurs inscrits dans les circonscriptions des États-Unis d'Amérique pour les élections au Conseil supérieur des Français de l'étranger le 1er juin 2003.

2 Source : ministère des Affaires étrangères.

2. LES CHAMBRES DE COMMERCE ET D'INDUSTRIE

Plusieurs textes ont introduit la possibilité du vote électronique pour les élections consulaires, les élections aux tribunaux paritaires des baux ruraux et pour les élections prud'homales [1] et, prochainement, pour les élections professionnelles [2].

La CNIL a aussi été amenée à se prononcer dans une délibération n° 03-049 du 20 novembre 2003 sur le vote pour les élections des membres des chambres de commerce et d'industrie.

a) Un scrutin bien encadré

L'article 19 de la loi n° 2003-591 du 2 juillet 2003 [3] habilitant le Gouvernement à simplifier le droit, introduit la possibilité de mise en œuvre du vote électronique pour les élections aux chambres de commerce et d'industrie, aux chambres de métiers, aux chambres d'agriculture, aux tribunaux paritaires des baux ruraux et pour les élections prud'homales.

L'article 7 de d'ordonnance 2003-1067 du 12 novembre 2003 [4] relative à l'élection des membres des chambres de commerce et d'industrie, à la prorogation des mandats des délégués consulaires et modifiant le Code de commerce, consacre l'introduction du vote électronique pour les élections des membres des chambres de commerce et d'industrie et fixe la primauté du vote électronique sur le vote par correspondance.

C'est en application de ces textes que la Commission a été saisie le 10 novembre 2003 d'un projet de décret modifiant le décret n° 91-739 du 18 juillet 1991 relatif aux « chambres de commerce et d'industrie, aux chambres régionales de commerce et d'industrie, à l'assemblée des chambres françaises de commerce et d'industrie et aux groupements interconsulaires ».

Outre une refonte du texte, le projet introduit le vote électronique pour les élections des membres des Chambres de commerce et d'industrie. Au-delà du vote électronique, l'ensemble du processus de dématérialisation de l'organisation des élections consulaires est pris en compte : la collecte des renseignements nécessaires à la constitution des listes électorales, la mise à disposition de la liste électorale par des voies dématérialisées, les modalités pratiques du vote lui-même, la gestion de la

1 Loi n° 2003-591 du 2 juillet 2003 habilitant le gouvernement à simplifier le droit ; ordonnance n° 2003-1067 du 12 novembre 2003 relative à l'élection des membres des chambres de commerce et d'industrie, à la prorogation des mandats des délégués consulaires et modifiant le Code de commerce ; décret en projet modifiant le décret n° 91-739 du 18 juillet 1991 relatif aux chambres de commerce et d'industrie, aux chambres régionales de commerce et d'industrie, à l'assemblée des chambres française de commerce et d'industrie et aux gouvernements interconsulaires (délibération n° 03-049 de la CNIL du 20 novembre 2003).

2 Projet de loi pour la confiance dans l'économie numérique, en discussion en seconde lecture au Sénat en avril 2004.

3 Loi n° 2003-591 du 2 juillet 2003 habilitant le Gouvernement à simplifier le droit, publiée au *JO* n° 152 du 3 juillet 2003.

4 Ordonnance n° 2003-1067 du 12 novembre 2003 relative à l'élection des membres des chambres de commerce et d'industrie, à la prorogation des mandats des délégués consulaires et modifiant le Code de commerce, publiée au *JO* du 13 novembre 2003.

liste d'émargement et les opérations de dépouillement. Le décret renvoie à un arrêté, pris après avis de la CNIL, le soin d'apporter les précisions nécessaires.

b) Un mode opératoire complet

L'examen de ce projet de décret, qui constituait une première application concrète de la recommandation relative au vote électronique, a permis de voir que cette recommandation était bien perçue et comprise et que les préoccupations exprimées relatives au secret et à l'unicité du vote, ainsi qu'au contrôle des opérations électorales étaient partagées. Le projet reprend les recommandations relatives à la sécurité des systèmes de vote électronique émises par la CNIL. Ainsi, le projet de décret prévoit :
— les sécurités à mettre en place pour gérer le retour des questionnaires destinés au recensement des électeurs, la transposition des conditions physiques du retour se traduisant par une exigence d'authentification ;
— les conditions de la mise à disposition par des voies dématérialisées de la liste électorale, afin d'assurer la restriction de la consultation aux seuls électeurs prévue par le texte, la mise en ligne devant être entourée de conditions de sécurité assurant le respect du Code électoral ;
— la nécessité d'une expertise du système de vote électronique afin de garantir le respect des mesures de sécurité et de confidentialité exigées et d'assurer l'effectivité du contrôle du juge ;
— les garanties prévues pour assurer l'authentification de l'électeur, la confidentialité et l'unicité du vote dans les mêmes conditions que le vote physique ;
— la nécessaire confirmation de la prise en compte du vote auprès de l'électeur, afin de permettre de vérifier que tous les votes ont bien été pris en compte en assurant la confirmation de la bonne réception du vote et de l'émargement ;
— la sécurité et la confidentialité du contenu de l'urne électronique et du fichier des électeurs, afin de garantir le cloisonnement des fichiers contenant les votes exprimés (l'urne électronique) et le fichier des électeurs, les traitements automatisés devant être effectués sur des systèmes informatiques non seulement distincts, mais également dédiés et isolés, et le chiffrement du contenu de l'urne électronique assurant la sécurité de l'expression des votes en cours de scrutin ;
— la nécessité de permettre le contrôle de l'état du scellement du système de vote avant de procéder au dépouillement, la commission électorale devant pouvoir s'assurer à tout moment du scellement du système et notamment avant le dépouillement et être à cet effet être dotée d'outils permettant d'authentifier l'état du scellement ;
— la nécessité de permettre le contrôle a posteriori du juge en assurant une transparence complète du système de vote électronique permettant le déroulement de l'ensemble des opérations électorales afin de prouver de façon irréfutable que :
1) tous les votes ont été pris en compte ;
2) le procédé de scellement est resté fiable tout au long du scrutin ;
3) le vote est resté anonyme ;
4) la liste d'émargement ne comprend que les électeurs ayant voté ;
5) l'urne dépouillée est bien celle contenant les votes des électeurs et qu'elle ne contient que ces votes ;
6) aucun dépouillement partiel n'a pu être effectué durant le scrutin.

Dès lors, la Commission ne pouvait que donner un avis favorable à ce projet de décret.

III. DONNÉES PUBLIQUES, DONNÉES PRIVÉES

À la question classique de l'interconnexion des grands fichiers publics ayant des finalités distinctes, vient s'ajouter celle de l'utilisation par la puissance publique de gisements de données constituées par des entreprises privées. La question est récurrente mais elle prend un tour particulier à un moment où l'État dans un souci d'efficacité à moindre coût budgétaire recherche des collaborations ou des synergies avec le secteur privé.

À l'inverse, le monde du commerce et des services marchands, particulièrement celui des téléservices, ne peut ignorer que les données publiques sont une véritable mine.

A. Du privé au public : trois cas

Quand le ministère de l'Intérieur loue un fichier de La Poste comme une société commerciale, il se trouve des administrés pour s'en étonner, voire s'en plaindre, mais la CNIL n'a rien à y objecter. Quand le ministère des Finances, pour lutter contre la fraude à la redevance audiovisuelle, souhaite disposer du fichier des abonnés aux télévisions payantes, la CNIL est amenée à rappeler les limites du droit de communication de l'administration fiscale.

Il est intéressant de comparer ces démarches avec les pratiques des administrations américaines.

1. L'UTILISATION DU FICHIER DE LA POSTE POUR L'INSCRIPTION SUR LES LISTES ÉLECTORALES

Afin de sensibiliser les personnes ayant récemment déménagé à la nécessité de s'inscrire sur les listes électorales de leur nouvelle commune de résidence et pour leur permettre, le cas échéant, d'accomplir ces formalités par correspondance, le ministère de l'Intérieur a demandé à La Poste de mettre à sa disposition le fichier appelé « nouveaux voisins ».

Il convient de préciser que ce fichier des « nouveaux voisins », qui a recueilli l'avis favorable de la CNIL (*cf.* 23e rapport, p. 144), recense les coordonnées des personnes qui, ayant déménagé, ont souscrit auprès de La Poste un contrat de réexpédition définitive de leur courrier.

Les formulaires de demandes de réexpédition définitive du courrier précisent la possibilité pour La Poste de communiquer les nouvelles coordonnées aux

organismes liés contractuellement à La Poste, qu'ils aient ou non connaissance de l'ancienne adresse de la personne ayant déménagé. Les personnes qui remplissent ces formulaires ont la faculté de s'opposer à une telle communication en cochant une case, prévue à cet effet.

Un certain nombre de personnes, étonnées de recevoir un courrier du ministère de l'Intérieur les invitant, à la suite de leur déménagement, à s'inscrire sur les listes électorales de leur nouveau domicile, ont interrogé la CNIL sur la régularité de l'opération menée par le ministère de l'Intérieur.

En l'espèce, le ministère de l'Intérieur avait informé la CNIL, préalablement aux envois qu'il allait effectuer auprès de nombreux citoyens, qu'il avait loué auprès de La Poste le fichier des « nouveaux voisins » afin de leur adresser un courrier. La CNIL a toutefois demandé au ministère de l'Intérieur des précisions sur les modalités de traitement des informations nominatives recueillies auprès de La Poste, ainsi que de celles qui auraient été collectées à partir du formulaire que les personnes concernées devaient renvoyer pour s'inscrire sur les listes électorales de leur nouvelle commune de résidence.

Le ministère de l'Intérieur a déposé une demande d'avis relative à la mise en œuvre de ce traitement, répondant ainsi aux interrogations de la CNIL. Cette demande a reçu un avis favorable de la CNIL.

La Commission a, dès lors, pu préciser aux personnes qui l'avaient saisie que l'envoi du courrier et du formulaire d'inscription sur les listes électorales avait été confié, par le ministère de l'Intérieur, à un prestataire de service chargé de traiter les réponses, acheminées au moyen d'enveloppes T, et de les envoyer à la mairie du nouveau domicile de chaque électeur. Cette société, seule destinataire de ces informations, s'est engagée à ne procéder à aucune modification ni à aucune cession des données recueillies et à les détruire à l'issue des opérations d'inscription sur les listes électorales, le 1er mars 2004.

Certaines des réclamations reçues par la CNIL ont toutefois fait apparaître des anomalies. Par exemple, bien que n'ayant souscrit aucun contrat de changement d'adresse auprès de La Poste, certaines personnes ont reçu le courrier du ministère de l'Intérieur. La CNIL a interrogé les services de La Poste et ces réclamations sont en cours d'instruction.

2. LES FICHIERS DES TÉLÉVISIONS PAYANTES

Le projet d'utilisation des fichiers d'abonnés à des services payants de programme de télévision par le service de la redevance audiovisuelle, figurant dans le projet de loi de finances pour 2004, a conduit la CNIL à rappeler fermement le principe-clé de finalité.

a) En 1991 déjà

La direction générale de la comptabilité publique a transmis à la CNIL, pour information et remarques éventuelles, les articles du projet de loi de finances pour

2004 visant à modifier le régime juridique de cette taxe fiscale et, en particulier, à autoriser l'administration à recevoir, sur sa demande, les fichiers d'abonnés des diffuseurs ou distributeurs de services payants de programmes de télévision. Un projet similaire avait été, une première fois, rejeté par le Conseil constitutionnel en 1991 au motif qu'il constituait un cavalier budgétaire. La CNIL s'était, à l'époque, prononcée sur ce projet qui se présentait comme une extension du droit de communication des agents du service de la redevance de l'audiovisuel. Elle avait contesté le fait que le droit de communication des services de la redevance puisse conduire à transformer, dans leur totalité, les fichiers d'abonnés aux télévisions payantes en « fichiers de référence » pour l'administration, c'est-à-dire en sources permanentes d'informations, sans tenir compte de la finalité de leur constitution.

Le projet de 1991 s'exposait, en effet, aux critiques que la CNIL a toujours exprimées à l'égard du droit de communication des administrations fiscales lorsqu'il est abusivement interprété comme permettant la transmission de fichiers entiers, relatifs à un ensemble de personnes qui répondent seulement à un ou plusieurs critères, au risque d'attribuer ainsi à ces fichiers une finalité secondaire d'ordre fiscal. Aussi, la CNIL a-t-elle toujours, depuis 1978, cherché à encadrer le recours au droit de communication et à en redéfinir la portée de telle manière qu'il n'autorise que la présentation de demandes de renseignements ponctuelles et motivées, portant sur des personnes nommément désignées. C'est en ce sens que la CNIL était intervenue en 1991 pour s'opposer à toute transmission de la totalité des fichiers des câblo-opérateurs et des chaînes de télévision payantes.

b) Des demandes ponctuelles et motivées

Le projet présenté à l'automne 2003 ne se différencie pas, pour l'essentiel, de celui de 1991 : il s'agit toujours de l'extension du droit pour l'administration d'avoir communication, sur sa demande mais de manière régulière, quasi-systématique, de fichiers exhaustifs dont elle n'est pas destinataire au sens de la loi du 6 janvier 1978, nonobstant leur finalité déclarée, afin de les mettre en relation, à des fins de contrôle, avec le fichier des personnes imposées à la redevance audiovisuelle.

Une telle proposition ne peut que heurter le principe, essentiel, de finalité, tel qu'il est défini par l'article 6 de la directive 95/46/CE : *« Les États membres prévoient que les données à caractère personnel doivent être* […] *collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités »*. Si l'article 13 de cette directive permet aux États de prendre des mesures législatives visant à limiter la portée de cette règle lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder un intérêt économique ou financier d'un État, y compris dans le domaine fiscal, l'atteinte portée en l'espèce aux dispositions protectrices des données personnelles a paru à la CNIL, quelle que soit la légitimité de l'objectif de réduction de la fraude à la redevance, disproportionnée par rapport aux bénéfices espérés. Dès lors, la Commission a réaffirmé sa doctrine constante, selon laquelle le droit de communication n'autorise que la transmission de demandes ponctuelles et motivées. Cette disposition du projet de loi de finances pour 2004 n'a pas reçu l'aval du Parlement.

c) Collecte privée à des fins publiques

La question des rapports entre données publiques et données privées n'est pas sans lien avec une autre disposition de la réforme de la redevance audiovisuelle : la loi de finances pour 2004 prévoit la collecte de données personnelles complémentaires — les date et lieu de naissance — sur les déclarations de récepteur de télévision souscrites par les détenteurs, y compris lorsque celles-ci sont transmises par les vendeurs.

L'objectif de réduction du risque d'erreur d'imposition pour cause d'homonymie a été approuvé par la Commission. Cependant, les craintes d'utilisation commerciale de données recueillies pour les besoins de l'administration ont conduit la CNIL à souhaiter qu'il soit précisé, par voie réglementaire, que les renseignements collectés au titre de l'accomplissement de cette nouvelle obligation fiscale ne peuvent pas être conservés par le vendeur sur un autre support que la déclaration prévue par la loi, ni utilisés à d'autres fins, ni communiqués à d'autres personnes que les agents habilités du service de la redevance audiovisuelle.

Dans le même désir d'améliorer la qualité des informations portées sur les déclarations transmises par les commerçants, la CNIL a rappelé que le recueil des données destinées à l'administration devait respecter les obligations de transparence de l'article 27 de la loi du 6 janvier 1978 : la collecte des données doit s'effectuer directement auprès du client, celui-ci étant préalablement informé de leur destination, afin qu'il puisse en vérifier la pertinence et disposer d'une copie de sa déclaration.

3. L'UTILISATION DE FICHIERS PRIVÉS PAR LES ENTREPRISES AMÉRICAINES

a) « *Big Brother* fait de la sous-traitance »

Le recours par les administrations américaines aux fichiers privés pour l'accomplissement de leurs missions est une pratique établie, qui n'a fait que s'affirmer au cours des années écoulées. Ainsi, ne serait-ce qu'au niveau fédéral, le FBI, la *Ruge Enforcement Agency*, *l'Inland Revenue Service* ou encore l'*US Immigration & Naturalization Service* sont d'importants clients de sociétés dites de *Lookup Services*, dont l'activité consiste à fournir contre rémunération un accès à leurs bases de données centralisant toutes sortes d'informations sur les personnes, les sources de ces sociétés étant aussi bien des fichiers publics que des fichiers privés (*Crédit Bureaus*, sociétés de marketing, opérateurs de téléphonie, etc.) [1]. La société la plus connue en la matière est *ChoicePoint Inc.* [2], qui propose ses services tant aux sociétés privées (compagnies d'assurance et organismes de crédit, notamment) qu'aux administrations fédérales et des États pour toutes sortes de finalités (amélioration de la fourniture des services publics en matière d'application de la loi, de santé, etc., mais aussi amélioration de la gestion des embauches, notamment).

1 Ces bases sont généralement indexées en ayant recours aux numéros de sécurité sociale des personnes.
2 Voir l'offre détaillée des services de cette société sur http://www.choicepoint.com

Cette tendance, jugée préoccupante par les défenseurs de la *Privacy* aux États-Unis, s'explique par le cadre juridique applicable à la tenue de fichiers de données personnelles par les autorités publiques américaines. En effet, le *Privacy Act* de 1974, qui encadre la collecte et l'utilisation de données personnelles détenues par les administrations fédérales américaines, impose le respect d'un principe de finalité incompatible avec le fait, pour ces administrations, de collecter des données aussi variées que celles détenues par les *Lookup Services*. En ayant recours aux services de sociétés tierces, les administrations fédérales ont donc la possibilité de contourner cet obstacle juridique… tout en étant en pleine contradiction avec l'esprit de la loi. C'est ainsi qu'une étude sur le sujet titre avec humour que « *Big Brother* n'a pas disparu ; il fait juste de la sous-traitance » [1] !

Cette situation, pour étonnante qu'elle paraisse aux yeux d'un citoyen européen, pourrait pourtant presque passer pour négligeable au vu des développements législatifs qui ont suivi les dramatiques événements du 11 septembre 2001.

b) Lutte contre le terrorisme

Le *Patriot Act*, adopté le 24 octobre 2001, contient en effet une disposition, intitulée la section 215, qui autorise le FBI à exiger de toute personne physique ou morale (par exemple des bibliothèques, des fournisseurs d'accès internet, des hôpitaux, etc.) qu'elle lui produise « toute chose tangible » (y compris des fichiers automatisés) dès lors qu'il lui est précisé que cet ordre est pris dans le cadre d'une enquête de lutte contre le terrorisme international ou des activités d'espionnage. [2] En vertu de cette disposition, le FBI n'a pas besoin, pour ce faire, de démontrer qu'il existe une « cause probable » ou une raison avérée de croire que la personne sur laquelle sont effectuées des recherches a commis un acte ou a exercé des activités répréhensibles. Par ailleurs, les sociétés dont les fichiers ont fait l'objet d'un tel ordre ont l'interdiction d'en informer les personnes concernées dont les données ont pu être consultées.

C'est dans ce mouvement général de renforcement des pouvoirs des forces de l'ordre face au risque terroriste que, dans le courant de l'année 2003, une nouvelle forme d'intrusion dans la vie privée des citoyens américains par les autorités fédérales américaines a été révélée au grand public par voie de presse. Dans cette affaire, la compagnie aérienne « JetBlue » a reconnu avoir cédé à une société dénommée « Torch Concepts », sous-traitante du ministère de la Défense américain (DoD), les données personnelles d'environ 40 % de ses passagers, aux fins de tester le controversé système CAPPS II *(Computer Assisted Passenger Pre-Screening System)* [3]. « Torche Concepts » obtenait par ailleurs certaines données de la société « Acçlomate », un des principaux agrégateurs de données personnelles américains (sexe, propriétaire ou locataire de son domicile, années de résidence, revenus,

1 Glenn Simpson, « *FBI's reliance on the private sector has raised some privacy concerns* », 13 avril 2001, http://www.atgpress.com/atgpress/pri/pri004.htm

2 Voir le dossier constitué sur le sujet par l'*American Civil Liberties Union* (ACLU) : http://www.aclu.org/SafeandFree/SafeandFree.cfm ? ID=12126&c=207

3 Pour mémoire, ce système vise à centraliser dans une seule et même base les données de tous les passagers voyageant vers ou à partir des États-Unis ; il permettrait de déterminer avant le vol le « niveau de dangerosité » d'une personne sur la base d'un code couleur.

nombre d'enfants, d'adultes, numéro de sécurité sociale, profession, informations sur le véhicule, etc.) afin de les croiser avec celles obtenues de « JetBlue » (nom, adresse, numéro de téléphone, etc.) ; le sous-traitant essayait alors de déterminer en fonction de quels critères le système était susceptible de mieux distinguer les passagers « normaux » de « JetBlue » de ceux ayant potentiellement commis des actes terroristes par le passé.

La révélation de cette affaire a provoqué un tollé aux États-Unis. D'une part, en septembre 2003, *l'Electronic Privacy Center* (EPIC) a porté plainte à l'encontre de « JetBlue » devant la *Federal Trade Commission* (FTC), et ce en dépit des excuses publiques présentées par la société à ses clients. Cette procédure tend à faire juger que cette société s'était rendue coupable de pratiques commerciales trompeuses en communiquant ces informations à « Torch Concept », dans la mesure où les *Privacy Policy* de « JetBlue » et d'« Acxiom » indiquaient que ces sociétés s'engageaient à respecter la vie privée des personnes et, en particulier, à ne pas communiquer de données à des tiers.

D'autre part, une commission sénatoriale a été chargée d'enquêter sur la possible violation par le ministère de la Défense du *Privacy Act* de 1974 : cette commission, qui reconnaît la valeur de l'argument selon lequel la lutte contre le terrorisme impose de trouver de nouveaux moyens de pister les terroristes potentiels, affirme par ailleurs avec force que *« la meilleure manière d'emporter l'adhésion à des systèmes effectifs de sécurité intérieure consiste à assurer au Congrès et au public que les administrations ont pris en compte de manière appropriée l'impact de leurs mesures sur la protection de la vie privée des personnes »*.

Ultérieurement, le ministère de l'Intérieur (DHS) a relayé cette action : celui-ci, dans le cadre de ses compétences consistant à assurer la sécurité des aéroports et des compagnies aériennes, a annoncé qu'il cherchait à déterminer si de hauts fonctionnaires avaient également violé les règles de protection de la vie privée en aidant à coordonner ce projet.

Les deux volets de cette affaire étaient toujours en cours en 2004, mais il semblerait que des doutes aient été émis en plus haut lieu quant à la continuation du programme CAPPS II, en particulier pour des raisons opérationnelles et budgétaires.

B. Du public au privé : la directive sur la réutilisation des données publiques

Données publiques, données privées : si les fichiers du secteur privé peuvent être utilisés par les administrations pour leurs besoins propres, l'inverse est tout aussi vrai : la ressource que représentent les informations détenues par les administrations et organismes publics en général est tout aussi précieuse pour les sociétés du secteur privé. C'est d'ailleurs pour répondre aux problèmes spécifiques que pose cette autre problématique que l'Union européenne a adopté, courant 2003, une directive en la matière.

1. PHILOSOPHIE GÉNÉRALE DE LA DIRECTIVE

Le 17 novembre 2003 a été adoptée la directive du Parlement et du Conseil concernant la réutilisation des données du secteur public. Cette directive, fondée sur une proposition de la Commission de juin 2002, vise à une harmonisation minimale des règles régissant la réutilisation des données du secteur public au sein de l'Union européenne. En effet la possibilité de réutiliser de telles données (par exemple, des données de nature sociale, géographique, commerciale, touristique, météorologique, routière, mais encore des informations sur les entreprises, les brevets, l'enseignement, etc.), originellement collectées pour l'accomplissement de missions de service public, revêt un intérêt économique de première importance : ces données constituent la matière première de nombreux produits et services numériques. Il y a donc là un potentiel énorme de développement de certaines activités de commerce électronique.

Or la volonté de créer un marché unique offrant des conditions favorables au développement de tels services au niveau européen se heurte à différents facteurs, et notamment aux règles et pratiques des États membres en matière d'exploitation des informations du secteur public. En effet, les traditions nationales en la matière ont été fortement divergentes ; selon les cas la réutilisation des informations publiques est ainsi plus ou moins aisée (en particulier du fait de l'existence de monopoles de service public, d'accords d'exclusivité pour la diffusion de ces données, etc.). Or, à l'heure de la numérisation et de la diffusion sur internet de ces produits et services, l'écart existant en la matière risquait de se creuser davantage entre les pays de l'Union européenne : il importait dès lors d'harmoniser les règles en la matière, afin d'assurer notamment que les conditions de réutilisation de ces données soient équitables, proportionnées et non discriminatoires.

C'est ainsi que cette directive impose, par exemple, que le coût financier de cette réutilisation soit raisonnable ; que soient fixés des délais raisonnables de réponse à toute demande de réutilisation ; que l'objectif de facilitation de cette réutilisation ait pour effet que les organismes du secteur public mettent leurs documents à la disposition du public dans tous les formats et toutes les langues existantes, et que ces formats ne soient pas, dans la mesure du possible, liés à l'utilisation d'un logiciel spécifique, etc.

2. IMPACT SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Les données à caractère personnel ne constituent pas, à l'évidence, l'objet principal de la directive. Toutefois, certaines données publiques sont des données à caractère personnel susceptibles d'être réutilisées pour de nouvelles finalités, comme par exemple des données issues de registres d'état civil, du commerce, d'immatriculation ou de crédit ou encore des données médicales, professionnelles ou sociales. À cet égard, la directive du 17 novembre 2003 prévoit explicitement que la directive 95/46 du 24 octobre 1995 est entièrement d'application lorsque des données à caractère personnel, font l'objet d'une demande de réutilisation.

C'est à ce titre, et en vertu de l'article 30 de la directive 95/46/CE, qui prévoit que le groupe de l'article 29 peut formuler des recommandations sur toutes les questions concernant la protection des données à caractère personnel au sein de la Communauté, qu'a été adopté l'avis 7/2003 sur la réutilisation des données émanant du secteur public et la protection des données à caractère personnel [1].

Le groupe était déjà intervenu sur le sujet à l'occasion en 1999 [2]ainsi que de manière connexe en 2001 [3] ; le nouveau document du groupe, qui doit dès lors être lu à la lumière de ces précédents documents, ne fait que confirmer les grandes lignes de la doctrine dégagée antérieurement sur ce sujet par le groupe — doctrine par ailleurs parfaitement conforme à celle appliquée par la CNIL depuis de nombreuses années.

PRINCIPE FONDAMENTAL : DES DONNÉES PERSONNELLES RENDUES PUBLIQUES RESTENT DES DONNÉES PERSONNELLES

Une première règle, rappelée avec force par le groupe, est que les données à caractère personnel contenues dans un document officiel, ou détenues par une administration ou un organisme public et qui auraient été rendues publiques conservent ce caractère personnel ; elles doivent donc, à ce titre, être protégées conformément à la législation de protection des données à caractère personnel. Dès lors, la communication à des tiers de données à caractère personnel collectées et détenues par des organes du secteur public doit être considérée comme un traitement de données à caractère personnel, et le respect des règles de la directive s'impose pour cette communication comme pour n'importe quel autre traitement.

LÉGITIMATION DU TRAITEMENT

Le groupe rappelle que le traitement de données à caractère personnel consistant à communiquer des données sur demande doit être légitimé en vertu de l'article 7 de la directive : cette communication doit par exemple avoir été acceptée par la personne concernée au moment de la collecte initiale des données ou au moment où leur réutilisation est envisagée ; cette communication peut aussi être requise pour se conformer à une obligation juridique, par exemple.

ANALYSE DE LA COMPATIBILITÉ DES FINALITÉS DU TRAITEMENT ORIGINAL ET DE LA RÉUTILISATION

Par ailleurs, les principes liés à la qualité des données, et en particulier le principe de finalité, méritent une attention particulière dans ce contexte. En vertu de ce principe prévu à l'article 6 de la directive, les données à caractère personnel doivent ainsi être « *collectées pour des finalités déterminées* [...] *et ne pas être traitées*

1 Avis 7/2003 sur la réutilisation des données émanant du secteur public et la protection des données à caractère personnel — trouver le juste milieu, 12 décembre 2003, disponible sur le site du groupe à l'adresse suivante : http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp83_fr.pdf

2 Avis 3/99 sur les informations du secteur public et la protection des données à caractère personnel — contribution à la consultation lancée par la Commission européenne dans son « Livre vert » intitulé *L'information émanant du secteur public : une ressource clef pour l'Europe* COM (1998) 585, 3 mai 1999.

3 Avis 5/2001 sur le rapport spécial du médiateur européen à l'attention du Parlement européen faisant suite au projet de recommandation adressé à la Commission européenne dans la plainte 713/98/IJH, 17 mai 2002.

ultérieurement de manière incompatible avec ces finalités ». Dès lors c'est en fonction de l'interprétation de la notion de « finalités compatibles ou incompatibles » qu'il sera possible de décider, selon les cas, si la communication de données personnelles détenues par des organismes du secteur public est légale ou non, en vertu des dispositions de la directive 95/46.

L'évaluation de la compatibilité de la finalité du traitement initial avec la finalité de la réutilisation des données constitue, de toute évidence, un exercice difficile, qui exige de prendre en compte différents facteurs (nature des données, des destinataires, finalité du traitement original, etc.). Le document du groupe fournit quelques éléments de réflexion à cet égard, mais précise que cette analyse ne peut, en pratique, être faite qu'au cas par cas.

Un cas particulier concerne l'évaluation de ces finalités compatibles en cas d'exploitation commerciale des données par la personne formant la demande de réutilisation. En effet, le risque réside alors dans le fait que les organes du secteur public puissent être tentés de chercher à utiliser les informations obtenues à des fins spécifiques pour des finalités non-compatibles, dans le seul but d'en retirer des contreparties financières. La règle est celle d'une incompatibilité de principe entre la finalité d'un traitement original effectué par un organisme public et la réexploitation des données en cause pour des fins commerciales, notamment de marketing direct. C'est ainsi, par exemple, que la loi française interdit l'exploitation purement commerciale des listes électorales. Dans certains cas, toutefois, cette réutilisation commerciale des données publiques peut être envisageable quand cette possibilité est expressément envisagée par la loi. Il est alors impérieux que des garanties spécifiques soient mises en place, telles que, par exemple, la possibilité pour les personnes de s'opposer à cette réutilisation.

DROITS DES PERSONNES CONCERNÉES

Enfin, dans son avis, le groupe rappelle également l'exigence d'information des personnes concernées de l'éventuelle réutilisation de leurs données personnelles. En effet, seule cette information met les personnes en mesure d'exercer leurs droits, notamment le droit d'exiger une rectification des données erronées ou le droit de s'opposer au traitement de leurs données à des fins commerciales et de marketing direct.

La délicate articulation des règles de protection des données personnelles avec le principe de réutilisation des données détenues par des organismes publics fournit un nouvel exemple de la difficile conciliation de ces premières règles avec celles, de valeur tout aussi fondamentale, relatives au droit des personnes à avoir accès à l'information détenue par les organismes publics. Il revient régulièrement à la CNIL, comme aux autres autorités de protection des données personnelles à travers le monde, de se pencher sur cette problématique générale. Celle-ci l'a ainsi conduite à réfléchir, par exemple, sur l'utilisation qui pouvait être faite d'informations personnelles contenues dans les annuaires, mais aussi sur les listes électorales ou encore sur le problème de la publication en ligne des décisions de justice.

Toutes ces oppositions entre ces deux ordres de règle ne peuvent bien évidemment être tranchées de la même manière. Chaque nouveau conflit entre eux

impose de rechercher, inlassablement, un équilibre qui soit conforme aux souhaits et aux intérêts des citoyens. S'il est un principe, toutefois, qui doit dominer tous ces débats, c'est celui selon lequel le législateur, lorsqu'il souhaite qu'une donnée soit rendue accessible au public, n'entend pas pour autant qu'elle devienne une *res nullius* qui ne bénéficierait désormais plus de la protection que la loi garantit à la personne concernée en vertu des principes fondamentaux de défense de l'identité humaine. C'est dans cet esprit que la CNIL œuvre pour régler ces situations de conflit, afin que l'exercice d'un droit par une personne ne soit pas conditionné par le renoncement à un droit alternatif par autrui.

Chapitre 4

LE MAIRE, L'INFORMATICIEN ET LE CITOYEN

L'informatique municipale connaît des évolutions importantes. Si aujourd'hui la plupart des communes ont informatisé les principaux services, le développement des nouvelles technologies de l'information, et en particulier d'internet, leur permet désormais de concevoir l'informatique, non plus seulement, dans une approche traditionnelle, comme un simple outil de gestion mais comme le moyen — en particulier par l'interactivité qu'elle offre — de (re) nouer une relation plus personnalisée avec le citoyen. Sites internet, téléservices, bornes d'information interactives, cartes de vie quotidiennes… l'administration électronique ouvre sans aucun doute la possibilité de rapprocher le citoyen de sa mairie, de développer une administration de proximité plus transparente et davantage à l'écoute des préoccupations de chacun.

Ces évolutions ne relèvent pas seulement d'une perspective technologique ; elles contribuent, dans le mouvement des réformes de la décentralisation, à replacer le citoyen au cœur de l'action municipale et sans doute à « repenser » en conséquence les missions de l'administration communale de demain, plus encline à vouloir mieux connaître la situation individuelle de chacun de ses administrés. Aussi de telles évolutions appellent-elles une réflexion toute particulière sur le terrain de la protection des données à caractère personnel. La mairie, parce qu'elle est au centre des démarches administratives que tout citoyen est amené à accomplir au cours de sa vie est en effet conduite naturellement, à recueillir et à conserver des informations sur lui. Le maire, comme pour les nombreuses autres législations ou réglementations relevant de ses compétences, est responsable du respect, dans sa commune, de la loi « informatique et libertés » du 6 janvier 1978. L'application de la loi peut, dès lors, apparaître comme une contrainte supplémentaire. Pourtant la prise en compte des règles de protection des données est avant tout un facteur de transparence envers les citoyens et un gage de sécurité juridique pour les élus.

Consciente de la nécessité de mieux faire connaître, dans ce secteur, la loi « informatique et libertés » et soucieuse d'apporter aux responsables municipaux des réponses concrètes et adaptées aux réalités de l'action municipale, la Commission a entendu évaluer en ce domaine les modalités d'application de la loi et mesurer les difficultés rencontrées. Dans cette optique, une délégation de la Commission s'est rendue, au cours de l'année 2003, dans une dizaine de communes de plus de 15 000 habitants [1] afin de dresser un premier état des lieux. Un rapport d'étape sur « L'application par les communes de la loi informatique et libertés », s'appuyant sur les constats effectués lors de ces visites, a été adopté le 9 décembre 2003. Il rappelle un certain nombre de principes clés de la protection des données et prend position sur des questions plus spécifiques d'application de la loi.

Les maires ont besoin de connaître avec précision leurs administrés. La multiplication des fichiers spécifiques est une réponse. L'exploitation des données d'un recensement constamment réactualisé en est une autre, souvent complémentaire, parfois alternative. À la veille du démarrage du « nouveau recensement » qui met fortement à contribution les communes, la CNIL a poursuivi son travail d'analyse de ses conditions de réalisation.

I. L'APPLICATION DES PRINCIPES DE PROTECTION DES DONNÉES PERSONNELLES PAR LES COMMUNES

Les élus et les personnels des collectivités locales rencontrent parfois de réelles difficultés à appliquer la loi informatique et libertés voire même à en mesurer toutes les exigences. Certaines mairies doivent cependant être saluées pour leur souci du respect de la loi. Cette sensibilité particulière aux principes de protection des données paraît pour beaucoup résulter de la formation qu'ont pu recevoir sur ce sujet les responsables informatiques ou les directeurs généraux des services. De même, il convient de souligner l'attachement à la confidentialité des données dont font tout particulièrement preuve les personnels municipaux œuvrant dans le domaine social.

Plusieurs principes-clés peuvent être ainsi dégagés à la lumière des missions menées ainsi que quelques lignes d'action.

1 Aix-en-Provence, Carpentras, Clichy-sous-Bois, Goussainville, Hautmont, La Rochelle, Le Mans, Tarascon, Vaulx-en-Velin, Villeparisis.

A. Les principes-clés

1. LE MAIRE, RESPONSABLE DE L'APPLICATION DE LA LOI « INFORMATIQUE ET LIBERTÉS »

Au regard de la loi « informatique et libertés » les fichiers informatiques mis en œuvre dans la commune relèvent de la responsabilité du maire. Il ne peut se décharger de cette responsabilité ni sur les prestataires techniques ni sur les établissements de coopération.

a) Les prestataires informatiques

Les progiciels proposés par les prestataires informatiques doivent être conformes à la législation en vigueur et adaptés tant aux besoins réels des utilisateurs qu'à l'évolution des textes.

Les prestataires de services informatiques, lorsqu'ils proposent leurs logiciels aux communes, affirment parfois que leurs produits bénéficient d'un agrément de la CNIL ou même d'un « label CNIL ». Les responsables municipaux rencontrés sont dès lors enclins à penser être en règle avec la loi du 6 janvier 1978. Or, un tel agrément ou label n'existe pas. Si certains prestataires informatiques consultent les services de la Commission avant de commercialiser les progiciels notamment afin de pouvoir ensuite assister leurs clients dans l'accomplissement de leurs démarches déclaratives auprès de la CNIL, il ne peut y avoir de régime particulier pour ces produits.

En revanche, le devoir de conseil des prestataires reste fondamental afin d'aider les responsables municipaux à opérer les choix déterminants qui leur reviennent (telle que l'évaluation précise des objectifs recherchés par l'informatisation du service ou encore les mesures de sécurité informatique à mettre en œuvre…).

b) Les EPCI

La mise en œuvre de fichiers par les établissements publics de coopération intercommunale (EPCI) est parfois également source de confusion quant à la détermination du responsable juridique de ces fichiers, au regard de la loi du 6 janvier 1978. Tel est le cas lorsque la commune et l'EPCI disposent d'un service informatique commun ou encore lorsque des applications développées par l'EPCI sont accessibles en ligne aux communes de son territoire de compétence.

Si l'EPCI intervient exclusivement comme prestataire technique de la commune, seule la commune reste responsable du fichier et doit en conséquence le déclarer auprès de la CNIL. Il en est ainsi par exemple si la gestion technique du fichier du personnel d'une commune est confiée à la direction informatique d'un EPCI qui agit alors comme sous-traitant, la responsabilité du fichier continuant de reposer sur le maire. Si, en revanche, l'EPCI, dans le cadre d'un transfert de compétences, s'est vu confier la gestion administrative du service des ressources humaines de la commune et à cet effet la tenue du fichier du personnel (tel était le cas pour une des communes visitées), la responsabilité de ce traitement reposera sur le président de l'EPCI.

Par conséquent, les statuts de l'EPCI [1] doivent explicitement prévoir que les transferts de compétences entraînant transferts de fichiers nominatifs conduisent à transmettre à cet établissement public la responsabilité de ces fichiers et notamment à effectuer les déclarations nécessaires auprès de la CNIL.

En définitive, la collectivité territoriale responsable du fichier, au regard de la loi du 6 janvier 1978, est celle qui a le pouvoir d'en déterminer les finalités et les moyens [2].

2. LE CONTENU DES FICHIERS MUNICIPAUX LIMITÉ AUX SEULES DONNÉES PERTINENTES

La question de la pertinence des données collectées par les services municipaux au regard des finalités du fichier est au cœur de la loi « informatique et libertés ».

Les progiciels mis en œuvre au sein des mairies comportent parfois des champs d'informations à remplir largement excessifs au regard des renseignements dont ont réellement besoin les services municipaux. Les prestataires informatiques peuvent ainsi être à l'origine de collectes de renseignements inutiles, au surplus sans que les utilisateurs aient la possibilité technique de supprimer les zones concernées. À l'inverse, les progiciels proposés ne permettent pas toujours aux services municipaux d'enregistrer les données avec le degré de précision souhaité. Il en est ainsi, par exemple, de situations familiales complexes pour les inscriptions scolaires (il est parfois difficile de préciser l'exacte qualité du nouveau mari ou compagnon de la mère d'un enfant parfois inscrit à tort comme « père »).

Même s'il a pu être constaté que les services municipaux ne faisaient en général qu'un usage limité des outils informatiques mis à leur disposition par rapport aux larges potentialités qui leur sont cependant souvent offertes, ils peuvent aussi être enclins à collecter et enregistrer plus de données qu'il n'est nécessaire.

Ainsi en est-il du numéro de Sécurité sociale enregistré dans les dossiers de demandes de logements sociaux et dans les traitements des inscriptions scolaires, ces derniers contenant, en outre, fréquemment, les coordonnées de l'employeur [3], le détail des revenus du foyer (alors même que seul le résultat du calcul du quotient familial est durablement utile), sans que cela soit toujours justifié, ni conforme aux prescriptions de la loi du 6 janvier 1978.

Seules les informations adéquates, pertinentes et non excessives au regard de la finalité du fichier doivent être collectées et enregistrées. Les logiciels proposés aux collectivités locales doivent, par conséquent, être adaptés à leurs besoins réels et

1 Dans le cadre, en particulier, de la loi n° 99-586 du 12 juillet 1999 relative au renforcement et à la simplification de la coopération intercommunale.

2 Comme le précise l'article 2 d) de la directive communautaire du 24 octobre 1995.

3 Cette information est enregistrée d'une part pour faciliter le recouvrement d'éventuelles créances impayées (*cf. infra* II/ position de la CNIL sur les demandes de renseignements des tiers) et d'autre part, pour prévenir les parents sur leur lieu de travail en cas d'urgence. Dans ce dernier cas, il suffirait d'indiquer les coordonnées de la personne à prévenir.

être paramétrables simplement afin de permettre l'enregistrement des seules données réellement nécessaires. La Commission entend engager une action en ce sens auprès des principaux prestataires informatiques.

3. UNE DURÉE DE CONSERVATION DES DONNÉES DÉFINIE

Dans l'ensemble des mairies visitées, la détermination précise des durées de conservation des données enregistrées dans les traitements était en général insuffisante. Le plus souvent, les données sont conservées aussi longtemps que les moyens informatiques le permettent et ce n'est que lorsque les micro-ordinateurs deviennent moins performants qu'un apurement est opéré.

La Commission a ainsi pu constater que le service des ressources humaines d'une commune détenait un fichier récapitulant les agents depuis 1891 (avec le numéro de Sécurité sociale depuis l'apparition de ce dernier). Dans un autre domaine, un système de contrôle d'accès pour les résidents d'une zone piétonne conservait sans utilité réelle pendant un mois toutes leurs allées et venues (dates, heures de passage et immatriculations).

De même, dans le cadre de la procédure de délivrance des cartes nationales d'identité ou de passeports, où les communes jouent un rôle d'intermédiaire entre les administrés et la préfecture ou sous-préfecture territorialement compétente, les services municipaux conservent parfois sous forme informatisée un registre nominatif recensant l'identité et les coordonnées du demandeur afin d'assurer le suivi administratif des demandes de titres. Une fois le titre remis à son titulaire, ces données n'ont pas lieu d'être conservées en informatique.

Par conséquent, la CNIL a rappelé que les données nominatives informatisées ne peuvent être conservées de façon indéfinie. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier (par exemple, un mois pour les enregistrements de vidéosurveillance, deux ans à compter de la dernière aide pour le fichier d'aide sociale, un an après le dernier contact avec l'intéressé pour le fichier des demandeurs d'emploi...). Au-delà, les données doivent être archivées dans les conditions définies par la loi du 3 janvier 1979 sur les archives c'est-à-dire sur des supports indépendants et en dehors de l'application informatique elle-même.

B. Les lignes d'action

1. PENSER À LA SÉCURITÉ INFORMATIQUE

Un autre constat important des missions effectuées est l'insuffisante sécurité des systèmes informatiques municipaux. La conscience de l'importance et de la confidentialité des données est très variable d'une collectivité à une autre ainsi que leur degré de sensibilité.

La gestion des mots de passe est ainsi quasi inexistante : il est fréquent que les mots de passe permettant d'accéder aux informations soient trop simples (nom, prénom ou initiales de l'agent, abréviations répandues correspondant à des

fonctions, etc.), leur nombre de caractères est souvent limité et ils ne sont pas renouvelés régulièrement. Les mots de passe sont souvent partagés par plusieurs personnes au sein d'un même service, et en cas d'absence temporaire du titulaire habituel du poste, confiés, sans autre formalisme, aux remplaçants. De plus, des mesures de sécurité simples, telles que la fermeture des logiciels lors des pauses des personnels, sont assez peu appliquées. La hiérarchisation des accès en fonction des habilitations des agents est rarement mise en œuvre de même que les dispositifs de journalisation des connexions.

Au demeurant, les accès internet et extranet sont de nature, d'une part à fragiliser les systèmes d'information qui se voient ainsi exposés à d'éventuelles tentatives d'intrusion, d'autre part à « ouvrir » plus que nécessaire les accès aux fichiers gérés par les différents services municipaux.

Les responsables municipaux doivent veiller à ce que leurs personnels mettent en œuvre et appliquent, de manière effective, les mesures de sécurité informatique tout particulièrement lorsqu'il s'agit de systèmes informatiques en réseau et « ouverts ». Il est également essentiel que des mesures de protection logicielles permettent de restreindre l'accès des applications aux seuls personnels habilités, en raison de leurs fonctions, à en connaître.

Cette situation n'est pas propre au secteur des collectivités locales. Cependant, l'informatique communale se développe dans un contexte social et technique dans lequel les risques de piratage et d'intrusion dans les systèmes informatiques s'accroissent et doivent, eu égard aux conséquences qui pourraient résulter pour les élus de la divulgation de tel ou tel fichier, être particulièrement pris en compte par les municipalités.

Or, en cas de divulgation des données, la responsabilité des élus et des personnels communaux pourrait être engagée, tant dans l'exploitation politique ou médiatique qui pourrait en être faite qu'éventuellement sur le plan pénal.

Les communes visitées ne sont, cependant, pas égales à cet égard. Les grandes villes, parce qu'elles disposent des moyens matériels et humains nécessaires, ont parfois élaboré une véritable politique de sécurité. En outre, les personnels des centres communaux d'action sociale et des services de vaccination, quelle que soit la taille de la commune, ont sans doute plus que d'autres services le souci d'assurer la confidentialité des informations qui leur sont confiées. Disposant de moyens informatiques dédiés, ils ont généralement mis en œuvre des procédures plus rigoureuses de contrôle d'accès aux fichiers sociaux.

Les missions menées par la CNIL dans les communes visitées ont cependant suscité de réelles mobilisations sur ce sujet et des améliorations significatives des dispositifs et pratiques de sécurité ont depuis été engagées.

L'élaboration d'une charte de sécurité, adoptée en associant étroitement l'ensemble des personnels, revêt, par ailleurs, un intérêt particulier pour sensibiliser les utilisateurs sur les risques potentiels et les mesures de sécurité à prendre individuellement et collectivement.

2. INFORMER LES USAGERS SUR LEURS DROITS

La CNIL a reçu, en 2003, plusieurs réclamations de particuliers s'étonnant du contenu d'un questionnaire nominatif que la mairie de leur domicile leur demandait de compléter et de retourner en mairie. Ces questionnaires avaient la plupart du temps pour objet de permettre à la mairie d'évaluer les attentes de la population en matière d'infrastructures publiques (jardins, salles de sport, etc.). Ces personnes souhaitaient connaître la régularité d'une telle manière de procéder et l'étendue de leurs droits.

La CNIL a dû intervenir auprès de plusieurs collectivités locales afin de leur rappeler que les questionnaires adressés aux administrés doivent comporter les mentions d'information, notamment l'existence de leur droit d'accès et de rectification ainsi que les destinataires des données recueillies, prévues par l'article 27 de la loi du 6 janvier 1978.

Les visites sur place ont permis de constater que l'information des usagers sur les droits qui leur sont reconnus au titre de la loi du 6 janvier 1978 était assez rarement mise en œuvre. Dans la plupart des cas, les formulaires ou fiches de renseignement diffusés par les services municipaux ne comportent aucune des mentions légales prévues par l'article 27 de la loi (caractère obligatoire ou facultatif des réponses, conséquences d'un défaut de réponse, destinataires des informations, existence d'un droit d'accès et de rectification).

En outre, peu de services ont apposé dans les locaux ouverts au public des affiches informant les personnes de l'existence d'un fichier, manuel ou automatisé, et des droits qui leur sont reconnus, alors même que la CNIL propose des modèles d'affiches. Cette obligation légale est parfois ressentie comme purement formaliste dans la mesure où les administrés constatent, quand ils se déplacent, que leurs données sont informatisées.

Une information claire et précise des usagers en particulier sur les droits qui leur sont ouverts au titre de la loi de 1978 ne peut que contribuer à instaurer un climat de transparence et de confiance entre les élus et leurs administrés. De même, l'indication systématique de l'origine des informations utilisées pour adresser un courrier aux habitants de la commune est de nature à apaiser toute suspicion sur l'existence d'éventuels fichiers constitués à l'insu des personnes.

Les choix informatiques de la commune peuvent faire l'objet d'une communication municipale pour informer ainsi clairement les usagers des garanties prises pour assurer la protection de leurs données et le respect de leur vie privée, tout particulièrement lorsqu'il s'agit d'applications sensibles faisant appel à des technologies potentiellement intrusives (vidéosurveillance, biométries...).

3. DÉCLARER TOUS LES FICHIERS DE LA COMMUNE

Loin de répondre à de seules exigences purement formelles, la procédure de déclaration des fichiers à la CNIL permet au maire, avec l'appui de ses services, d'avoir une vue synthétique de l'informatique municipale. Les élus disposent ainsi

d'un inventaire précis de tous les fichiers informatiques mis en œuvre dans la commune, ce qui doit leur permettre d'éviter les développements « spontanés » d'applications. À cet égard, les personnels municipaux amenés à créer de leur propre initiative des fichiers doivent en informer leur hiérarchie et cette obligation doit leur être rappelée à intervalles réguliers.

Par ailleurs, la prise en compte, par les responsables municipaux, des règles de protection des données à caractère personnel, présente l'avantage de les inciter, lors de la conception de l'application informatique ou du choix du logiciel, à déterminer précisément la nature et les conditions d'utilisation des informations à enregistrer, les personnes ou services en ayant un réel besoin. Les mesures prises pour assurer la confidentialité des informations et les modalités d'information des administrés (par exemple, sous la forme d'une publication régulière dans le journal municipal ou encore sur le site internet de la commune) permettront, à cette occasion, d'assurer la transparence de l'informatique de la commune.

Les visites effectuées auprès des mairies ont souvent révélé la mise en œuvre de traitements automatisés d'informations nominatives, sans que les formalités déclaratives requises au titre de la loi du 6 janvier 1978 aient été accomplies. Ces formalités préalables sont pourtant un moyen pour les maires de conserver la maîtrise de l'informatique municipale.

La Commission met à disposition des collectivités locales un guide pratique leur donnant toutes indications utiles sur les modalités de déclaration et permettant au maire de veiller à la déclaration des fichiers communaux.

II. DES ENJEUX SPÉCIFIQUES POUR LES COMMUNES

Au-delà des difficultés générales d'application de la loi, élus et personnels territoriaux sont également confrontés à des questions spécifiques qui touchent, à des degrés divers, à la protection des données personnelles.

A. La communication municipale

Dans le souci d'informer plus complètement les habitants de la commune sur la vie municipale, les communes désirent légitimement développer des actions de communication plus personnalisées, en particulier envers les nouveaux arrivants ou encore en direction de certaines catégories de population telles que les personnes âgées. À cet effet, elles souhaitent savoir dans quelles conditions les fichiers municipaux peuvent ou non être utilisés.

1. L'UTILISATION DES FICHIERS D'ÉTAT CIVIL

En tant qu'officiers d'état civil, le maire ou ses adjoints sont tenus de dresser actes des naissances, mariages et décès afin de leur conférer un caractère authentique et de les transcrire dans des registres. La tenue des registres d'état civil constituant une obligation pour les maires, les administrés ne peuvent donc s'opposer à ce que les informations nécessaires à la rédaction d'un acte fassent l'objet d'un traitement informatique.

La question se pose, en revanche, de l'utilisation des informations recueillies lors de l'établissement de l'acte pour publication dans la presse locale ou dans le bulletin municipal des avis de décès ou de mariage ou encore pour des actions de communication personnalisée envers les administrés notamment aux fins d'envoi de messages de félicitations à l'occasion d'une naissance ou d'un mariage, ou de condoléances lors d'un décès. Si certaines mairies demandent l'accord des personnes concernées avant toute utilisation des données à des fins « secondaires », la publication des événements familiaux dans la presse et leur utilisation par les élus se font parfois sans information des intéressés.

La Commission considère que les informations recueillies pour assurer la tenue du registre de l'état civil ne peuvent être utilisées à d'autres fins, notamment de communication personnalisée (envoi de félicitations à l'occasion d'une naissance par exemple) que dans la mesure où lors de l'établissement de l'acte d'état civil ou de sa transmission à la mairie de résidence, les personnes concernées ont la possibilité de refuser toute publication et tout envoi de messages personnalisés [1].

2. L'UTILISATION DE LA LISTE ÉLECTORALE

Aux termes de l'article L. 28 second alinéa du Code électoral, tout électeur, tout candidat, tout parti ou groupement politique peut prendre communication et copie de la liste électorale. L'article R. 16, troisième alinéa, du même Code subordonne la communication de la liste électorale aux électeurs qui en feraient la demande à la condition qu'ils s'engagent à ne pas en faire un usage purement commercial. En tout état de cause, toute question concernant la communicabilité de la liste électorale relève, depuis la loi du 12 avril 2000, de la compétence de la Commission d'accès aux documents administratifs (CADA).

Un maire peut donc utiliser la liste électorale pour adresser des courriers aux administrés, par exemple, le bulletin de la commune. Il serait utile, dans une telle hypothèse, d'assurer une transparence sur l'origine des informations utilisées [2] et de permettre aux destinataires de faire supprimer, s'ils le souhaitent, leurs coordonnées du fichier constitué à cet effet. Un tel fichier doit faire l'objet de formalités préalables de déclaration auprès de la CNIL, contrairement aux copies de la liste électorale utilisées à des fins de diffusion de la propagande électorale.

1 L'égalité entre tous les élus devant être assurée.

2 Ainsi que la CNIL l'a préconisée à diverses reprises s'inspirant en cela des principes de protection des données à caractère personnel relatifs à la loyauté de la collecte et au droit à l'information sur l'origine des données.

En ce qui concerne les conditions d'utilisation de la liste électorale, il faut rappeler que :
— Les tris informatiques opérés sur la consonance des noms des personnes, qui sont susceptibles de faire apparaître les origines raciales ou les appartenances religieuses des intéressés, qu'elles soient réelles ou supposées, sont interdits en application de l'article 31 de la loi du 6 janvier 1978 ;
— de même un tri informatique du lieu de naissance des personnes à partir de la liste électorale n'est pas justifié au regard du principe de finalité de la liste électorale qui ne comporte une telle information qu'afin de s'assurer de l'identité de l'électeur et d'éviter les fraudes au scrutin. La Commission estime qu'un tel tri n'est pas conforme à la loi comme elle l'a précisé lors de sa délibération n° 03-030 du 27 mai 2003 portant sur une demande présentée par une collectivité locale et visant à assurant la promotion de la collectivité auprès des personnes originaires de cette dernière mais n'y résidant pas.

B. Les renseignements demandés par des organismes tiers

1. LES DEMANDES DE RENSEIGNEMENTS

Les communes qui ont été visitées par la CNIL sont confrontées à un afflux massif de demandes de renseignements au sujet de leurs administrés. Les administrations et organismes à l'origine de ces sollicitations sont très divers : Trésor public, URSSAF, caisses d'allocations familiales, caisses de retraites, mutuelles, EDF/GDF, opérateurs téléphoniques, établissements de crédits, compagnies d'assurances, notaires, avocats, huissiers de justice... Dans la plupart des cas, la demande porte sur l'adresse de la personne ou son décès éventuel mais peut également concerner les références bancaires, la situation familiale, la profession, les revenus, etc.

Les collectivités locales ont de grandes difficultés à distinguer parmi ces demandes celles qui sont fondées de celles qui ont un caractère abusif. Cela génère une grande incertitude juridique pour les élus et des coûts de traitement ou de réponse non négligeables.

De telles demandes soulèvent des difficultés tant dans le fonctionnement quotidien des collectivités qu'au regard des dispositions de la loi du 6 janvier 1978. Aux termes des articles 19 et 29 de la loi, les informations nominatives figurant dans un fichier ne peuvent en effet être communiquées qu'aux destinataires énumérés dans le dossier de demande d'avis ou la norme simplifiée de référence et aux tiers autorisés à en connaître en vertu d'une disposition législative.

Même pour ces dernières, la CNIL considère que les organismes autorisés par la loi à exercer un droit de communication (appelés plus communément « tiers autorisés ») [1] ne doivent faire appel aux services des communes que de façon subsidiaire,

1 La liste de ces organismes est disponible dans la fiche n° 14 « Les conditions de délivrance de renseignements sur les administrés » du guide thématique *Collectivités locales* accessible sur le site (www.CNIL.fr) rubrique « approfondir » puis « dossiers ».

c'est-à-dire seulement si leur propre recherche d'informations dans leurs fichiers internes est restée infructueuse.

La Commission rappelle, dans un souci de clarification, que la communication à un tiers de renseignements sur un administré ne peut être effectuée qu'à titre exceptionnel et que si un texte législatif autorise le demandeur à solliciter la commune. La demande doit être ponctuelle et écrite, elle doit préciser le texte législatif sur lequel elle se fonde, et ne concerner qu'une personne nommément désignée, sans jamais porter sur un fichier ou une partie d'un fichier.

Les particuliers, les caisses de retraite ou des sociétés privées, telles que les organismes de recouvrement de créances ou organismes de crédit, ne sont, en principe, pas juridiquement fondés à obtenir communication de renseignements nominatifs contenus dans les fichiers municipaux.

Aux termes de l'instruction générale de l'état civil, les copies ou extraits d'actes d'état civil peuvent toutefois être obtenus dans les conditions fixées par ce texte. Il doit cependant ne s'agir là encore que d'une demande ponctuelle sur une personne identifiée et non d'une demande de consultation de l'ensemble d'un registre ou de copies d'actes de toutes les personnes y figurant. Seule la consultation des registres de l'état civil datant de plus de cent ans est libre (article 7-3 de la loi du 3 janvier 1979 sur les archives). Les personnes effectuant des recherches généalogiques ne peuvent en conséquence avoir accès aux registres d'état civil que dans les conditions précitées [1].

La Commission appelle l'attention des responsables locaux sur le fait que les mairies ne peuvent, pour le renseignement des tiers autorisés, notamment les services du ministère des Finances à l'origine de nombreuses demandes, constituer des fichiers ou collecter systématiquement et de manière préventive des informations. Seules les informations figurant déjà dans les fichiers, manuels ou informatisés, détenus par les mairies peuvent être communiquées aux tiers autorisés. L'exercice du droit de communication sur place ne peut se traduire par un accès à l'ensemble d'un fichier.

Dans la mesure où les demandes de renseignements devraient rester exceptionnelles, il n'est pas nécessaire que les personnels chargés de répondre à ces demandes bénéficient d'accès permanents aux fichiers municipaux. [2]

Il peut paraître légitime que le Trésor public puisse demander à la mairie, en sa qualité d'ordonnateur, de préciser les indications fournies sur les débiteurs de la commune et, à ce titre, celle-ci doit pouvoir procéder à des recherches complémentaires. Toutefois, il ne s'agit pas de l'exercice d'un droit de communication au profit du Trésor public.

1 Les mairies sont souvent sollicitées par des demandes pressantes de professionnels ou de particuliers désireux d'accéder, pour des recherches généalogiques, à des actes ou des registres qui ne sont pas encore légalement communicables.

2 Les fichiers des centres communaux d'action sociale (CCAS), qui sont des entités juridiques distinctes de la mairie, ne peuvent être utilisés pour répondre à des demandes de renseignements adressées aux communes. En revanche, les CCAS peuvent être sollicités de manière spécifique conformément aux dispositions relatives au droit de communication.

Les demandes de renseignements et les réponses apportées ne peuvent être conservées, le cas échéant, qu'aux seules fins de suivi et d'archivage des demandes traitées. Le traitement des données n'a pas à donner lieu à la constitution ou à l'alimentation d'un fichier nominatif.

2. LES ENQUÊTES RÉALISÉES POUR LE COMPTE D'ORGANISMES EXTÉRIEURS

Les communes peuvent être tentées, pour répondre à des demandes d'organismes extérieurs, de diligenter des enquêtes. Certaines communes disposent ainsi de véritables services d'enquêtes [1], composés de plusieurs agents, où sont parfois installés des postes de travail permettant de consulter différents fichiers (fichier électoral, fichier des abonnés au service des eaux, etc.). Si l'information demandée n'est pas disponible sur ces fichiers ou doit être vérifiée, le service dépêche l'un de ses agents sur le « terrain » pour enquêter auprès des voisins, du gardien, du propriétaire, etc. Ces services conservent parfois les renseignements obtenus sur les administrés dans des fichiers manuels ou informatisés. Dans l'hypothèse où les informations recueillies sont conservées, sous forme manuelle ou informatisée, il arrive fréquemment qu'elles soient consultées par les services de police ou de gendarmerie.

En aucun cas, ces enquêtes ne sont assimilables aux recherches d'informations que peuvent légitimement réaliser les mairies pour leurs besoins de gestion interne (recherche des personnes dont les cartes d'électeurs n'ont pas pu être distribuées par La Poste, enquêtes sociales dans le cadre de l'attribution d'une aide par la mairie, enquête de satisfaction de la population…). Si ces dernières peuvent s'avérer nécessaires dans le cadre du fonctionnement courant des services municipaux, il n'en est pas de même des enquêtes réalisées pour le compte des organismes considérés par la loi comme des « tiers autorisés » et *a fortiori* pour ceux qui ne peuvent se prévaloir de cette qualité.

La Commission rappelle qu'aucune disposition législative ne permet aux mairies de diligenter des enquêtes à la demande d'administrations même qualifiées de tiers autorisés. La Commission a ainsi rendu un avis défavorable sur une demande présentée par une mairie visant à constituer un fichier d'adresses destiné à diligenter des enquêtes sur les débiteurs du Trésor public [2].

1 L'intervention de tels enquêteurs peut, en revanche, se justifier pour les besoins de la gestion interne, voire sociale, de la mairie (ainsi, corrections des adresses du fichier électoral, vérification de domiciliations, etc.).

2 *Cf.* délibération n° 93-112 du 7 décembre 1993 : la CNIL a estimé qu'aucun texte n'impose aux communes de diligenter des enquêtes pour satisfaire la demande des services du Trésor public visant à obtenir, en application de l'article L. 83 du Livre des procédures fiscales relatif au droit de communication, les documents de service qu'elles détiennent ; le droit de communication consiste pour le détenteur d'une information relative à une personne identifiée en une obligation purement passive de mise de cette information à la disposition d'une administration financière, sur sa demande qui doit être ponctuelle et motivée.

C. Les systèmes d'information géographiques et la diffusion des données cadastrales

Le cadastre recense, décrit et fixe les limites des propriétés foncières et en donne une évaluation qui est utilisée en matière fiscale. Cette documentation, qui est tenue à jour par la direction générale des impôts, a un caractère directement nominatif lorsqu'elle comporte l'identité du propriétaire, indirectement nominatif tant que les informations sont rattachées à la parcelle. Nombre de collectivités locales et d'établissements publics de coopération intercommunale (EPCI) reçoivent sur support informatique les fichiers cadastraux qui se rapportent à leur territoire, pour en permettre l'exploitation par leurs services, pour répondre aux demandes de renseignement du public, voire pour créer un système d'information géographique (SIG). Dans certains cas, les EPCI et les conseils généraux acquièrent ces fichiers auprès des services fiscaux pour les mettre à disposition des collectivités de leur ressort. Plusieurs difficultés ont été constatées lors des visites, qui conduisent à rappeler un certain nombre de règles d'usage.

1. LES CONDITIONS D'ACCÈS AU SYSTÈME D'INFORMATION GÉOGRAPHIQUE

Un SIG est un système de gestion de bases de données qui permet la saisie, la conservation et l'obtention de données localisées. Plusieurs couches de représentations graphiques peuvent y être superposées à partir d'un même fond de plan, ce qui rend techniquement possible le croisement de différentes catégories de données. Il peut réunir ainsi la cartographie numérique du plan cadastral, le plan local d'urbanisme, la photographie aérienne de la commune, la localisation de bâtiments ou de points particuliers, le dessin des réseaux électriques, de gaz, de télécommunication, d'assainissement, d'eau potable, d'irrigation… Des informations directement ou indirectement nominatives, de nature diverse, sur la population peuvent y être associées, au premier rang desquelles figurent les données cadastrales littérales sur les biens immobiliers bâtis ou non-bâtis et leurs propriétaires.

La CNIL constate une tendance à permettre à un nombre croissant de services municipaux d'avoir accès aux SIG du fait de leur attrait, notamment ergonomique, sans que ces services en aient toujours une utilisation bien définie et qu'ait été posée la question de la pertinence de cet accès au regard de leurs missions. Ainsi, il a été constaté, lors d'une visite dans une commune, qu'un SIG permettant notamment d'obtenir la liste des propriétaires immobiliers avait été mis à disposition de la police municipale sans justification concrète.

La Commission a pu également observer qu'un SIG, mis en place par un EPCI parmi les plus importants de France ne prévoyait aucun accès sélectif aux données cadastrales nominatives. Chaque commune pouvait ainsi prendre connaissance des nom, adresse et date de naissance de tous les propriétaires de l'ensemble de la communauté urbaine concernée — soit plusieurs centaines de milliers de noms — mais aussi de la valeur locative des propriétés et des éléments de confort des habitations. Ces données n'auraient dû être accessibles dans les mairies que pour le

territoire communal. Dans le cas des SIG départementaux ou intercommunaux, tant la direction générale des impôts, partie aux conventions de numérisation du cadastre, que les responsables des traitements doivent s'assurer que les communes n'accèdent qu'aux données relatives à leur territoire.

De la même façon, les services d'une commune ou d'un EPCI ne doivent pouvoir consulter les données du cadastre que pour des finalités pertinentes, en rapport avec leurs compétences d'attribution et correspondant à un besoin permanent. En outre, cet accès ne doit porter que sur des catégories d'informations elles-mêmes pertinentes au regard de ces finalités. Par exemple, les services techniques d'une commune n'ont besoin d'accéder qu'aux nom et adresse des propriétaires pour les prévenir en cas de réalisation de travaux dans leur rue.

Les applications de consultation à distance d'un SIG doivent, par ailleurs, bénéficier d'accès sécurisés (cryptage, réseau privé dit VPN, etc.) et de protection contre les détournements de finalité par un tiers (limitation des interrogations, des horaires de connexion, identification de l'opérateur, etc.).

2. LA DIFFUSION DES INFORMATIONS CADASTRALES AUPRÈS DU PUBLIC

La documentation cadastrale comporte à la fois des informations cadastrales, par nature publiques, et des données recueillies à des fins purement fiscales (description des locaux, situation fiscale des personnes...). Ces dernières ne peuvent être communiquées qu'au contribuable concerné. Dans la plupart des communes visitées, sans pour autant qu'il y ait toujours une vérification formelle, les agents ont en général le souci de s'assurer de la légitimité de la demande. Mais la Commission n'ignore pas que, dans quelques communes, la diffusion est plus large, le cadastre étant même parfois en libre accès, au risque de porter atteinte à la vie privée des personnes, de permettre des détournements de finalité et, de ce fait, d'engager la responsabilité des élus.

La CNIL estime que seules les données relatives à l'identification et à la localisation des parcelles, à l'identité des propriétaires, à leur adresse, devraient être communiquées au public, à l'exclusion de toute autre information (description précise du logement, niveau de confort, valeur locative, motif d'exonération des taxes foncières). En outre, les informations cadastrales ne peuvent être utilisées ni à des fins de démarchage commercial ou politique, ni de manière à porter atteinte à la réputation des personnes.

Les mairies ne doivent délivrer des renseignements qu'en réponse à des demandes ponctuelles et précises, concernant une parcelle déterminée et, en cas de doute, après avoir fait signer au demandeur un engagement de ne pas utiliser les données à des fins de démarchage commercial ou politique et de ne pas les divulguer. Dans la mesure où l'une des finalités des fichiers cadastraux pour les communes est de permettre, à partir de l'adresse de la parcelle ou de sa numérotation, d'en identifier le propriétaire, les demandes de consultation de ces fichiers par le public doivent s'effectuer, de façon privilégiée, à partir de l'adresse ou du numéro de la

parcelle. Il convient de rappeler que les requérants peuvent, en toute hypothèse, s'adresser au centre des impôts fonciers du secteur qui est chargé, à titre principal, d'assurer la publicité du cadastre.

La CNIL estime, enfin, qu'en l'absence d'un cadre juridique approprié, la diffusion de données cadastrales nominatives sur des sites internet ou des bornes interactives publics comporte un risque d'utilisation détournée de l'information, alors même que les personnes concernées n'en sont pas informées et qu'elles n'ont aucune possibilité de s'y opposer.

D. La lutte contre la délinquance locale

1. LA CARTOGRAPHIE DE LA DÉLINQUANCE LOCALE

a) Un projet pilote ?

La mairie de Roubaix a saisi la Commission d'un projet d'arrêté municipal portant création, au sein du poste de police municipale de cette ville, d'un traitement automatisé de données nominatives ayant pour objet la localisation et la cartographie des phénomènes de délinquance locale.

Cette application qui a principalement pour objet d'apporter, en collaboration avec la police nationale, une réponse appropriée aux phénomènes de délinquance locale, vise également à corriger certaines interprétations erronées des statistiques actuellement disponibles, dont les résultats ne sont pas jugés assez fins (la dernière étude statistique disponible indiquait que la plupart des vols de voiture étaient commis dans le centre ville de Roubaix alors même qu'ils ont lieu à la périphérie de cette zone car le centre de la ville et sa périphérie constituent, dans le découpage administratif de la ville, un seul et même territoire). Cette application est enfin susceptible de servir d'outil d'aide à la décision en matière d'installation de systèmes de vidéosurveillance et de positionnement des caméras sur la voie publique afin, toujours, de lutter contre la délinquance.

Elle constitue la traduction pratique de la convention de coordination et de partenariat, passée entre la ville et l'État le 14 mars 2002, qui prévoit l'instauration, entre la municipalité et la police nationale, d'un programme d'échange de données statistiques géographiques et non nominatives.

Les informations utilisées pour constituer la base permettant d'établir la cartographie de la délinquance locale portent sur les faits concernés (type d'infraction et information selon laquelle elle a été commise ou seulement tentée), la localisation géographique précise de la commission des faits, la date et l'heure des faits, le sexe, la tranche d'âge, la qualité de majeur ou mineur et la catégorie socioprofessionnelle s'agissant de la victime, le nombre d'auteurs et leur qualité de majeur ou mineur, la présence d'armes et l'indication « usage » ou « trafic » en cas d'infraction à la réglementation sur les stupéfiants.

Elles proviennent de deux sources différentes : le système de traitement des infractions constatées (STIC), tenu par le ministère de l'Intérieur et créé par un décret

du 5 juillet 2001 après avis de la Commission (*cf.* le 21e rapport d'activité de la Commission, p. 73 et ss.), et une base mise en œuvre par la ville (SIC) alimentée par le service de médiation de la ville, la police municipale et, à terme, d'autres services municipaux. Les catégories d'informations utilisées, qui sont les mêmes pour les deux fichiers, concernent l'origine du fichier (STIC ou SIC).

Le seul traitement appliqué aux informations collectées consiste en leur représentation sous la forme de points géocodés sur un plan de la ville, à l'adresse de commission des faits. À chaque point est associée une fiche informatique récapitulant les informations relatives à l'infraction ainsi matérialisée.

Seuls les deux responsables du service « prévention et relations police justice », ainsi que le technicien chargé de la saisie ont accès aux informations permettant d'établir la cartographie. L'usage de la carte tracée est réservé aux personnes précédemment citées, ainsi qu'au maire, aux adjoints au maire, aux maires de quartier, au personnel de la ville chargé de la police municipale et de la prévention, ainsi qu'aux partenaires de la ville au contrat local de sécurité. En aucun cas, la carte produite par cet outil cartographique n'est accessible au public.

Dans la mesure où la géolocalisation des faits à une adresse précise, avec la date et l'heure exactes de leur commission, peut permettre une identification indirecte des personnes physiques concernées et, en particulier, des victimes, même si ni la base de données ni le logiciel utilisé ne permettent d'associer un nom à un fait, le traitement relève de la compétence de la Commission.

b) Un regard circonspect sur ce type d'application

La Commission a rendu le 28 janvier 2003 un avis favorable, en émettant toutefois un certain nombre de réserves, à la mise en œuvre à titre expérimental de ce traitement.

Ainsi, la Commission a rappelé au déclarant que les informations enregistrées relativement aux faits constatés devaient nécessairement être objectives afin d'éviter que ne soient enregistrés dans la base des événements qui ne constitueraient pas des infractions, mais relèveraient plus de manquements — non punissables pénalement — à la vie en société.

S'agissant de la durée de conservation des informations utilisées, la mairie de Roubaix a indiqué que les données elles-mêmes étaient mises à jour chaque semaine, mais que la base de données ainsi constituée pour alimenter l'outil cartographique est conservée *« dans la limite de la durée autorisée pour la conservation des données »* dans le STIC. La Commission a émis sur ce point une réserve de principe et a demandé au déclarant, en l'état, de limiter la durée de conservation des données à une durée expérimentale d'un an à compter de la publication de l'arrêté municipal en portant création. En effet, au-delà même de la difficulté à mettre à jour la base sans disposer de l'identité des personnes concernées, la finalité purement statistique du traitement ne justifie pas de conserver les informations traitées pour des durées allant de cinq à quarante années.

La Commission a également demandé au déclarant de prendre toute mesure appropriée (affiche dans les locaux de la police municipale, insertion dans le bulletin d'informations municipales, etc.) afin d'informer les intéressés, de la mise en œuvre de ce traitement.

Comme on l'a vu plus haut, les systèmes d'information géographiques tendent aujourd'hui à se généraliser dans les collectivités locales et répondent à une demande forte. Ceux permettant de tracer la cartographie de la délinquance locale justifient une vigilance particulière, par la multiplicité des sources pouvant venir les alimenter et les risques de rapprochement et d'interconnexion avec des fichiers locaux pouvant faciliter l'identification des personnes concernées.

Il conviendra en particulier que le ministère de l'Intérieur définisse clairement sa position sur l'alimentation de telles applications par la transmission d'informations issues des fichiers de la police nationale.

2. LA VIDÉOSURVEILLANCE

L'utilisation croissante par les communes de procédés de vidéosurveillance à des fins de sécurité mérite que soit précisée la position de la CNIL sur ce sujet, d'autant que le contexte technologique a fortement évolué ces dernières années.

a) L'évolution technologique

Les moyens de vidéosurveillance sont aujourd'hui, en effet, indissociables des techniques et supports numériques. Les caractéristiques de ces systèmes permettent notamment désormais :

— une intégration aisée et totale des dispositifs de vidéosurveillance dans une configuration informatique, facilitant le stockage d'images sur disque dur, l'accessibilité et la manipulation des séquences enregistrées ;

— la gestion « intelligente » des images captées mettant en œuvre des dispositifs de détection et d'alerte automatisés (lesquels peuvent être paramétrés de façon à ne se déclencher qu'en cas de survenance d'un événement particulier) ;

— le couplage du dispositif de vidéosurveillance avec des systèmes biométriques de reconnaissance faciale ;

— une manipulation à distance aisée d'un réseau de caméras ;

— l'amélioration du contrôle de l'orientation des caméras ainsi que des zones visualisées par des solutions logicielles permettant la définition de zones de masquage dynamique (masquant par exemple les fenêtres et entrées d'immeubles) ;

— une facilité accrue de transmission des images (notamment vers des supports « nomades » de type ordinateur portable ou assistant personnel) grâce à l'orientation vers des solutions reposant sur la technologie internet, et en particulier du type « webcam ».

Ainsi donc, la miniaturisation, les facilités actuelles de branchement et de déploiement, l'amélioration de la définition des images et des capacités de stockage sous forme de données numérisées rendent ces applications plus efficaces, mais aussi plus dangereuses pour les libertés individuelles.

b) Les critères de la compétence de la CNIL

Aux termes de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité et du décret d'application n° 96-926 du 17 octobre 1996, l'installation de dispositifs de vidéosurveillance dans les lieux publics ou établissements ouverts au public *« particulièrement exposés à des risques d'agression ou de vol »* se trouve subordonnée à une autorisation du préfet délivrée après avis d'une commission départementale. Les enregistrements doivent notamment être détruits dans le délai d'un mois et toute personne intéressée peut, en s'adressant au responsable du système, obtenir l'accès aux enregistrements qui la concernent.

Selon l'article 10 de cette loi, la CNIL n'est compétente pour se prononcer sur de tels dispositifs — et doit donc être saisie de dossiers de formalités préalables — que s'ils *« sont utilisés pour la constitution d'un fichier nominatif »*. Le simple fait qu'un organisme public utilise un système de vidéosurveillance ayant recours à un procédé de numérisation des images suffit-il à emporter la compétence de la CNIL ? On peut le soutenir, d'autant que la loi de 1995 et ses textes d'application, conçus dans un contexte technologique très différent, n'apportent pas d'éclaircissements sur ce point. Mais le recours aux techniques numériques étant aujourd'hui très largement répandu, la Commission, eu égard aux capacités actuelles de traitement des images, estime utile de proposer une définition plus précise que le seul critère de l'enregistrement numérique.

La Commission retient donc deux critères alternatifs : l'existence ou non d'un procédé de reconnaissance des visages à des fins d'identification, le rapprochement possible avec des enregistrements d'informations nominatives. Si le dispositif de vidéosurveillance comporte l'une ou l'autre de ces caractéristiques, il doit être soumis à la CNIL.

Ces précisions présentent l'avantage de s'inscrire dans la ligne de la nouvelle rédaction de l'article 10 de la loi du 21 janvier 1995. En effet, le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel prévoit en son article 15, tel qu'amendé par le Sénat, que désormais les enregistrements de vidéosurveillance *« utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques »* sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

III. LES COMMUNES MISES À CONTRIBUTION POUR LE NOUVEAU RECENSEMENT

A. Les traitements mis en œuvre

La Commission suit avec une particulière attention les différentes phases de mise en œuvre du nouveau recensement de la population dont les lignes directrices ont été définies par la loi du 27 février 2002. Après avoir examiné le projet de décret

en Conseil d'État relatif au recensement de la population [1], la Commission a été saisie de la création de trois traitements automatisés par l'INSEE en vue de la préparation des opérations du recensement.

1. LA COLLECTE DES DONNÉES LORS DU RECENSEMENT DES PERSONNES RÉSIDANT DANS LES COMMUNAUTÉS

Aux termes de l'article 21 du décret du 5 juin 2003, la collecte des informations auprès des personnes résidant dans les communautés relève exclusivement de l'INSEE, alors que les communes et les établissements de coopération intercommunale sont désormais chargés de la préparation et de la réalisation des enquêtes auprès des ménages.

La communauté est un ensemble de locaux d'habitation relevant d'une même autorité gestionnaire et dont les habitants partagent à titre habituel un mode de vie commun (communautés religieuses, casernes, établissements pénitentiaires...). La population de la communauté comprend les personnes qui résident dans la communauté à l'exception de celles résidant dans des logements de fonction.

Le recensement dans les communautés suit les nouvelles procédures fixées par l'article 156 de la loi de février 2002 lesquelles diffèrent en fonction de la taille des communes. Dans les communes dont la population est inférieure à 10 000 habitants, la collecte des données a lieu la même année que l'enquête de recensement et porte sur l'ensemble des communautés. Dans les autres communes, les communautés sont recensées en une fois tous les cinq ans. La liste des communes dont les communautés sont recensées figure dans l'arrêté du ministre chargé de l'Économie établissant le programme des enquêtes statistiques publiques.

La collecte est effectuée auprès de l'ensemble des personnes résidant dans la communauté via des questionnaires spécifiques. Les données collectées sont identiques à celles recueillies lors des précédents recensements. Il convient toutefois de relever que les personnes résidant dans les communautés (hors logement de fonction) n'ont pas à répondre aux questions sur le logement. De même, les questions sur les activités professionnelles ne sont pas posées aux détenus.

Les destinataires des données sont les agents habilités des différentes directions régionales de l'INSEE.

Le traitement n'ayant pas appelé d'observation, la CNIL a, par délibération n° 03-003 du 28 janvier 2003 émis un avis favorable. L'arrêté portant création du traitement a été publié le 26 juin 2003.

L'INSEE, en septembre 2003, a adressé à la Commission une demande d'avis portant modification du traitement pour être autorisé à introduire une question sur la catégorie professionnelle et la formation des détenus. Un avis favorable lui a été notifié le 20 octobre 2003.

1 Délibération n° 02-111 du 19 décembre 2002 — décret publié le 5 juin 2003 au *Journal officiel*.

2. L'UTILISATION DES FICHIERS DE LA TAXE D'HABITATION PAR L'INSEE

Comme pour les recensements précédents, l'INSEE a demandé à la CNIL l'autorisation de créer un traitement automatisé à partir de l'exploitation des données issues des fichiers de la taxe d'habitation afin de contrôler l'exhaustivité de la collecte des données, d'estimer les résultats du recensement et de mettre à jour le répertoire des immeubles localisés (RIL [1]).

Il s'agit, pour l'INSEE, en vue de la préparation de la collecte des données du recensement, de s'assurer sur le terrain de la réalité des adresses. Les contrôles opérés par du personnel INSEE sont aléatoires. La connaissance des logements nouveaux permet enfin d'estimer les résultats du recensement ainsi que la mise à jour du RIL, créé dans les communes de plus de 10 000 habitants.

Les données sont transmises à L'INSEE en application de l'article 5 de l'arrêté du 8 mars 1996 relatif au traitement informatisé de la taxe d'habitation. Le fichier constitué fait l'objet d'une mise à jour annuelle et est détruit au bout de six ans, soit un an après la fin d'un cycle de recensement.

Après avoir relevé d'une part que la mise en œuvre d'un tel traitement avait été autorisée pour les recensements de 1990 et 1999 et d'autre part que le décret relatif au recensement le prévoyait dans son article 39, la Commission a émis un avis favorable par délibération n° 03-004 du 28 janvier 2003.

3. L'ENQUÊTE CARTOGRAPHIQUE DANS LES DÉPARTEMENTS D'OUTRE-MER

Les départements d'outre-mer ne disposant pas d'outils cartographiques, notamment du RIL, l'INSEE a été conduit à mettre en place un traitement spécifique concernant la localisation des immeubles dans l'ensemble des communes afin de contrôler la qualité de la collecte des enquêtes de recensement et d'envisager, pour les communes de 10 000 habitants et plus, la mise en place du RIL. L'utilisation de ce traitement est prévue jusqu'à la fin de l'année 2008.

Les données enregistrées sont définies par l'article 26 du décret relatif au recensement. Ce sont des données dites de localisation qui concernent les immeubles bâtis et les logements et qui sont nécessaires à la préparation et à la réalisation des enquêtes de recensement. Elles sont à cette fin, conformément à l'article 156 de la loi du 27 février 2002, librement échangées entre l'INSEE et les communes.

Il convient de noter que le nom de l'occupant principal figure au titre des données de localisation des logements. La Commission a considéré que cette donnée est utile pour identifier avec certitude les logements recensés et assurer ainsi l'exhaustivité de la collecte.

1 Le RIL doit permettre la mise en place des enquêtes par sondage dans les communes de plus de 10 000 habitants. Le territoire communal est divisé en cinq groupes d'immeubles et chaque année, une partie des adresses d'un groupe est sélectionnée et les logements situés à ces adresses recensés.

La Commission a, par délibération n° 03-005 du 28 janvier 2003, émis un avis favorable à la création du traitement.

B. Les modalités de saisie et d'exploitation des données

La Commission a été saisie par l'INSEE, en application de l'article 33 du décret du 5 juin 2003, de la mise en œuvre de traitements pour la saisie et l'exploitation des données recueillies lors de la collecte réalisée chaque année, à compter de 2004, d'une part par les communes et les établissements publics de coopération intercommunale auprès des ménages (en janvier-février), d'autre part par l'INSEE, pour ce qui concerne les communautés (en mars).

Cette phase de saisie et d'exploitation des données suppose différentes étapes : « l'acquisition » sur support informatique par lecture optique des données, la mesure de la qualité de l'acquisition des données, le contrôle de la cohérence des questionnaires et le redressement des non-réponses, et enfin la validation des données.

1. LES DONNÉES RECUEILLIES

Les données traitées sont issues des bulletins individuels et des feuilles de logement récupérées par les agents recenseurs, conformément aux dispositions des articles 26 et 38 du décret précité de 2003, complétées pour ce qui concerne les communautés, par l'article 2 de l'arrêté du 26 juin 2003 susvisé. Il convient de relever que les nom et prénoms ne sont pas saisis dans le fichier informatisé.

Figurent dans le traitement :

— s'agissant des personnes physiques : la date et le lieu de naissance, le sexe, la nationalité, la situation familiale, le niveau et la nature de la formation, les études, les activités professionnelles, le lieu de résidence, le lieu d'étude ou de travail, la résidence antérieure, les moyens de transport, les conditions de logement et l'équipement en véhicules automobiles ;

— s'agissant des logements : les caractéristiques de confort et d'occupation, l'immeuble auquel appartient le logement et l'étage du logement ;

— s'agissant des immeubles : les coordonnées géographiques des immeubles bâtis, le type et le nom de la voie, le numéro dans la voie, un complément d'adresse si celui-ci est nécessaire, le type d'immeuble, la date de construction, la date d'entrée dans le répertoire d'immeubles localisés, la date de dernière modification (ou de destruction), l'aspect du bâti, le nombre de logements, le nombre d'étages, le nombre de communautés, le nombre d'établissements, le nombre d'équipements urbains ;

— un code à barres, apposé automatiquement sur chaque questionnaire lors de leur impression, qui comporte dix chiffres : le premier désigne le millésime de l'enquête de recensement, le second donne le type de questionnaire, les huit derniers chiffres composent un numéro d'ordre non significatif. Ce code à barres permet à l'INSEE, lors de la réception des questionnaires d'établir un lien entre le code à barres de la feuille de logement et celui de chacun des bulletins individuels qui lui sont rattachés.

Ce code facilite ainsi à tous les stades de la saisie, des contrôles et de l'exploitation, le suivi des questionnaires.

2. LES FICHIERS CONSTITUÉS

À l'issue de la phase d'acquisition des données et de contrôle de la qualité de cette saisie, sont constitués deux fichiers de données et une base d'images :
— le fichier « complet anonyme », qui comporte toutes les données, à l'exception du nom et des prénoms des personnes. Il est complété par l'INSEE, pour les personnes ayant une activité salariée et pour les entrepreneurs individuels, par les mentions de l'activité économique, de la catégorie juridique, de la tranche d'effectif, de la localisation de l'établissement concerné. C'est à partir de ce fichier que l'INSEE travaille traditionnellement pour élaborer les résultats du recensement de la population ;
— le fichier de l'échantillon démographique permanent, qui intègre les nom, prénom, sexe, date et lieu de naissance, code à barres issus des bulletins individuels des personnes nées entre le 1er et le 4 octobre chaque année, qui de ce fait, appartiennent à l'échantillon permanent. Ce fichier est destiné à la mise à jour de l'échantillon démographique permanent ;
— la base image « adresses issues de la feuille de logement », qui reprend les données de localisation, telles que prévues par l'article 26 du décret du 5 juin 2003 ainsi que le code à barres. Cette base sert à préparer les enquêtes statistiques ultérieures menées par l'INSEE. En effet, pour chaque enquête, l'INSEE effectue un tirage au sort de logements pour interroger leurs habitants.

Dès réception des fichiers, l'INSEE réalise un travail de codification des données et de redressement des non-réponses. Par ailleurs, l'INSEE procède, afin de calculer la population comptée à part des communes, au rapprochement de la liste des personnes rattachées administrativement à une commune dans les conditions prévues par la loi du 3 janvier 1969 avec les bulletins individuels des personnes résidant dans une habitation mobile et ceux des personnes sans abri recensées sur le territoire de cette commune. Ce rapprochement réalisé manuellement ne donne lieu à aucune saisie nominative.

3. LA CONFIDENTIALITÉ

Le seul destinataire de l'ensemble des données est l'INSEE. Les Archives de France, moyennant la signature de protocoles d'accord avec l'INSEE, lesquels seront soumis à la CNIL ainsi que s'y est engagé l'INSEE, pourront recevoir des documents, des fichiers et des bases d'images.

L'INSEE détruira le fichier de l'échantillon démographique permanent au plus tard à la fin de l'année suivant celle de sa réception définitive ; la base « adresse des logements » sera, pour sa part, supprimée au plus tard à la fin de la sixième année suivant celle de sa réception définitive.

Les bases images échantillon réalisées lors du contrôle de la qualité de la saisie seront détruites par l'INSEE dans les deux jours ouvrés qui suivent la

notification de la réception définitive du fichier complet anonyme par les sous-traitants. Ces derniers détruiront, dans ce même délai, toutes les données en leur possession à l'exclusion des questionnaires qui seront retournés à l'INSEE.

Des mesures spécifiques de sécurité ont été définies par l'INSEE dans les marchés signés avec les sous-traitants. Elles portent sur le transport et le stockage des documents, les locaux, les procédures, les matériels et logiciels utilisés, les contrôles exercés par l'INSEE. Elles font l'objet d'annexes détaillées jointes au dossier de demande d'avis déposé par l'INSEE auprès de la CNIL.

La Commission a pris acte de ce que les modalités de mise en œuvre des traitements, la nature des données traitées et les finalités poursuivies pour le nouveau recensement sont identiques à celles du recensement général de la population. Elle s'est par ailleurs assurée des mesures de sécurité prises aux différents stades du traitement pour garantir la confidentialité des données.

Elle a donc émis un avis favorable à la mise en œuvre du traitement par délibération n° 03-068 du 18 décembre 2003.

Chapitre 5

LA TRAÇABILITÉ DES DÉPLACEMENTS

Quo vadis ? Où vas-tu ? Quand et comment te déplaces-tu ? Pour des finalités diverses, de nombreuses entreprises cherchent aujourd'hui, par l'exploitation de fichiers informatiques, à rassembler des données sur ces questions essentielles concernant leur personnel ou leurs clients. Elles bénéficient, à cet effet, notamment du développement de la géolocalisation utilisée généralement en vue de protéger les véhicules contre le vol ou de porter secours aux conducteurs, ou encore de vérifier les itinéraires empruntés par des salariés. Dans le même temps, des sociétés d'autoroutes se proposent d'enregistrer les vitesses des automobiles et de rappeler leurs propriétaires à la limitation imposée, tandis que, dans les transports collectifs, la validation des billets, et donc la connaissance des parcours effectués, est considérée comme devant permettre de lutter efficacement contre la fraude et qu'il est envisagé, par ailleurs, pour des raisons présentées comme sécuritaires, de mettre en œuvre le suivi de personnes à partir du téléphone portable. La CNIL, chargée notamment de veiller au respect de la vie privée et de la liberté d'aller et venir, a récemment adopté des décisions confirmant le droit à l'anonymat des personnes dans tous leurs déplacements.

L'anonymat est en effet une condition nécessaire de la liberté d'aller et venir ou de la préservation de la vie privée et l'analyse prospective menée par la CNIL sur les technologies de radio-identification ou étiquettes intelligentes montre le risque de suivi des individus qui en sont porteurs.

Les technologies de géolocalisation sont également utilisées par le ministère de la Justice qui a souhaité expérimenter le placement sous surveillance à distance par bracelet électronique comme une alternative à la prison. Il s'agit bien là d'un procédé de surveillance totale du déplacement.

I. LA LIBERTÉ D'ALLER ET VENIR ANONYMEMENT

A. Aux prises avec la billettique

De nombreux traitements automatisés d'informations nominatives reposent sur l'utilisation d'une carte à puce. L'essor de cette technologie est lié au fait qu'il s'agit d'un outil simple d'utilisation sur lequel il est possible de stocker un nombre relativement important d'informations tout en bénéficiant d'un niveau de sécurité élevé. En outre, grâce au développement des dispositifs sans contact, via par exemple l'utilisation de la technologie RFID, les cartes à puces peuvent être utilisées sans avoir à les introduire dans un lecteur, il suffit désormais de les passer à proximité de celui-ci.

Cette évolution a notamment permis d'avoir recours aux cartes à puce dans le cadre des services de transports collectifs comme en témoigne le nombre croissant d'exploitants de réseaux de transport faisant appel à ce qu'il convient de nommer des applications billettiques.

1. LA RATP

Le dispositif dénommé « Navigo » mis en œuvre par la RATP, constitue l'une des plus ambitieuses applications billetiques dans la mesure où il s'inscrit dans le cadre de la généralisation de la billettique en Ile-de-France, devant à terme être mise en œuvre par toutes les entreprises de transports collectifs de la région, sous le pilotage du syndicat des transports d'Ile-de-France (STIF).

Il s'agit d'une carte à puce permettant le passage des contrôles d'accès « sans contact » grâce à une transmission radio. La télétransmission des données s'effectue à distance, lorsque l'on approche la carte de la cible de validation repérée sur les tourniquets et portillons. Ce titre de transport apporte une amélioration notable du service rendu aux voyageurs par l'utilisation du même passe quel que soit le transporteur (train, métro ou bus) et un passage plus fluide aux tourniquets, les usagers n'ayant plus à introduire un ticket.

Sa mise en œuvre doit s'échelonner jusqu'en 2007, avec trois phases principales. La première phase, aujourd'hui achevée, portait sur la conversion en 2002 des abonnements annuels des cartes « Intégrale » [1] et « Imagine R » [2]. La seconde concerne la conversion des abonnements mensuels et hebdomadaires de l'actuelle « carte orange » au cours de l'année 2004, selon deux axes, d'une part, des cartes nominatives avec remplacement en cas de perte ou vol, d'autre part, des cartes déclaratives comme à l'heure actuelle sans recueil d'information sur le porteur de la carte. Enfin, il est prévu que d'ici 2007 les billets à la journée et les carnets passent également au format billettique, sur le modèle des cartes téléphoniques prépayées.

1 La carte « Intégrale » est un abonnement personnel et permanent, il s'agit d'un coupon unique, valable toute l'année pour tous les déplacements en Ile-de-France.

2 La carte « Imagine R » est un abonnement personnel annuel destiné aux jeunes de moins de 26 ans, il s'agit d'un coupon unique permettant d'utiliser les transports en commun pour tous les déplacements en Ile-de-France.

En 2002, afin de pouvoir initier la première phase, la RATP a saisi la CNIL d'une demande d'avis concernant le traitement des statistiques de validation et de détection de titres frauduleux des cartes « Navigo ». À cette occasion, la Commission a constaté que les données relatives aux déplacements des personnes, c'est-à-dire l'indication de la date, de l'heure et du lieu d'entrée sur le réseau et d'un passage en correspondance, étaient collectées puis traitées par le système central. Ces informations étant automatiquement associées au numéro de carte, il est ainsi possible d'identifier la personne à laquelle elles sont rattachées.

Considérant que la liberté d'aller et venir et le droit à la vie privée supposent que les personnes puissent se déplacer de manière anonyme, la CNIL s'est alors interrogée sur la constitution d'un traitement d'informations nominatives retraçant les déplacements, sur le réseau RATP, des usagers utilisant le passe sans contact « Navigo » ainsi que sur une possible utilisation du traitement à des fins étrangères aux finalités qui auraient présidé à sa mise en œuvre. Dès lors, la Commission a estimé devoir différer son avis sur la demande dont elle était saisie, d'autant plus que les informations apportées par la RATP concernant les finalités de ce traitement, les conditions de sa constitution, ses incidences et la nature des données collectées ont été jugées incomplètes.

La RATP a en conséquence fait parvenir à la CNIL, le 5 novembre 2002, un dossier dans le cadre duquel elle a apporté les compléments d'informations demandés et a exposé l'ensemble des modifications devant être apportées au traitement billettique « Navigo ». La RATP a ainsi indiqué que c'est uniquement dans le cadre du traitement de détection de la fraude que les données de validation, contenant des informations relatives aux déplacements des personnes, seraient associées au numéro de carte et ce pendant une journée plus une au maximum (J+1). En outre la RATP s'est engagée, pour tous les traitements étrangers à la lutte contre la fraude, à ce que le numéro de série de la carte soit remplacé par un « identifiant anonyme du passe ».

Considérant que ces aménagements étaient de nature à préserver la liberté d'aller et venir anonymement, la Commission a émis un avis favorable (délibération n° 03-008 du 27 février 2003) tout en précisant qu'il ne couvrait que les traitements relatifs aux abonnements annuels des cartes « Intégrale » et « Imagine R », ceci afin que la RATP présente un nouveau dossier avant la fin de l'année 2003 concernant la conversion des « cartes oranges ». Ce dernier est actuellement en cours d'instruction.

2. RECOMMANDATION GÉNÉRALE

Compte tenu des enjeux apparus à l'occasion de l'instruction de ce dossier, la Commission a décidé de mener des missions de contrôles auprès de cinq sociétés de transports collectifs [1] qui se sont déroulées durant les mois de septembre et octobre 2002. Ces missions de contrôle ont notamment permis de constater que tous les exploitants de réseaux de transports collectifs procédaient à la collecte et au trai-

1 La Régie des transports marseillais (RTM), la Société d'économie mixte des transports amiénois (SEMTA), la Société d'économie mixte intercommunale pour l'amélioration de la circulation et du stationnement (SEMIACS/Nice), la Société d'économie mixte des transports urbains de la région de Valenciennes (SEMURVAL) et la Société lyonnaise des transports en commun (SLTC).

tement des données relatives aux déplacements des personnes dans le cadre de la mise en œuvre d'un dispositif billettique.

À la suite de ce constat, la Commission a adopté une recommandation (délibération n° 03-038 du 16 septembre 2003) relative à la collecte et au traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques, après avoir consulté les représentants de l'Union des transports publics (UTP), du Groupement des autorités responsables de transport (GART) et du ministère de l'Équipement, du Logement et des Transports.

Parmi les principaux éléments de cette recommandation, il convient de souligner que les finalités justifiant la mise en œuvre des traitements de billettique doivent être clairement indiquées et détaillées, que les traitements appliqués aux données relatives aux déplacements des personnes doivent être anonymisés, à l'exception de ce qui relève de la gestion de la lutte contre la fraude et qu'en toute hypothèse, il est hautement souhaitable que la possibilité de circuler de façon anonyme, au moyen d'un titre billettique ou non, soit maintenue.

Par ailleurs, la Commission indique que la collecte de la photographie devant figurer sur le support du titre de transport devrait être accompagnée de la possibilité, pour l'usager, de s'opposer à sa conservation, sous une forme numérique. Enfin, elle estime que les données relatives aux déplacements des personnes, sous la forme d'une indication de la date, de l'heure et du lieu, associées à un élément permettant d'identifier la personne à laquelle elles sont rattachées, tels un numéro de carte, ne devraient être conservées que le temps nécessaire à la détection de la fraude. Ce délai ne devant pas excéder deux jours consécutifs y compris le délai de sauvegarde.

B. Aux prises avec les puces RFID

La radio-identification apparaît au travers de puces miniatures (quelques millimètres au plus constitués d'un microprocesseur et d'une antenne) sous les vocables synonymes de RFId, de *Smart Tag*, *Transponder* ou encore de radio-tags. Ces étiquettes intelligentes (*Smart Tags*) sont pour la plupart d'entre elles passives et sans énergie propre ; dans un flux magnétique variable elles émettent selon des fréquences radio bien définies une simple suite alphanumérique fixe qui sert d'identifiant à l'objet étiqueté. La portée de cette diffusion radio est variable suivant la norme technique choisie et contextuelle : quelques centimètres jusqu'à quelques mètres. Enfin, certains tags sont capables de recevoir de l'information et de l'enregistrer.

Si la radio-identification fait déjà partie de nos vies au travers des cartes de transport sans contact (dont « Navigo » pour la RATP) ou de nombreuses clés de voiture, c'est dans le secteur de la distribution que se place l'avenir le plus massif en tant que code-barre radio. Ce dernier est l'objet de projets et de normalisation mondiale qui ont pris un contour net au cours de l'année 2003. Au-delà des effets d'échelle opérant sur les coûts de production des RFIds (moins de 20 cents à ce jour), la nature des identifiants permet une différenciation entre deux items d'un même produit dès leur fabrication.

L'analyse prospective conduite par la CNIL qui a débouché sur une communication du 30 octobre sur le sujet de la radio-identification identifie quatre pièges qui concourent à minorer le risque que présente cette technologie en matière de protection des données personnelles et de la vie privée : l'insignifiance (apparente) des données, la priorité donnée aux objets (en apparence toujours vis-à-vis des personnes), la logique de mondialisation (normalisation technologique basée sur un concept américain de *Privacy* sans prise en compte des principes européens de protection de la vie privée) et enfin le risque de « non vigilance » individuelle (présence et activation invisibles).

Les technologies de radio-identification peuvent être utiles pour des finalités légitimes bien définies. Néanmoins, le maillage dense de milliers d'objets qui entoureront une personne, pouvant être analysé de façon permanente (le potentiel de rayonnement d'un RFId est illimité dans le temps car aucune batterie n'est nécessaire), ces technologies permettent potentiellement le « profilage » des individus et font peser sur ceux-ci un risque particulier comprenant notamment la traçabilité de leurs déplacements.

Pour toutes ces raisons, la Commission considère que les RFIds sont des données personnelles au sens de la loi « informatique et libertés » comme à celui de la directive 95/46.

La conférence internationale des commissaires à la protection des données (Sydney, 2003) a d'ailleurs pris position dans cette direction et formulé des recommandations élémentaires impliquant pour les responsables de traitement de veiller à strictement utiliser les radio-identifiants pour des finalités dans lesquelles cette technologie est incontournable, de veiller à l'obligation d'information des individus possesseurs d'objets radio-identifiables et enfin de garantir la capacité qui doit être donnée aux individus possesseurs de neutraliser le caractère activable ou identifiant de ces éléments. S'agissant de ce dernier point, des dispositifs techniques garantissant la neutralisation ou le détachement des RFIds devraient donc être incorporés dès la fabrication. Si des solutions théoriques existent déjà, la recherche doit encore avancer pour trouver des moyens pratiques de mise en œuvre.

C. Aux prises avec les téléphones portables

L'utilisation d'un téléphone portable nécessite son rattachement, à partir du moment où il est mis en service, à un relais radioélectrique de l'opérateur en charge d'acheminer la communication. Ce rattachement technique donne lieu à la création d'une nouvelle donnée, spécifique à la téléphonie mobile : la donnée de localisation. L'année 2003, en même temps qu'elle aura vu le cadre légal concernant la conservation et l'utilisation de la donnée de localisation se préciser (projet de loi relatif aux communications électroniques et projet de décret relatif à la conservation des données de connexion), aura permis à la Commission de se pencher sur les premiers services basés sur la localisation d'une personne par un tiers sans que soit en cause la délivrance d'une prestation de service ou la situation d'une personne à l'égard de laquelle existe un lien de subordination hiérarchique issu d'un contrat de travail.

1. LA GÉOLOCALISATION DES ENFANTS

La Commission a été saisie d'une demande de conseil relative à la mise en œuvre d'un service permettant de connaître la localisation d'un téléphone portable et, en conséquence, de son utilisateur. Ce service est conçu principalement à destination des parents soucieux de connaître la position de leurs enfants à qui ils auraient confié un téléphone portable.

Après son inscription et l'inscription des numéros de téléphone dont elle souhaite connaître à l'avenir la localisation, une personne peut, en se connectant sur le site web édité par la société, visualiser à tout moment sur une carte la localisation des personnes utilisatrices des téléphones portables inscrits. Une procédure d'authentification forte empêche l'inscription, à l'insu des personnes, de leurs téléphones portables, en même temps que leur est offerte la possibilité de se désinscrire à tout moment. La Commission a souhaité que soient renforcées les garanties offertes aux personnes inscrites et, en faisant une application stricte des dispositions de la directive du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, a demandé que la personne dont le téléphone aura été inscrit doive valider cette inscription par retour de message texte (SMS). De la même manière, le souci d'une parfaite transparence a conduit la Commission à exiger que chaque opération de localisation effectuée soit portée à la connaissance de la personne dont le téléphone aura fait l'objet d'une requête de localisation par un envoi d'un message texte sur son téléphone l'avertissant qu'elle aura été localisée et par qui.

2. QUESTIONS DE LÉGITIMITÉ

Ces services ne doivent porter atteinte « *ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » (article 1er de la loi du 6 janvier 1978).

D'un point de vue parental, la possibilité de localiser un enfant utilisateur d'un téléphone portable répond bien à une attente de certains parents. En effet, la médiatisation d'affaires criminelles mettant en cause des enfants et le développement d'une vie de plus en plus « nomade » conduisent certains parents à vouloir être « rassurés » en pouvant, à tout moment, connaître la position de leur(s) enfant(s) sans pour autant les appeler directement. Cette utilisation, nouvelle, du téléphone portable au bénéfice du parent qui en supporte la charge financière, peut être conçue comme une sorte de « contrat » au sein de la famille : une plus grande autonomie au bénéfice de l'enfant pour ses communications en échange d'une possibilité nouvelle pour les parents de le localiser.

À ce titre, le service proposé répond à un « besoin » contemporain identifié et constituerait une nouvelle manifestation de la « commercialisation » des potentialités des données de géolocalisation.

D'un autre côté, l'enfant dispose de droits, définis en particulier par la Convention internationale des droits de l'enfant qui précise dans ses articles 3 et 18 que

« *l'intérêt supérieur de l'enfant doit être une considération primordiale* » dans toute décision le concernant. Au cas présent, le fait de pouvoir être localisé à tout moment par un parent est-il de l'intérêt supérieur de l'enfant ou tout simplement légitime ?

La Commission a déjà abordé la question de l'incidence de dispositifs techniques de surveillance sur l'épanouissement de l'enfant à travers l'examen d'une demande d'avis relative à la diffusion sur internet d'images d'une crèche municipale (délibération n° 01-002 du 16 janvier 2001). À cette occasion, la Commission avait relevé que l'enfant avait besoin, pour sa construction personnelle, d'une certaine part d'autonomie qui contribue à sa socialisation, ce qui excluait l'utilisation de moyens de surveillance trop intrusifs. Ce qui est vrai pour un enfant en bas âge dans une crèche ne l'est-il pas aussi pour un enfant ou un adolescent en âge d'utiliser un téléphone portable ?

Le recours à ce type de service n'est-il pas susceptible de perturber le jeu normal des relations de confiance entre parents et enfants ? Ce service ne tendra-t-il pas, de façon perverse, à favoriser le désengagement de certains parents qui pourraient avoir l'illusion de maîtriser — ou à tout le moins de contrôler — l'activité de leurs enfants ? Enfin, d'un point de vue sociétal, le développement de ces services ne va-t-il pas contribuer à habituer l'individu, dès son plus jeune âge, à une forme de contrôle quasi permanent dont il ne percevra même plus le caractère intrusif ?

3. CONSULTATION

Face à ces questions, la Commission a décidé de lancer sur son site internet une consultation permettant aux personnes qui s'y connectent d'exprimer leur position sur cette question.

Les premiers résultats de ce sondage font apparaître que seuls 20 % des personnes qui se sont identifiées comme « parents » excluent catégoriquement d'utiliser ce service quelles que soient les circonstances, alors que la proportion des personnes réfractaires à ce type de service atteint plus de 40 % chez les personnes qui ne sont pas « parents ». Pour autant, les personnes ayant répondu au questionnaire estiment, indifféremment de leur qualité de parent ou non, que ce service de localisation n'est pas destiné à s'appliquer à des enfants âgés de plus de 16 ans. De la même manière, la question de la validité du consentement de l'enfant entraîne le même pourcentage de réponses selon que les personnes sont parents ou non, puisque 45 % des personnes estiment que le consentement de l'enfant est une garantie appropriée pour limiter les dérives d'utilisation de ce service.

La majorité des commentaires des personnes favorables à l'utilisation de ce type de service mettent en avant leur souci d'une meilleure sécurité vis-à-vis de leurs enfants. Néanmoins, un grand nombre de ces personnes pratiquent une confusion entre ce service — qui est destiné aux parents dans le cadre d'une relation familiale — et les potentialités offertes par la géolocalisation aux forces de l'ordre dans le cadre de leurs activités de recherche des personnes. L'idée d'une utilisation raisonnable par les parents se retrouve de nombreuses fois, de même que l'impératif de surveillance à la charge des parents. À ce titre, beaucoup de commentaires reflètent la

perception d'un lien fort entre la connaissance de la localisation d'un enfant et la connaissance de l'activité de ce même enfant ! Certaines personnes envisagent une utilisation de ce service limitée au seul cas extrême né d'une maladie grave qui commanderait aux parents de pouvoir, à tout moment, localiser leurs enfants. D'autres n'envisagent une utilisation qu'en cas d'événements ponctuels (retards, sorties nocturnes, etc.).

Les personnes défavorables à ce type de service pointent les dangers issus d'une société de surveillance et la nécessaire autonomie des enfants vis-à-vis de leurs parents. D'autres mettent en avant les risques de déresponsabilisation des parents, issue de l'utilisation de cette nouvelle technologie. Enfin, la dérive d'une utilisation de ce service pour localiser, non plus des enfants, mais d'autres adultes est, elle aussi, envisagée.

Ce dossier de la géolocalisation des mineurs a constitué l'amorce d'une réflexion plus générale sur la géolocalisation que la CNIL entend poursuivre en 2004.

II. LA SURVEILLANCE SUR LES ROUTES

A. Le développement des services de géolocalisation

À ses débuts, la technologie GPS servait essentiellement d'aide à la navigation pour les automobilistes, se bornant à indiquer la position et le trajet à suivre. Son association avec la technologie GSM a permis de communiquer vers l'extérieur les informations relatives à la position des véhicules. L'offre de ces services n'a cessé de croître et de se diversifier ainsi qu'en témoigne le nombre croissant des déclarations et demandes de conseil reçues par la CNIL à ce sujet au cours de l'année 2003.

Les systèmes de géolocalisation GSM/GPS reposent le plus souvent sur un même schéma : un boîtier est installé à bord du véhicule, la demande d'information est adressée par le biais du réseau de téléphonie GSM ; via le réseau satellitaire le récepteur GPS calcule en temps réel la position du véhicule, cette information est ensuite renvoyée par le réseau GSM central vers un serveur, la situation du véhicule est alors affichée sur une carte routière consultable en se connectant audit serveur.

Certaines de ces applications visent une cible de clientèle de particuliers alors que d'autres sont destinées aux employeurs afin d'assurer la localisation de leurs salariés lorsqu'ils utilisent des véhicules professionnels. Dans les deux cas, le risque d'atteinte à la liberté d'aller et de venir et à la vie privée existe, du fait que les dispositifs envisagés permettent de connaître avec précision les itinéraires des conducteurs des véhicules mais la problématique diffère selon qu'il s'agit de salariés ou non.

1. LES SERVICES À DESTINATION DES PARTICULIERS

S'agissant des services à destination des particuliers, c'est en 1999 que la CNIL a été pour la première fois amenée à examiner un dispositif GSM/GPS [1]. Il s'agissait d'un service proposé par la Régie Renault et qui permettait aux personnes abonnées à ce service d'être géolocalisées en situation d'urgence (accident, panne, malaise...) afin de faciliter et d'accélérer l'action des services compétents. Deux aspects de ce dossier avaient retenu l'attention de la Commission, celui de l'information préalable de l'abonné et celui de la durée de conservation des informations relatives à la localisation. Bien que le dispositif en question ait été abandonné, l'évolution des technologies, notamment la perspective d'une connexion permanente par les technologies de téléphonie mobile GPRS/UMTS, et la baisse escomptée des prix d'équipement et des coûts de transaction incitent de nouveaux acteurs à élaborer des offres similaires qui devraient être prochainement présentées à la CNIL.

a) Vol de voitures

Par ailleurs, les dossiers récemment soumis à la Commission laissent apparaître que les services de géolocalisation proposés aux particuliers concernent de plus en plus des dispositifs de détection de véhicules volés. Afin de bénéficier de ce type de service, les particuliers, de même que les entreprises souhaitant assurer la sécurité de leur parc automobile, concluent un contrat d'abonnement avec une société prestataire de service qui équipe les véhicules d'un boîtier GSM/GPS, assure le traitement des données et effectue la transmission des informations aux autorités compétentes. Le fonctionnement du dispositif comporte deux phases. Une phase « veille » durant laquelle le véhicule n'est pas géolocalisé et une phase « vol » qui donne lieu à la transmission des coordonnées du véhicule. Le passage en phase « vol » est consécutif soit à l'appel du propriétaire constatant la disparition de son véhicule, soit à la détection d'une tentative d'effraction sur le véhicule. Dans cette hypothèse, l'entreprise prestataire de service demande confirmation au propriétaire afin de s'assurer qu'il ne s'agit pas d'une fausse alerte.

Il convient de souligner que la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité a donné une base légale à la mise en œuvre de ce type de traitements. En effet, l'article 15 de cette loi prévoit explicitement qu'en vue de prévenir les infractions contre les véhicules et leurs équipements, l'installation de dispositifs de sécurité ou de marquage, y compris des procédés électroniques, peut être rendue obligatoire. Le législateur a également prévu de sanctionner le fait de détourner les dispositifs en question pour localiser à distance des véhicules non volés, ce qui correspond au souci de la Commission de s'assurer que ces systèmes ne puissent être détournés de leur finalité et utilisés pour suivre les déplacements des personnes.

L'instruction des demandes de conseils et de déclarations relatives à ces services a permis à la Commission d'attirer l'attention des prestataires sur le fait que les particuliers ou les sociétés abonnés à ce service ne sauraient être destinataires des

1 20e rapport d'activité 1999 de la CNIL, édition 2000, La Documentation française, p. 120.

informations de géolocalisation des véhicules afin d'éviter qu'ils se mettent en danger en voulant récupérer le véhicule volé, voire se faire justice eux-mêmes. Dès lors, seules les autorités de police apparaissent habilitées à avoir connaissance des données. Par ailleurs, la Commission a rappelé que la durée de conservation des données doit être limitée aux nécessités de l'enquête et de l'instruction du dossier par les autorités judiciaires.

b) Géolocalisation libre

La CNIL a été saisie d'une demande de conseil concernant les services de géolocalisation « libre ». L'aspect novateur de ce type de service est que le client dispose d'un accès direct, après identification, aux données de géolocalisation en se connectant via internet aux serveurs du prestataire de service auprès duquel il s'est abonné et qui lui a fourni le boîtier GSM/GPS. En permettant la localisation d'un véhicule et donc par conséquent de son conducteur, par toute personne abonnée au service, ces systèmes comportent des risques importants de violation de la vie privée. En outre, l'article 9 de la directive du 12 juillet 2002, relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques dispose que lorsque des données de localisation sont traitées, elles ne peuvent l'être que moyennant le consentement de la personne concernée. Il appartient en conséquence au responsable du traitement d'obtenir le consentement de toutes les personnes susceptibles d'utiliser le véhicule et donc d'être localisées, ce qui pose un problème pratique évident.

2. LE SUIVI DES VÉHICULES PROFESSIONNELS

Les services à destination des particuliers ne constituent qu'une faible part des dossiers relatifs à des dispositifs de géolocalisation soumis à la Commission. En effet, au cours de l'année 2003, la Commission a majoritairement reçu des dossiers de déclaration relatifs à la mise en œuvre de dispositifs de suivi de véhicules professionnels utilisés par des salariés.

Le plus souvent les finalités poursuivies sont le décompte des heures de travail et le contrôle de l'activité des salariés, cependant certains dossiers présentent également les traitements en question comme un outil destiné à améliorer la gestion de la flotte de véhicules, les performances ou à rationaliser les déplacements. S'agissant des données traitées, l'information de base est celle relative au trajet effectué, certains dispositifs permettant également d'associer aux données de géolocalisation des informations relatives au temps d'arrêt, à l'heure de départ et d'arrivée et à la vitesse des véhicules. Les durées de conservation des données annoncées par les déclarants varient quant à elles entre un et quatre ans.

b) Filature électronique ?

Dans un premier temps, la Commission s'est s'interrogée sur la légitimité de la mise en œuvre des systèmes de géolocalisation dans un contexte professionnel. La légitimité du contrôle de l'activité des salariés par l'employeur ne fait pas de doute.

L'employeur dispose notamment d'un pouvoir disciplinaire lui permettant de sanctionner le salarié dans le cadre du contrôle de la bonne exécution du travail. De même, l'article L. 212-4 du Code du travail dispose que la durée du travail effectif est le temps pendant lequel le salarié est à la disposition de l'employeur et doit se conformer à ses directives sans pouvoir vaquer librement à des occupations personnelles.

Pour autant, doit-on considérer que l'utilisation d'un dispositif de suivi GSM/GPS est compatible, d'une part, avec l'article L. 120-2 du Code du travail qui dispose que nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature des tâches à accomplir ni proportionnées au but recherché et d'autre part, avec l'article 5 c) de la convention du 28 janvier 1981 du Conseil de l'Europe qui dispose que les données collectées doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ?

Ainsi, l'application du principe de proportionnalité a amené la CNIL à considérer que la mise sous surveillance permanente des déplacements des personnes apparaît disproportionnée lorsque la tâche à accomplir ne réside pas dans le « déplacement » en lui-même, mais dans la réalisation d'une prestation pouvant faire elle-même l'objet d'une vérification (fiche d'intervention signée par le client…).

Par ailleurs, il convient de signaler que dans un arrêt du 26 novembre 2002, la chambre sociale de la Cour de cassation, visant les articles 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, 9 du Code civil, 9 du Nouveau Code de procédure civile et L. 120-2 du Code du travail, a considéré qu'une filature organisée par l'employeur pour contrôler et surveiller l'activité d'un salarié constitue un moyen de preuve illicite, sans reprendre la distinction antérieure suivant que le salarié a été ou non informé de l'existence d'un tel contrôle.

Elle estime, en effet, qu'une filature porte nécessairement atteinte à la vie privée du salarié sans pouvoir être justifiée, eu égard à son caractère disproportionné, par les intérêts légitimes de l'employeur. Dès lors, la question se pose de savoir si le fait de suivre les déplacements d'un salarié de façon permanente, dans l'hypothèse où ce dernier serait autorisé à utiliser son véhicule afin de se rendre à son domicile, pourrait être assimilé à une filature, quand bien même il en serait informé au préalable.

b) Optimisation des trajets

En revanche, la mise en œuvre de dispositifs de surveillance via GSM/GPS s'agissant de salariés dont la fonction même est de se déplacer (flotte de taxis, vigiles assurant des rondes…) permet à l'employeur d'optimiser l'organisation du travail. Un tel type de traitement est légitime sous réserve que l'information des personnes concernées soit correctement effectuée et que les finalités du traitement, ainsi que les conséquences résultant de l'analyse de ces données pour les salariés soient clairement indiquées à la Commission. Il apparaît également nécessaire que la durée de conservation soit proportionnée aux finalités poursuivies. À cet égard, l'article L. 122-44 dispose qu'aucun fait fautif ne peut donner lieu à lui seul à l'engagement de poursuites disciplinaires au-delà d'un délai de deux mois à compter du jour où

l'employeur en a eu connaissance, à moins que ce fait n'ait donné lieu dans le même délai à l'exercice de poursuites pénales. Dès lors, dans le cadre d'un contrôle de l'activité ou des horaires du salarié, la durée de conservation des données de localisation pourrait se limiter à ce laps de temps.

En conclusion, il apparaît que les choses sont plus claires dans le domaine de la vie professionnelle que dans la vie personnelle, en particulier en ce qui concerne la géolocalisation des enfants.

B. La constatation automatique des infractions routières

La lutte contre l'insécurité routière constituant une des priorités gouvernementales, la loi du 12 juin 2003 renforçant la lutte contre la violence routière a exploré certaines pistes juridiques nouvelles pour essayer de faire baisser le nombre de blessés et de morts sur les routes françaises. À côté de mesures pédagogiques ou préventives, la loi a aussi rendu possible la constatation de certaines contraventions au Code de la route par des appareils homologués de contrôle automatique (article L. 130-9 du Code de la route).

L'inscription dans la loi de ce mode de constatation des infractions et de sa valeur probante s'est traduite par la mise en place, après des tests concluants, d'une expérimentation à grande échelle concernant une centaine d'appareils de contrôle automatisés. Le ministère de l'Intérieur a en conséquence sollicité l'avis de la CNIL sur ce dispositif dénommé « système contrôle sanction automatique » (CSA), pour une durée d'un an, et permettant principalement, au titre de cette expérimentation, l'automatisation du contrôle et de la sanction des infractions aux limitations de vitesse.

1. LE DISPOSITIF TECHNIQUE

Le dispositif expérimental du « contrôle sanction automatique » repose, sur le terrain, sur le déploiement de cent radars, fixes ou mobiles, jumelés à des appareils photographiques numériques. Les clichés pris et les informations collectées sont ensuite transmis à une vingtaine de centres de supervision et de paramétrage, qui les communiquent à leur tour au centre de traitement national, qui gère et exploite le système d'informations automatisé du CSA et procède notamment à l'ensemble des opérations nécessaires au traitement des amendes (lecture et reconnaissance automatisées des photographies numériques, identification automatique du titulaire du certificat d'immatriculation du véhicule, édition et expédition des documents nécessaires et traitements des réponses, des contestations et des recours des contrevenants).

S'agissant de la reconnaissance automatisée des plaques minéralogiques à partir des clichés numérisés, la Commission a demandé au ministère de l'Intérieur de préciser, dans le bilan de cette expérimentation, le taux d'échec (non reconnaissance) et le taux d'erreur (attribution erronée) du logiciel utilisé.

L'ensemble du processus de traitement opéré au sein du centre de traitement national se fait sous la supervision d'officiers de police judiciaire et d'un officier du ministère public, placé sous l'autorité du procureur général de la juridiction concernée. La Commission a, sur ce point, demandé que l'arrêté créant ce traitement expérimental indique explicitement que le centre national de traitement est placé sous la responsabilité du procureur de la République dont dépendent les officiers de police judiciaire en charge de la supervision de ce centre.

Afin d'identifier le titulaire de la carte grise, redevable pécuniairement des amendes encourues sauf s'il apporte la preuve d'un vol de son véhicule, d'un événement de force majeure ou fournit les éléments permettant d'établir qu'il n'est pas l'auteur véritable de l'infraction, et de lui adresser l'avis de contravention correspondant, le centre national va procéder à un certain nombre de rapprochements et d'interconnexions de fichiers.

2. LES ÉCHANGES INFORMATIQUES

a) Les véhicules loués

C'est le fichier des véhicules loués, créé pour l'occasion et recensant uniquement la raison sociale et l'adresse des sociétés de location, personnes morales auxquelles ne s'appliquent pas les dispositions de la loi du 6 janvier 1978, qui sera consulté le premier lors de la phase d'identification du propriétaire du véhicule.

Cette consultation, par envoi automatique d'une requête, vise à obtenir directement du loueur concerné, les nom, prénom, date de naissance, adresse et numéro de permis de conduire du locataire du véhicule en infraction. L'automatisation de cette procédure d'interrogation a principalement pour objet, compte tenu du volume d'infractions potentiellement concernées par le « système contrôle sanction automatique », d'éviter de devoir submerger de requêtes les loueurs de véhicules. Si les loueurs de véhicules ne transmettent pas les informations relatives au locataire du véhicule au moment de la constatation des faits, ils devront mettre en œuvre la procédure de contestation prévue par l'article 529-10 du Code de procédure pénale.

Préalablement à tout échange de données, le centre national de traitement signera, avec chaque société de location de véhicules souhaitant utiliser cette possibilité d'échange, une convention prévoyant, notamment, l'impossibilité pour la société de location de garder trace des requêtes effectuées par le centre national de traitement et la mise en place de contraintes techniques d'échange informatique et de mesures destinées à assurer la sécurité des systèmes d'information des données et des mécanismes d'échange.

b) Le fichier national des immatriculations

Une fois cette première vérification effectuée, le fichier national des immatriculations, tenu par le ministère de l'Intérieur et créé par un arrêté du 20 janvier 1994, sera interrogé automatiquement afin d'obtenir l'adresse du titulaire du certificat d'immatriculation et de lui adresser l'avis de contravention correspondant. Cette

possibilité d'interrogation du fichier par des officiers ou agents de police judiciaire, dans l'exercice de leurs missions, résulte de la combinaison des articles L. 330-1 et L. 330-2 du Code de la route.

La Commission a estimé nécessaire, sur ce point, que la mise en place de cette interconnexion apparaisse explicitement dans l'arrêté du 20 janvier 1994 portant création du fichier national des immatriculations dans la mesure où la seule mention, au titre des destinataires des informations, des personnels visés à l'article L. 330-2 du Code de la route, ne fait pas apparaître clairement pour eux la possibilité nouvelle d'interroger automatiquement le fichier national des immatriculations.

c) Le fichier des changements d'adresse

Bien que la loi du 12 juin 2003 ait complété l'article 530 du Code de procédure pénale en instaurant une présomption selon laquelle l'adresse du titulaire du certificat d'immatriculation figurant au fichier national des immatriculations est son adresse actuelle et bien que le fait de ne pas déclarer ce changement d'adresse constitue une infraction, le choix a été fait, principalement pour des raisons de délais et de coûts, de vérifier à partir du fichier « Charade » de La Poste que le titulaire de la carte grise n'a pas changé d'adresse avant de lui adresser un avis de contravention.

Ce souhait a toutefois soulevé la question de la pertinence et de l'utilité de cette vérification au regard, d'une part, des erreurs figurant dans ce fichier — comme en attestent les nombreuses réclamations dont est saisie la Commission — et, d'autre part, de la présomption instituée par l'article 530 du Code de procédure pénale.

La Commission, tout en prenant acte que cette consultation concernera uniquement les personnes qui ne se sont pas opposées à la communication de leur nouvelle adresse, conformément à ses délibérations n° 02-071 du 15 octobre 2002 et n° 03-011 du 11 mars 2003 (*cf.* 23e rapport d'activité, p. 144 et ss., ainsi que le présent rapport), a toutefois demandé au ministère de l'Intérieur de procéder, au cours de l'expérimentation du « système contrôle sanction automatique », à l'évaluation des avantages et des inconvénients de cette procédure supplémentaire de vérification.

d) Les autres fichiers publics

À l'issue de la procédure, le dispositif expérimental devra, comme dans le cas où l'avis d'amende n'est pas adressé de façon automatique au contrevenant, transmettre au système national du permis de conduire le nombre de points retirés, soit que le contrevenant ait acquitté l'amende forfaitaire, soit qu'il l'ait contestée et qu'il ait fait l'objet d'une décision judiciaire le condamnant. Cette alimentation constitue, aux termes de l'article L. 225-1 du Code de la route, une obligation. Cet envoi d'informations sera effectué, pour des raisons de sécurité, par l'officier du ministère public et le système national du permis de conduire n'alimentera pas en retour le traitement du centre de traitement national.

Enfin, afin de pouvoir donner la suite adéquate aux infractions constatées (envoi d'une amende forfaitaire majorée, notamment), le centre national de

traitement doit obtenir des services du Trésor public les informations nécessaires quant à l'effectivité du paiement des amendes et des consignations par les débiteurs [1]. À cette fin, un échange d'informations est prévu, d'une part, avec le centre d'encaissement des amendes de Rennes s'agissant des amendes forfaitaires, d'autre part, avec les directions informatiques du Trésor, s'agissant des amendes forfaitaires majorées et des opérations de recouvrement. Cette transmission d'informations trouve son fondement dans l'arrêté du 18 juillet 1994 portant création du traitement automatisé de suivi du recouvrement des amendes et des condamnations pécuniaires.

3. LE FICHIER DES CONTREVENANTS

Au-delà des conséquences de ces différentes mises en relation et interconnexions, la Commission s'est prononcée également sur le fichier constitué par le centre national de traitement.

S'agissant des informations collectées, la Commission, tout en constatant qu'elles étaient pertinentes au regard de la finalité du traitement, a demandé que l'arrêté interministériel portant création du traitement, soit complété de façon à préciser que les clichés pris par les radars automatisés concernent le véhicule et ses passagers.

Bien que la durée de conservation des informations traitées soit expressément fixée par l'article L. 130-9 du Code de la route tel qu'issu de la loi du 12 juin 2003 et tout en prenant acte de la possibilité nouvelle offerte au contrevenant de demander au procureur de la République compétent d'ordonner l'effacement des informations le concernant lorsqu'il a récupéré le nombre de points retirés de son permis ou lorsque la procédure le concernant a donné lieu à une décision définitive de non-lieu ou de relaxe, la Commission a néanmoins recommandé au ministère de l'Intérieur de profiter de l'expérimentation de ce dispositif pour évaluer la pertinence du choix de fixer à dix ans et de façon uniforme cette durée de conservation.

S'agissant enfin du droit d'accès direct au cliché numérique constatant l'infraction, il a été indiqué à la Commission que son organisation pratique était susceptible de poser certaines difficultés dans la mesure où cette information, enregistrée dans la base du centre national de traitement, constitue à la fois une donnée nominative au sens de la loi du 6 janvier 1978 et une donnée relative à l'infraction pénale commise dont l'article 529-11 du Code de procédure pénale ne prévoit l'accès qu'en cas de contestation de l'infraction, et non pendant la phase administrative préalable.

Il a également été avancé qu'en permettant l'accès au cliché au titulaire du droit d'accès, ce dernier pourrait avoir accès à des informations ne le concernant pas, à savoir les personnes qui pourraient être photographiées en même temps que le conducteur et son véhicule.

1 Pour faciliter le paiement des amendes forfaitaires adressées par le centre national de traitement, le Trésor public a mis en place un système de télépaiement par serveur vocal et internet, à la création duquel la Commission a émis un avis favorable.

La Commission, consciente du caractère délicat de cette question — les droits institués par la loi du 6 janvier 1978 devant évidemment se conjuguer avec d'autres droits ou avec les règles de communication de pièces instituées par le Code de procédure pénale — a toutefois estimé contraire à la loi de limiter à certaines informations le droit d'accès des contrevenants qui se seraient acquittés du montant de l'amende sans la contester.

Elle a en conséquence demandé que les contrevenants aient accès à l'ensemble des informations les concernant en tant que propriétaire de véhicule, y compris le cliché, quitte à ce que des mesures soient prises pour masquer la partie du cliché ne le représentant pas et ainsi assurer la confidentialité des informations visuelles figurant sur le cliché et pouvant concerner d'autres personnes.

Sur ce point particulier, la Commission a également recommandé au ministère de l'Intérieur d'envisager une modification des règles de procédure applicables afin que le titulaire du certificat d'immatriculation du véhicule en infraction puisse avoir accès, dès réception de l'avis de contravention, à l'ensemble des informations le concernant, y compris la partie du cliché représentant le conducteur.

La Commission a ainsi pu, dans sa délibération n° 03-041 du 23 septembre 2003, émettre un avis favorable à la mise en œuvre expérimentale du « système contrôle sanction automatique ». Les demandes formulées par la CNIL dans sa délibération ont reçu une traduction concrète dans le texte de l'arrêté du 27 octobre 2003 portant création du système de contrôle sanction automatisé.

Un premier bilan de cette expérimentation sera présenté à la Commission au cours du premier semestre 2004.

C. L'alerte automatisée des conducteurs en excès de vitesse

Si l'enregistrement des numéros de plaque d'immatriculation par la puissance publique dans le cadre de la répression des infractions routières ne peut être contesté, il n'en est pas de même lorsque ces numéros sont exploités par une société d'autoroute.

a) En 1996

Il convient de rappeler que la CNIL, par une délibération n° 96-069 du 10 septembre 1996, avait émis un avis défavorable à la mise en œuvre d'un traitement reposant sur la lecture automatique des plaques d'immatriculation des véhicules aux points de péage par la société des autoroutes Paris-Rhin-Rhône (SAPRR), dont l'objet était de mesurer les temps de transit entre l'entrée et la sortie de la section à péage de l'autoroute et de détecter automatiquement un conducteur dans une situation « à risque », notamment, du fait de sa vitesse ou de la trop faible distance le séparant des autres, en vue éventuellement d'alerter les autorités compétentes. La SAPRR prévoyait de conserver les informations collectées pendant un mois sous forme indirectement nominative, puis de les conserver ensuite sous forme anonymisée à des fins statistiques.

La Commission avait considéré que ce dispositif portait atteinte à la vie privée et à la liberté fondamentale d'aller et de venir des personnes, dans la mesure où la possibilité de se déplacer anonymement n'était plus garantie, élément qui paraissait sans proportion avec la finalité qui lui était assignée. En outre, elle avait précisé que le recensement automatique d'infractions au Code de la route relevait exclusivement de missions de police judiciaire dont n'est pas investie une société concessionnaire d'autoroutes.

b) « Trop vite ! »

En 2003, la CNIL a eu à se prononcer sur un dispositif relativement similaire. En effet, la compagnie financière et industrielle des autoroutes (Cofiroute) l'a saisie d'une demande d'avis relative à une expérimentation permettant, par lecture et reconnaissance automatisées des plaques minéralogiques, le contrôle des vitesses moyennes des automobilistes circulant entre les points kilométriques 60,6 et 73 de l'autoroute A10 (entre Saint-Arnoult-en-Yvelines et Orléans).

Cofiroute souhaitait mettre en œuvre ce traitement à des fins pédagogiques et d'autorégulation. Il s'agissait d'alerter les automobilistes sur le fait qu'ils étaient en excès de vitesse sans que les informations relatives à la plaque d'immatriculation soient conservées ou transmises. Ainsi, en cas de dépassement de la vitesse maximale autorisée, Cofiroute prévoyait d'afficher le numéro de plaque minéralogique du contrevenant en clair sur un panneau à message variable en l'accompagnant d'un message de prudence (« Trop vite ! »). Le numéro de plaque minéralogique et le message de prudence étant affichés chacun deux fois une seconde, alternativement, toute possibilité de captation de l'information était quasiment impossible.

La Commission s'est alors interrogée sur le fait de savoir si les fins de pédagogie et d'autorégulation, bien que légitimes, imposaient une « personnalisation » aussi poussée de l'avertissement délivré par Cofiroute ainsi que la collecte et le traitement d'informations nominatives permettant de tracer, même fugitivement, les déplacements des personnes. En définitive, elle a considéré que le dispositif mis en place par la société Cofiroute pouvait être admis à titre expérimental dans la mesure où ni les numéros de plaques minéralogiques ni les autres informations enregistrées (date et heure de passage, vitesse) n'étaient conservés au-delà du temps nécessaire au calcul de la vitesse des véhicules et n'étaient pas retransmis à des tiers.

Elle a cependant demandé que toutes les dispositions soient prises en vue d'informer clairement les usagers, avant qu'ils n'entrent sur le tronçon de l'A10 concerné, des modalités de déroulement de cette opération et de son caractère expérimental par la remise de dépliants explicatifs aux gares de péage et par la diffusion d'une annonce sur la radio locale de l'autoroute.

Elle a enfin souhaité être rendue destinataire d'un bilan de cette expérimentation. La société Cofiroute a en conséquence adressé à la CNIL un rapport faisant état du bilan de six mois d'expérimentation, dans le cadre duquel elle a indiqué avoir abouti à des performances techniques satisfaisantes et stabilisées après une brève période de mise au point. Il est également précisé que le dispositif a permis de constater une baisse effective de la vitesse moyenne des véhicules tendant à confirmer

l'impact significatif de l'expérimentation et du déploiement des radars automatiques au niveau national. Le rapport précise par ailleurs que les automobilistes étrangers ont moins diminué leur vitesse que les autres. Enfin, à l'occasion d'une enquête effectuée par la société Cofiroute, les automobilistes ont indiqué être favorables à cette expérimentation et que cela les avait incités à réduire leur vitesse.

III. L'EXPÉRIMENTATION DU BRACELET ÉLECTRONIQUE

Afin de lutter contre la surpopulation carcérale et d'éviter à certains délinquants d'être incarcérés une première fois, de faciliter la réinsertion des condamnés en fin de peine ou bénéficiant d'une mesure de liberté conditionnelle et de ne pas rompre les liens familiaux et sociaux de certaines personnes condamnées à des peines courtes d'emprisonnement ferme, le ministère de la Justice a souhaité expérimenter le dispositif de placement sous surveillance à distance par bracelet électronique.

Ce procédé consiste à imposer à une personne, condamnée ou prévenue, de se tenir dans un lieu déterminé, en permanence ou pendant certaines plages horaires de la journée, et à pouvoir vérifier à distance que l'intéressé respecte bien les obligations qui sont les siennes.

La Commission a en conséquence été saisie d'un projet d'arrêté relatif à la mise en œuvre, dans neuf établissements pénitentiaires, d'un traitement automatisé de données nominatives, destiné à assurer la gestion des détenus placés sous surveillance électronique.

A. Aspects techniques et réglementaires

1. LE DISPOSITIF TECHNIQUE

Le premier dispositif de contrôle électronique a été inventé au milieu des années 1960 par un psychologue de Harvard, mais ce n'est qu'en 1983 qu'un délinquant est pour la première fois « assigné électroniquement à domicile » aux États-Unis. En 1987, trente-deux États recouraient à ce dispositif (pour un total de 2 300 délinquants) ; en janvier 1998, plus de 95 000 dispositifs de contrôle électronique étaient utilisés aux États-Unis.

Le type de dispositif choisi par l'administration pénitentiaire française repose sur trois éléments : un émetteur (le bracelet électronique fixé au poignet ou à la cheville de la personne placée sous surveillance électronique), un émetteur/récepteur (boîtier installé au domicile de l'intéressé et relié au réseau téléphonique filaire qui capte et décode les signaux émis par le bracelet et vérifie automatiquement son bon fonctionnement) et un centre de surveillance (installé au greffe de l'établissement pénitentiaire dont dépend la personne placée sous surveillance et reçoit les messages d'alerte envoyés par l'émetteur).

L'émetteur, inséré dans un bracelet que l'intéressé doit porter en permanence au poignet ou à la cheville pendant toute la durée de la mesure émet automatiquement des signaux radio d'une portée de plusieurs dizaines de mètres, à destination du récepteur installé au lieu d'assignation fixé par le juge. Cet émetteur détecte aussi automatiquement et en permanence la chaleur de la peau de son porteur pour vérifier que le bracelet n'est pas ôté ; de même, si l'intéressé tente de retirer ou de couper le bracelet-émetteur, celui-ci déclenche un message d'alerte de manipulation ; l'émetteur émet également un signal en cas de baisse de charge de sa batterie.

L'émetteur/récepteur, qui prend la forme d'un boîtier placé sous le poste téléphonique au lieu d'assignation est relié à la fois au secteur et au réseau téléphonique filaire. La faiblesse ou l'absence de réception des signaux traduit l'absence de la personne assignée. L'émetteur/récepteur adresse alors, par l'intermédiaire du réseau téléphonique, un message d'alerte au centre de surveillance. Comme le bracelet, l'émetteur/récepteur procède automatiquement à différents contrôles qui permettent de s'assurer du bon fonctionnement du dispositif permettant de détecter toute opération de retournement, de déplacement, d'ouverture et de détérioration. En cas de débranchement ou de coupure de la liaison téléphonique, l'activité de la personne placée sous surveillance est enregistrée dans la mémoire du récepteur, qui peut contenir jusqu'à mille événements.

Si l'émetteur/récepteur est à la fois débranché du secteur et déconnecté du réseau téléphonique, le dispositif adresse quatre messages d'alarme lors de son rebranchement signalant qu'il a été débranché du secteur, déconnecté, déplacé puis rebranché.

Le centre de surveillance, installé au greffe de l'établissement pénitentiaire concerné, constitue le troisième élément de ce dispositif. Le traitement mis en œuvre au sein de ce centre permet la gestion des placements sous surveillance électronique, de définir pour chaque détenu les violations des obligations liées à l'assignation, d'appeler automatiquement au domicile de la personne placée sous surveillance électronique, de vérifier le bon fonctionnement de l'ensemble du dispositif de surveillance (bracelet, récepteur et ligne téléphonique) et d'être informé en temps réel des éventuelles alarmes.

2. L'ENCADREMENT JURIDIQUE

C'est l'introduction, par la loi du 19 décembre 1997, des articles 723-7 à 723-14 dans le Code de procédure pénale qui a consacré le placement sous surveillance électronique comme modalité d'exécution des peines privatives de liberté pour les personnes condamnées à une peine privative de liberté inférieure à un an ou celles dont le reliquat de peine n'excède pas cette durée ; le placement peut également être ordonné à titre probatoire, dans le cadre d'une mesure de liberté conditionnelle, et pour une durée n'excédant pas un an.

La loi du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes, puis celle du 9 septembre 2002 d'orientation et de

programmation pour la justice ont étendu le bénéfice de cette alternative à l'emprisonnement aux mineurs non émancipés, sous réserve de l'accord des titulaires de l'exercice de l'autorité parentale, ainsi qu'aux prévenus qui, dans le cadre d'une mesure de contrôle judiciaire, ne doivent pas s'absenter du domicile ou de la résidence fixée par le juge d'instruction qu'aux conditions et pour les motifs déterminés par ce magistrat (article 138 du Code de procédure pénale).

Le placement sous surveillance électronique n'est possible qu'à des conditions très strictes, qui constituent autant de garanties. Ainsi :
— le recours à la surveillance électronique est décidé par le juge de l'application des peines soit d'initiative, soit sur demande du procureur de la République, soit sur celle du condamné ; ce dernier peut également demander que les conditions d'exécution de cette mesure soient modifiées, voire que cette dernière prenne fin ;
— la décision de recourir à cette mesure ne peut être prise qu'après avoir recueilli le consentement du condamné, donné en présence de son avocat ;
— le juge de l'application des peines fixe les périodes (jours et heures) et le lieu d'assignation (domicile, foyer, lieu d'emploi…) en prenant en compte les obligations du condamné en matière de travail, de formation et de soins médicaux, ainsi que le cadre de sa vie familiale ;
— le procédé utilisé pour détecter à distance la présence ou l'absence du condamné est homologué à cet effet par le ministre de la Justice et sa mise en œuvre doit garantir le respect de la dignité, de l'intégrité et de la vie privée de la personne ;
— les agents de l'administration pénitentiaire chargés du contrôle à distance du placement sous surveillance électronique ne peuvent pénétrer dans les domiciles sans l'accord des personnes chez qui le contrôle est effectué ;
— le juge de l'application des peines peut à tout moment désigner un médecin afin que celui-ci vérifie que la mise en œuvre du procédé de contrôle à distance du placement sous surveillance ne présente pas d'inconvénient pour la santé du condamné ; cette désignation est de droit lorsqu'elle est faite à la demande du condamné.

La nouvelle section ainsi introduite dans le Code de procédure pénale par la loi du 19 décembre 1997 modifiée a été complétée par un décret en Conseil d'État du 3 avril 2002 relatif au placement sous surveillance électronique, puis par un arrêté du 1er juillet 2002 portant homologation de ce procédé de surveillance électronique.

Le bénéfice de ce dispositif a été étendu par un décret du 17 mars 2004 aux personnes mises en examen ou prévenues placées sous contrôle judiciaire dans l'attente d'un jugement définitif. Cette extension devrait permettre de mettre simultanément trois mille personnes sous placement électronique en 2006.

B. Une difficulté : la télémaintenance

Une délégation de la CNIL s'est rendue le 31 janvier 2003 à la maison d'arrêt de Loos-lès-Lille pour se faire présenter concrètement le dispositif de placement sous surveillance électronique, qui y est utilisé depuis la fin de l'année 2000. Au début de l'expérimentation, les deux tiers des mesures y concernaient des personnes

bénéficiant d'une mesure de libération conditionnelle ; cette proportion est aujourd'hui de 40 % contre 60 % de condamnés.

La délégation a constaté que les surveillants, qui sont affectés exclusivement au contrôle des personnes placées sous surveillance électronique [1], faisaient preuve d'un grand pragmatisme tant dans la mise en œuvre de cette mesure que dans la gestion des alarmes éventuelles.

L'enquête sociale, prévue par le décret du 3 avril 2002, est aussi menée avec un soin tout particulier. Outre l'appréciation technique de l'installation du dispositif qui se fait *in situ* (vérification de l'état des différentes prises du lieu de résidence, réglage du périmètre d'émission), cette enquête vise à déterminer, à travers différents entretiens, si la mesure est adaptée à la situation de la personne concernée, notamment au regard de sa situation pénale et de sa situation familiale (certaines familles refusant l'installation du dispositif à leur domicile).

1. CONFORMITÉ AUX PRINCIPES DE LA LOI DE 1978

L'expérimentation menée par le ministère de la Justice apparaît légitime puisque cette mesure vise tout à la fois à éviter d'incarcérer des primo-délinquants — et donc de les mettre en contact avec des criminels chevronnés — et à réinsérer des détenus en fin de peine ou bénéficiant d'une mesure de liberté conditionnelle, ce d'autant que ce choix suppose l'adhésion de la personne concernée à la mise en place de la mesure et un accompagnement social, voire un contrôle du respect par l'intéressé des obligations imposées par le jugement de condamnation (soins, indemnisation de la victime, etc.).

Les informations nominatives enregistrées comme leur durée de conservation (elles sont effacées dès la fin de la mesure [2]) sont apparues pertinentes au regard de la finalité du traitement.

Les mesures de sécurité physiques et logiques, propres à des établissements pénitentiaires, qui bénéficient déjà de mesures particulières de protection, n'ont pas appelé d'observations particulières dans la mesure où seuls sont autorisés à accéder physiquement à ces dispositifs les agents de l'établissement pénitentiaire dûment habilités.

S'agissant des mesures de sécurité logique, chaque modification d'horaire est enregistrée dans un journal d'événements qui permet d'identifier l'auteur et le poste de travail sur lequel a été effectuée la modification. Lors de la généralisation du système à l'ensemble des établissements, des fichiers « logs » seront mis en place tant au niveau du système qu'au niveau applicatif.

1 Au 31 novembre 2002, 122 mesures ordonnées par sept tribunaux de grande instance, étaient terminées ou en cours à la maison d'arrêt de Loos et seules sept s'étaient soldées par un échec (non-respect des obligations, changement de situation pénale de l'intéressé, difficulté de fonctionnement).

2 Selon les indications chiffrées fournies par le ministère de la Justice, la durée moyenne d'une mesure de placement sous surveillance électronique est actuellement de trois mois.

2. LE PROBLÈME DE LA SOUS-TRAITANCE

La Commission a relevé que, dans le cadre de l'extension de cette expérimentation, des transmissions de données peuvent notamment avoir lieu entre les établissements pénitentiaires et les centres de télémaintenance des fournisseurs des matériels et logiciels, dont certains sont situés à l'étranger (notamment en Israël). En effet, outre les services classiques de maintenance sur site — en établissement —, les sous-traitants peuvent, à distance, effectuer des diagnostics en cas de panne puis assister le personnel pénitentiaire pour la résoudre, voire procéder à une opération de maintenance.

Outre la mise en place de mesures de sécurité physiques et logiques particulières (ligne téléphonique dédiée physiquement déconnectée du réseau téléphonique, numéro téléphonique de télémaintenance connu uniquement des deux prestataires, différentes bases tenues par l'établissement pénitentiaire sur des serveurs différents pour que les sous-traitants n'aient accès qu'à la base « PSE ») a été élaboré, en collaboration avec la Commission, un modèle de contrat que le ministère de la Justice conclura avec chacune des sociétés concernées.

Ce modèle de contrat reprend les principales dispositions protectrices de la loi du 6 janvier 1978 : il prévoit notamment les cas dans lesquels ces sociétés peuvent agir à distance sur les bases, prohibe toute réutilisation des données pour le compte de ces sociétés, rappelle que les informations transmises sont couvertes par le secret professionnel et impose des mesures de sécurité particulières pendant les transferts d'informations qui seront précisées dans des annexes à ces contrats. Ce modèle de contrat prévoit en outre que le contrôle du respect des engagements des parties pourra être effectué sur place par un membre de la Commission ou par une société de contrôle spécialisée ou un organisme d'audit désigné par la CNIL.

Le ministère de la Justice a précisé que lors de la phase de généralisation du placement sous surveillance électronique, il sera demandé aux deux sous-traitants de disposer de plate-forme de télémaintenance sur le sol français.

En conséquence de quoi, la Commission a émis un avis favorable au projet d'arrêté du ministre de la Justice portant création, au sein de neuf établissements pénitentiaires, d'un système de gestion informatisée des personnes placées sous surveillance électronique.

Chapitre 6

RAPPELS AUX ÉTABLISSEMENTS FINANCIERS

Dans son rapport d'activité 2002, la Commission relevait déjà le fait que de nombreuses personnes s'adressaient à elle pour contester leur inscription au Fichier national des incidents de remboursement de crédits aux particuliers (FICP). Constatant qu'un nombre important de ces plaintes étaient fondées, la Commission a décidé, en 2003, d'adresser des avertissements à quatre établissements financiers. Ces décisions, rendues publiques, ont été suivies d'effets positifs, les organismes avertis ayant renforcé le contrôle des procédures d'inscription au FICP au sein de leurs services.

Le FICP est un fichier de « particuliers surendettés » que la loi a voulu protéger, ce n'est pas un fichier de « mauvais payeurs » dont l'alimentation est laissée au bon vouloir des établissements financiers et encore moins une « liste noire » des clients indésirables. La CNIL entend le rappeler chaque fois que cela sera nécessaire.

Les risques d'exclusion de l'accès au crédit par le profilage individuel sont d'autant plus grands que les règles relatives aux modalités d'inscription au FICP ont été assouplies par le législateur et que, par ailleurs, les banques, les établissements de crédit et les services financiers de La Poste entendent affiner, par l'enregistrement de nouvelles données, leurs techniques de *Credit-Scoring*.

Par ailleurs des efforts ont été accomplis par les banques pour améliorer, dans les nouvelles conventions de compte, l'information de leurs clients s'agissant des droits qu'ils tiennent de la loi du 6 janvier 1978. Mais encore faut-il que ces droits puissent être exercés dans des conditions satisfaisantes. Trop de plaintes ont en effet été adressées à la CNIL en 2003 par des personnes qui ne parvenaient pas à exercer leur droit d'accès auprès de leur banque ou d'un établissement de crédit.

Il est vrai que la conciliation entre les droits des personnes sur leurs données et les obligations de vigilance qui pèsent sur les banquiers n'est pas toujours aisée. Dans le domaine de la lutte contre le blanchiment, la CNIL a proposé un équilibre qui semble recueillir un large consensus.

I. L'EXCLUSION BANCAIRE

A. Les inscriptions intempestives au FICP

1. DE NOMBREUSES PLAINTES FONDÉES

La Commission est régulièrement saisie de réclamations (une cinquantaine de plaintes pour l'année 2003) par des personnes inscrites au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, par l'établissement bancaire, l'organisme de crédit ou les services financiers de la Poste dont elles sont clientes. Soit ces personnes contestent le bien-fondé de leur inscription au FICP, soit elles ne parviennent pas à obtenir la mainlevée de cette inscription alors qu'elles ont régularisé l'incident de paiement qui en était à l'origine. Le travail de la CNIL et particulièrement de son service des plaintes et des requêtes générales consiste alors à vérifier la régularité de l'inscription au FICP, au vu des éléments fournis par le plaignant et par l'établissement financier mis en cause.

a) Rappel de la réglementation

Le règlement n° 90-05 du 11 avril 1990, modifié, du comité de la réglementation bancaire relatif au FICP fixe les règles d'alimentation et de consultation de ce fichier, géré par la Banque de France [1].

Lors de la survenance d'un incident de paiement caractérisé dans le remboursement d'un crédit, l'établissement financier doit inscrire son client au FICP.

Cette inscription du débiteur au FICP, fichier dont il convient de rappeler qu'il a été créé par la loi dite « Neiertz » relative à la prévention et au règlement des difficultés liées au surendettement des particuliers et des familles, entrée en vigueur le 1er mars 1990, permet aux banques, aux établissements de crédit et aux services financiers de La Poste, qui consultent le FICP, de disposer de cette information pour apprécier les risques liés à l'octroi d'un crédit à cette personne.

1 *Cf.* II — A du présent chapitre s'agissant des récentes modifications du règlement FICP.

Cette « mise en observation » du particulier dure au maximum cinq ans lorsque l'incident n'est pas régularisé (sauf pour les cas de surendettement ou de rétablissement personnel). Au-delà de ces cinq ans, l'incident de paiement est effacé.

S'agissant de la date à laquelle doit intervenir l'inscription d'un débiteur au FICP, le règlement n° 90-05 prévoit que dès qu'un incident de paiement est caractérisé dans le remboursement d'un crédit, l'établissement financier doit mettre en demeure son client de régulariser sa situation et doit, si le client ne régularise pas, procéder à l'inscription de son client au FICP. Cette inscription qui doit être effectuée sans délai, et non plusieurs mois voire plusieurs années après que l'incident de paiement a été caractérisé, marque le point de départ de la durée légale de cinq ans pendant laquelle le fichage durera si le client ne rembourse pas sa dette.

Le règlement n° 90-05 prévoit enfin qu'un même incident de paiement ne peut pas donner lieu à plusieurs inscriptions successives au FICP.

b) Instruction des réclamations

Lorsque l'inscription est fondée, la CNIL informe le requérant de la réglementation en vigueur.

Dans un certain nombre de cas, l'instruction des réclamations dont la CNIL est saisie permet d'établir que l'inscription est abusive (infondée), tardive (inscription bien après la date réelle de l'incident de paiement) ou qu'elle aurait dû être levée par l'établissement financier (lorsque le débiteur a réglé la totalité de sa dette, ou qu'une décision de justice est intervenue, par exemple). La CNIL est alors amenée à demander à l'établissement financier concerné de prendre des mesures de nature à empêcher que ces faits ne se reproduisent (rappel des règles de fonctionnement du FICP auprès de ses services, par exemple).

Si pendant plusieurs années, la CNIL a ainsi privilégié la pédagogie en rappelant aux établissements financiers leurs obligations s'agissant de l'inscription de leurs clients au FICP, elle a décidé, en 2003, tout en poursuivant ses actions pédagogiques, de délivrer des avertissements, rendus publics, à certains établissements financiers qui ne respectaient manifestement pas la réglementation relative au FICP.

En effet, la CNIL a non seulement constaté une recrudescence du nombre d'inscriptions « abusives » au FICP, mais aussi le fait, pour les personnes fichées à tort au FICP, de devoir s'adresser à la Commission le plus souvent en « dernier recours », l'établissement les ayant fichés demeurant sourd à leurs démarches tendant à obtenir un « défichage ».

2. QUATRE AVERTISSEMENTS

a) Pédagogie par l'exemple

En choisissant de délivrer des avertissements à quatre établissements financiers, la CNIL a souhaité avant tout rappeler à l'ensemble de la profession le nécessaire respect tant des dispositions de la loi du 6 janvier 1978 relative à

l'informatique, aux fichiers et aux libertés, que du règlement n° 90-05 du 11 avril 1990 du Comité de la réglementation bancaire, modifié relatif au FICP.

Elle a voulu notamment rappeler aux établissements financiers que le FICP ne constitue aucunement une « liste noire » des « clients indésirables ». En effet, si en adoptant la loi du 31 décembre 1989 le législateur a entendu mettre en place un dispositif de prévention et de traitement des situations de surendettement, et a ainsi prévu la création du FICP, il a également souhaité que le fonctionnement de ce fichier soit strictement encadré.

Ainsi, en fixant à cinq ans la durée maximale du fichage au FICP, le règlement n° 90-05 du Comité de la réglementation bancaire relatif au fonctionnement du FICP, pris en application de la loi du 31 décembre 1989, a instauré le principe selon lequel un particulier qui n'a pas remboursé un établissement de crédit au terme de ce délai, s'il demeure débiteur de la somme vis-à-vis de son créancier, est automatiquement radié du FICP.

b) Les abus relevés

En pratique, l'instruction de quatre réclamations a conduit la CNIL, en 2003, à délivrer un avertissement aux établissements suivants :
— Fortis Banque (délibération n° 03-018 du 24 avril 2003) ;
— Crédit Agricole mutuel du Nord (délibération n° 03-033 du 19 juin 2003) ;
— Crédit immobilier de France-Ile-de-France (délibération n° 03-051 du 20 novembre 2003) ;
— Crédit Mutuel du grand Cronenbourg (délibération n° 03-052 du 20 novembre 2003).

Fortis Banque a fiché M. X. au FICP en août 2001. L'instruction du dossier a montré que ce client était débiteur de cette banque et qu'un incident de paiement caractérisé était intervenu en 1996, soit cinq ans avant son inscription effectuée en août 2001.

La Caisse régionale de crédit agricole mutuel du Nord a fiché abusivement M. Y. en août 2002, pour un incident de paiement datant de 1994, plusieurs décisions de justice étant intervenues dans l'intervalle. À la suite de l'instruction de ce dossier par la CNIL, cet établissement a défiché M. Y., reconnaissant que même si ce client lui devait de l'argent, il n'avait pas à être inscrit au FICP. Pourtant, quelques mois plus tard, cet établissement financier a réinscrit M. Y. au FICP, qui a à nouveau saisi la CNIL de ces faits.

Le Crédit immobilier de France — Ile-de-France — a inscrit M. Z. au FICP au mois d'août 2002 alors que l'incident de paiement avait eu lieu en 1991, soit onze ans auparavant. Là encore, un contentieux existait entre M. Z. et sa banque depuis de nombreuses années.

Le Crédit mutuel du grand Cronenbourg a maintenu l'inscription de M^me^ W. au FICP pendant près de dix-huit mois après la régularisation de l'incident.

Dans tous ces cas, seule l'intervention de la CNIL a permis le « défichage » des personnes concernées qui avaient vainement tenté de l'obtenir auprès de leur banque pendant plusieurs mois.

La CNIL a par ailleurs décidé de transmettre ces délibérations portant avertissement à la Commission bancaire, organisme public compétent pour prononcer des sanctions disciplinaires à l'encontre des établissements financiers qui ont enfreint une disposition législative ou réglementaire afférente à leurs activités (article L. 613-21 du Code monétaire et financier).

B. La réforme du surendettement

La Commission a été saisie le 17 novembre 2003 d'un projet de règlement modifiant le règlement n° 90.05 du Comité de réglementation bancaire et financière du 1er avril 1990 relatif au fichier des incidents de remboursement des crédits aux particuliers (FICP). Le projet de règlement a pour objet de prendre en compte les modifications [1] apportées à la procédure de surendettement des particuliers résultant des dispositions relatives au « rétablissement personnel » insérées dans la loi d'orientation et de programmation pour la ville et la rénovation urbaine du 1er août 2003 [2], dite « loi Borloo ».

1. LES MODIFICATIONS RÉSULTANT DE LA LOI DU 1er AOÛT 2003

La loi du 1er août 2003 crée la procédure de rétablissement personnel et élargit la définition et le périmètre du surendettement. L'engagement donné de cautionner ou d'acquitter solidairement la dette d'un entrepreneur individuel ou d'une société dès lors que l'intéressé n'a pas été, en droit ou en fait, dirigeant de celle-ci est ajouté à la définition précédente du surendettement comme étant l'impossibilité manifeste pour des débiteurs de faire face à l'ensemble de leurs dettes exigibles et à échoir, est ajouté (Code de la consommation article L. 330-1). Les dettes fiscales sont désormais incluses alors qu'elles étaient exclues du plan, et traitées séparément, et certaines mesures durcissent le dispositif de traitement du surendettement. Ainsi :
— les créances dont le prix a été payé au lieu et place du débiteur par la caution ou le coobligé ne peuvent faire l'objet d'un effacement ;
— la durée maximale du moratoire pour les débiteurs insolvables dont la situation n'est pas irrémédiablement compromise et qui ne relèvent donc pas de la procédure de rétablissement personnel est réduite de trois à deux ans ;

1 Ces dispositions sont désormais incluses dans les articles L. 331-1 et suivants du Code de la consommation relatifs au surendettement des particuliers et L. 628-1 et suivants du Code de commerce relatifs à la faillite civile applicable en Alsace-Moselle.

2 Loi d'orientation et de programmation pour la ville et la rénovation urbaine n° 2003-710 du 1er août 2003 publiée au *Journal officiel* du 2 août 2003.

— la durée d'inscription au FICP en cas d'adoption d'un plan conventionnel ou de recommandations est fixée à la durée de ces mesures sans pouvoir excéder dix ans [1], au lieu de huit ans auparavant (Code de la consommation article L. 333-4).

Par ailleurs, pour éviter que l'instruction du dossier par la commission ne soit trop longue, il est prévu un délai de six mois [2] à compter du dépôt du dossier pour son instruction et pour la décision à prendre concernant son orientation (Code de la consommation article L. 331-3, al. 1).

Des aménagements réglementaires figurant dans le projet de règlement présenté à la CNIL résultent directement de l'application de ces dispositions.

a) Une nouvelle définition des situations de surendettement

L'article 1 du règlement 90.05 du Comité de la réglementation bancaire et financière (CRBF) est modifié afin de redéfinir les situations de surendettement et d'y inclure la procédure de rétablissement personnel.

Trois situations sont désormais visées :
— les dossiers en cours d'instruction à la suite d'une part, des saisines par les débiteurs de la commission de surendettement instituée à l'article L. 331-1 dudit Code et, d'autre part, des décisions de recevabilité prononcées par les juges de l'exécution ;
— les mesures conventionnelles constituées des plans conventionnels de redressement établis, par la commission susvisée, en vertu de l'article L. 331-6 dudit Code ;
— les mesures judiciaires. Sont considérées comme mesures judiciaires pour l'application du présent règlement : les recommandations émises en vertu des articles L. 331-7 et L. 331-7-1 dudit Code, par la commission susvisée, auxquelles le juge a conféré force exécutoire en application de l'article L. 332-1 ; les mesures prises par le juge statuant dans le cadre de la procédure prévue aux articles L. 332-2 et L. 332-3 dudit Code ; les procédures de rétablissement personnel visées aux articles L. 332-5 et suivants du Code de la consommation.

b) L'inscription au FICP des dossiers de surendettement en cours d'instruction

L'inscription au FICP des dossiers en cours d'instruction dès la saisine de la Commission de surendettement par le débiteur constitue, après l'instauration de la procédure de rétablissement personnel, la deuxième grande innovation de la réforme du surendettement.

Le projet de règlement transcrit les dispositions de la loi en prévoyant l'enregistrement comme dossier en cours d'instruction des saisines de la commission instituée à l'article L. 331-1 du Code de la consommation qui sont communiquées par

1 Ce délai de dix ans correspond à celui retenu pour la durée maximale du plan conventionnel et de mesures recommandées (à l'exception des emprunts immobiliers liés à l'achat de la résidence principale), ainsi qu'il résulte des articles L. 331-3, al. 6) et L. 331-6, al. 5. et L. 331-7, 1°) du Code de la consommation.

2 Ce délai est à rapprocher du délai de neuf mois à l'issue duquel le débiteur demandeur à une procédure en rétablissement personnel peut saisir le juge de l'exécution aux fins d'ouverture de la procédure si la commission n'a pas instruit et décidé de l'orientation du dossier. (Article L. 332-5 al. 2 du Code de la consommation).

celle-ci à la Banque de France et des décisions de recevabilité prises par le juge de l'exécution en cas de recours qui sont communiquées à la Banque de France par le greffe du juge de l'exécution en application du 3e alinéa de l'article L. 333-4 dudit Code.

Deux modifications d'inspiration réglementaire viennent compléter ce dispositif [1] :

— une disposition formelle : la saisine de la commission de surendettement par le débiteur se traduit par la signature du débiteur apposée sur la déclaration de surendettement comportant les mentions suivantes : les noms patronymique et marital, prénoms, date de naissance, code géographique du lieu de naissance ou, dans l'ignorance de celui-ci, lieu de naissance des débiteurs ;

— une disposition de fond tenant à la durée de l'inscription provisoire : l'inscription des dossiers en cours d'instruction est conservée dans le fichier pour une durée de trente-six mois et peut faire l'objet de prorogation par période d'un an décidée par la commission.

S'agissant de la radiation de l'inscription, des modifications sont apportées afin d'inclure les nouveaux cas de figure. L'inscription est radiée :

— lorsque le dossier est irrecevable à la procédure de traitement du surendettement. La commission informe la Banque de France de cette irrecevabilité à l'expiration du délai de recours de sa décision. Le greffe du juge de l'exécution communique à la Banque de France le jugement confirmant l'irrecevabilité ;

— lorsque le débiteur bénéficie d'une mesure prise en vertu des articles L. 331-6, L. 331-7 ou L. 331-7-1 susvisés ;

— lorsque le débiteur bénéficie d'une procédure de rétablissement personnel prise en vertu des articles L. 332-5 et suivants susvisés ;

— en cas de clôture du dossier de surendettement prononcée par la commission, notamment lorsque le débiteur fait part de sa volonté de ne pas poursuivre la procédure ou lorsqu'il ne fournit pas les éléments nécessaires à cet effet ;

— en cas d'extinction de l'instance devant le juge de l'exécution portée à la connaissance de la Banque de France par le greffe.

c) L'allongement des durées de conservation des inscriptions

L'article L. 331-6 du Code de la consommation, tel que modifié par la loi du 1er août 2003, dispose que la durée totale du plan, y compris lorsqu'il fait l'objet d'une révision ou d'un renouvellement, ne peut excéder dix années. L'article L. 331-7 retient cette même durée pour les recommandations pouvant être émises par la commission, à une exception près : la possibilité d'excéder la durée de dix ans lorsqu'est concerné le remboursement de prêts contractés lors d'achat d'un bien immobilier constituant la résidence principale et dont les recommandations de la commission permettent d'éviter la cession.

Ces dispositions se traduisent dans le projet de règlement par l'allongement de la durée maximale d'inscription dans le FICP des informations concernant les

1 *Cf. supra* II A §2.

mesures du plan conventionnel et les recommandations exécutoires qui passe de huit ans à dix ans (article 8*bis* 2° du projet de règlement).

2. LES MODIFICATIONS RÉSULTANT D'UNE INITIATIVE RÉGLEMENTAIRE

a) Un accès immédiat au FICP

Répondant à une attente des professionnels et allant dans le sens d'une rapidité de l'information de la communauté des établissements de crédit sur l'inscription de nouveaux incidents de paiement, le projet de règlement prévoit que les déclarations d'incidents de paiement et la consultation du FICP pourront être effectuées par échanges sécurisés sur internet, aussi bien que par remise ou télétransmission d'un fichier informatique sécurisé.

Les modalités pratiques de l'accès par internet et les mesures de sécurité ont été décrites et examinées par les services de la CNIL à l'occasion de la demande d'avis relative [1] à un portail sécurisé d'accès aux fichiers tenus par la Banque de France qui a fait l'objet d'un avis tacite.

La possibilité d'alimenter ou de consulter le fichier par l'utilisation d'un imprimé est conservée, de même que la consultation par vidéotex. Est toutefois supprimée la possibilité de se voir remettre une bande magnétique (ou tout autre support informatique scellé).

Cette modification a notamment pour effet de rendre accessible en temps réel l'information contenue dans le FICP et permet de renforcer la prise en compte de l'obligation de sécurité et de mise à jour résultant de l'application de l'article 29 de la loi du 6 janvier 1978.

b) Une définition plus large de l'incident de paiement caractérisé

Le projet de règlement vise à l'accélération de la détection des incidents de paiement, dans une optique de prévention du surendettement. Les termes et seuils à atteindre avant de qualifier un défaut de paiement en incident caractérisé, pouvant dès lors donner lieu à une inscription au FICP, sont respectivement réduits d'une échéance ou d'un mois.

Ainsi, pour un même crédit comportant des échéances échelonnées, le montant cumulé entraînant une inscription au FICP est porté, pour les crédits remboursables mensuellement, au double de l'échéance mensuelle au lieu du triple, et, dans les autres cas, à l'équivalent d'une échéance, lorsque ce montant demeure impayé pendant plus de 60 jours (au lieu de 90 jours).

Lorsque le crédit ne comporte pas d'échéances échelonnées (cas d'une autorisation de découvert), sont caractérisés les défauts de paiement réunissant une

1 DA n° 866088 du 11 août 2003 ayant reçu l'avis tacite n° 034528 du 2 octobre 2003 avec effet au 10 octobre 2003.

double exigence en terme de retard et de seuil : les sommes exigibles plus de 60 jours (au lieu de 90 jours) après la date de mise en demeure du débiteur d'avoir à régulariser la situation, dès lors que le montant des sommes impayées est au moins égal à 500 euros.

3. LES EFFETS DE L'ABAISSEMENT DU SEUIL D'INSCRIPTION

L'abaissement du seuil d'inscription a particulièrement retenu l'attention de la Commission lors de l'examen du projet de règlement modifié du CRBF. En effet, s'il n'appartient pas à la Commission de fixer le seuil permettant de caractériser l'incident de paiement, elle a constaté que ces mesures auront des répercussions certaines sur le nombre de personnes fichées et potentiellement sur le nombre de contestations dont la Commission est saisie, alors que dans le même temps est noté un accroissement des plaintes relatives au non-respect des conditions d'inscription au FICP par les établissements de crédit.

La Commission a ainsi appelé, tout en émettant un avis favorable au projet de règlement dans sa délibération n° 03-050 du 20 novembre 2003, à encore plus de rigueur dans la gestion du fichier du fait de la redéfinition des conditions d'inscription.

La Commission a ainsi tenu à rappeler dans son avis que, s'agissant du FICP :
— la proportionnalité et la pertinence du traitement doivent être préservées ;
— le nombre de plaintes reçues justifie son inquiétude quant aux conditions de respect par les établissements de crédit du règlement du CRBF ;
— elle fera preuve d'une vigilance particulière sur les suites données à l'instruction des réclamations dont elle est saisie.

Par ailleurs, elle a attiré l'attention des autorités de contrôle des activités financières sur ce point ainsi que sur l'intérêt de la mise en place, au sein de la Banque de France, d'une instance de médiation chargée notamment, en liaison avec les médiateurs des établissements de crédit, de faciliter l'exercice des droits de rectification et d'opposition des personnes inscrites au FICP.

L'arrêté du 29 janvier 2004 publié au *Journal officiel* du 26 février 2004 a homologué le règlement n° 2004-01 modifiant le règlement n° 90-05 du 11 avril 1990 modifié relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP). Le texte adopté, hormis des modifications formelles (numérotation notamment) reprend l'intégralité des dispositions présentes dans le projet en y intègrant à l'article 3 la possibilité pour les établissements de ne pas déclarer les incidents de paiement d'un montant inférieur à 150 euros qui n'ont pas fait l'objet d'une déchéance du terme. Cette modification s'inscrit dans une prise en compte de la pertinence du traitement avec la fixation d'un seuil d'inscription destiné à caractériser l'incident donnant lieu à inscription.

La Commission appréciera lors de l'examen de la demande d'avis modificative de la Banque de France relative aux modalités de fonctionnement du FICP les mesures prises pour assurer le respect des dispositions du règlement du CRBF, tout particulièrement les mesures destinées à prévenir le détournement de finalité.

C. Les normes d'exclusion de crédit

La Commission a déjà eu à se prononcer à de multiples reprises sur la technique du *Scoring*, procédé automatisé d'aide à la décision mis en œuvre par les établissements bancaires et financiers dans le cadre de leur gestion commerciale. C'est ainsi que dans une délibération n° 88-083 du 5 juillet 1988 portant recommandation relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit, dont l'élaboration avait fait l'objet d'une concertation avec les professionnels concernés, la CNIL a précisé que le calcul automatisé de l'appréciation du risque devait faire l'objet d'une déclaration ordinaire comportant les informations traitées et les caractéristiques du processus d'établissement du score, c'est-à-dire les variables utilisées et leur pondération. Pour satisfaire aux dispositions de l'article 2 de la loi du 6 janvier 1978 qui prohibe toute prise de décision *« impliquant une appréciation sur un comportement humain »* sur le *« seul fondement d'un traitement automatisé donnant une définition du profil ou de la personnalité de l'intéressé »*, les établissements de crédit se sont engagés à procéder à un examen systématique du dossier [1]. Cette recommandation a été modifiée par une délibération n° 98-101 du 22 décembre 1998 qui a été annulée par le Conseil d'État par décision du 30 octobre 2001 [2]. Depuis lors, l'utilisation du score a connu de multiples évolutions que la Commission a examinées en séance plénière le 4 février 2003.

1. DE NOUVELLES FINALITÉS DU SCORE : OUTIL MARKETING ET ÉVALUATION DU RISQUE

Si les crédits à la consommation étaient jusqu'à présent le terrain d'élection de l'application des techniques de *Scoring*, il ressort de déclarations récentes reçues par la Commission que certains établissements de crédit, s'alignant d'ores et déjà sur les recommandations du comité de Bâle II relatives aux exigences en matière d'adéquation des fonds propres, utilisent des scores de risque, à l'occasion d'une demande d'ouverture d'un compte courant, afin de se prononcer sur l'opportunité d'accepter le nouveau client ou de lui consentir tel mode de paiement (chéquier, type de carte bancaire, facilité de caisse, découvert). En matière de prospection commerciale, les établissements de crédit ont développé des outils visant à sélectionner la clientèle susceptible d'être intéressée par les produits proposés (scores d'appétence ou de propension). Il ne s'agit plus des modèles classiques de segmentation comportementale de la clientèle bancaire car ces produits incluent des scores de risque afin d'exclure certaines personnes compte tenu du risque contractuel présenté.

Les établissements de crédit sont conduits à collecter un nombre croissant d'informations à l'ouverture du compte, cette tendance étant renforcée par les contraintes pesant sur les établissements de crédit, issues de la législation anti-blanchiment. Ils sont également amenés à utiliser des grilles de *Scoring* comportant un

1 La CNIL a cependant observé, à l'occasion de missions de contrôles menées en 1998, que le pourcentage des crédits accordés après un score insuffisant était inférieur à 0,02 %.

2 Affaire n° 204909 Association des sociétés financières et autres. *Cf.* délibération n° 98-101 du 22 décembre 1998 de la CNIL.

nombre de variables plus important, dont on peut se demander si elles ne sont pas de nature à porter atteinte au devoir de non-ingérence du banquier lorsqu'elles concernent le nombre et le montant des prélèvements vers des organismes de crédit concurrents, le solde net du foyer, et non du titulaire du compte, la détention d'une assurance extérieure à la banque, le nombre de paiements par carte à l'étranger, le montant de l'assurance-vie.

2. DE NOUVELLES VARIABLES DANS LES GRILLES DE SCORE

Les éléments traditionnellement retenus comme paramètres significatifs dans les grilles de score sont l'identité (complétée par l'âge du demandeur, le lieu de naissance et le cas échéant, la qualité du titre de séjour), la date de fin du séjour, l'ancienneté à l'adresse courante, la situation familiale (composition du foyer, personnes à charge), les données socio-économiques (profession et ancienneté à l'emploi de l'emprunteur et du conjoint, l'adresse de l'employeur, le ratio charges/ressources, la domiciliation bancaire, l'ancienneté dans l'établissement bancaire, le statut de l'habitation), les caractéristiques du financement envisagé (montant du crédit, durée du crédit, pourcentage d'apport personnel).

La pratique récente met en lumière l'intégration dans les grilles de *Credit Scoring* de nouvelles variables parmi lesquelles figurent : l'adresse du lieu de résidence, le segment de clientèle dans lequel se situe le client, le prénom, la différence d'âge entre l'emprunteur et son conjoint, ce qui n'est pas sans poser des problèmes au regard de la loi du 6 janvier 1978.

a) Le lieu de résidence

L'intégration du lieu de résidence dans la grille de score concrétise la crainte d'une utilisation des techniques d'îlotage négatif pour l'octroi du crédit. Il convient de rappeler que l'îlotage consiste à déterminer non pas le profil d'une personne, mais d'un territoire (l'îlot) dont les caractéristiques seront supposées être celles du groupe, de ses habitants. Certaines des déclarations adressées à la Commission intègrent l'utilisation de techniques d'îlotage non plus à des fins de prospection commerciale mais à des fins d'octroi de crédit (l'îlotage est dit négatif lors qu'il est utilisé à des fins d'exclusion), par l'intégration de l'adresse dans les grilles de score et la pondération particulière attribuée à chaque adresse.

Ainsi, l'adresse peut être prise en compte de plusieurs manières. Dans un cas, l'appartenance à une commune ayant un taux de maisons individuelles inférieur ou égal à un certain taux, ou à une agglomération « sensible », entraînera l'attribution d'une pondération négative. Dans l'autre, la pondération pourra varier en fonction de la taille de l'agglomération.

Jusqu'à présent, les professionnels faisaient valoir que l'application des techniques d'îlotage négatif avait été écartée en France dans le secteur du crédit en raison du manque de pertinence de l'outil, l'îlot étant défini en France de façon trop large et ne permettant pas de déterminer de profils sociologiques suffisamment

proches de la réalité pour être pertinents. Il semble qu'un stade soit franchi par certains établissements.

b) Le code segment de clientèle

Les établissements bancaires ont mis en œuvre de longue date des procédés de notation et de segmentation dite comportementale de leur clientèle sur lesquels la Commission s'était prononcée par une délibération n° 93-032 de 1993 [1]. Cette classification permet de gérer les portefeuilles de clientèle et de définir des plans d'action commerciale et de développement. Ce segment interne de l'établissement est parfois intégré dans les grilles de score et reçoit une pondération, ce qui montre l'interaction croissante entre la segmentation comportementale et le score.

c) Le prénom, le sexe, la différence d'âge

Bien que l'utilisation de ces variables soit très marginale, la Commission a pu constater l'utilisation de variables telles que le prénom, le sexe de l'emprunteur, la différence d'âge entre l'emprunteur et son conjoint. Une telle utilisation, quand bien même des corrélations pourraient être trouvées entre la variable et le risque de défaut de l'emprunteur, n'est pas compatible avec le principe de proportionnalité.

Le *Scoring* du prénom, s'il devait être admis, conduirait soit à une discrimination raciale interdite, soit à l'imputation d'une pondération négative au prénom d'une personne sur la seule base d'éléments statistiques, en l'absence de lien de causalité entre la variable et le défaut constaté. Si le prénom est susceptible de déterminer des probabilités d'appartenance à une tranche d'âge, ce critère manque de pertinence pour l'appréciation du risque, le prénom ne pouvant refléter une probabilité dans la génération d'événements considérés comme des risques opérationnels (risque de fraude, d'erreur…).

S'agissant du genre, la pondération affectée par certains organismes constitue une discrimination positive en faveur des femmes. Si ce principe a été admis en matière d'assurance automobile, sur la base d'éléments statistiques de nature à déterminer un profil de conducteur des personnes de sexe féminin (moins de tendance à l'alcoolémie, moins d'excès de vitesse…), la Commission s'interroge sur la pertinence de cette discrimination positive en matière d'appréciation du risque de crédit. De même, la prise en compte de la différence d'âge entre un emprunteur et son conjoint paraît peu pertinente au regard de la finalité.

Il est intéressant de noter qu'aux États-Unis (où est née la technique du *Credit Scoring*), la prise en compte de la nationalité de même que celle de la race, du statut marital, du sexe, est interdit aux termes d'un *Equal Credit Opportunity Act*.

1 Délibération relative au contrôle effectué le 2 octobre 1992 à la Caisse régionale de crédit agricole de Dordogne.

II. LES DROITS DU CLIENT

A. Protection de données et lutte contre le blanchiment d'argent

Si la lutte contre le blanchiment d'argent et le financement du terrorisme est une composante à la fois nécessaire et précieuse de nos sociétés démocratiques, le respect des droits fondamentaux et des libertés individuelles, en particulier le droit à la vie privée et la protection des données personnelles, doivent être assurés. À cet égard, la CNIL a adopté le 7 octobre 2003 un rapport d'étape, non publié, afin d'apporter un éclairage sur ces questions. L'activité de contrôle mise en œuvre par les organismes financiers, dont la légitimité ne saurait être contestée, doit s'exercer dans le respect des règles fondamentales relatives à l'informatique et aux libertés.

1. « SURVEILLE TON CLIENT »

La récurrence des questions relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme n'a pas manqué de raviver la volonté des organismes financiers de mieux connaître leurs clients, principe d'action désormais consacré par les services de *Private Banking* sous la formule *Know your Customer* [1], règle d'application générale exigeant de la part des organismes financiers l'identification systématique du client et, le cas échéant, celle de l'ayant droit économique lors d'une ouverture de compte. Ces règles visent également à élaborer des directives jugées appropriées dans le cadre des relations avec la clientèle bancaire.

Invoquant l'importance des obligations de vigilance mises à leur charge ainsi que le risque pénal encouru par les dirigeants sociaux, les organismes financiers ont ainsi été conduits à mettre en œuvre de nouveaux systèmes automatisés de surveillance de la clientèle.

Le rapport d'étape insiste sur la nécessité de veiller à ce que les moyens mis en œuvre dans le cadre de la surveillance de clients soient proportionnés à ce que justifie la finalité d'une telle démarche. À cet égard, ainsi que l'illustre l'avis adopté le 14 décembre 2001 par le groupe article 29 [2], les mesures de lutte contre le blanchiment d'argent et le terrorisme ne devraient pas avoir pour effet de réduire les niveaux de protection des droits fondamentaux qui caractérisent nos sociétés démocratiques.

En référence à l'article 2 de la loi du 6 janvier 1978, le rapport d'étape rappelle que l'ensemble des systèmes experts développés par les organismes financiers, devraient être utilisés comme un élément d'information et d'alerte, outil d'aide à la décision qui ne saurait se substituer à la décision définitive de l'organisme financier concerné, seul à même d'assurer une utilisation cohérente, efficace et non

1 *« Connais ton client ».*

2 Voir les travaux du « groupe de l'article 29 » et en particulier l'avis 10/2001 sur la nécessité d'une approche équilibrée dans la lutte contre le financement du terrorisme, adopté le 14 décembre 2001, 0901/02/FR/final.

disproportionnée des outils mis en œuvre dans le cadre de la lutte contre le blanchiment d'argent et le terrorisme.

2. LA CONFIDENTIALITÉ DES INFORMATIONS COLLECTÉES

Les nécessités de la lutte anti-blanchiment et la tentation du « tout transparent » ne doivent pas faire oublier l'existence de règles strictes relatives au partage d'informations nominatives, en particulier, mais non exclusivement, au regard du secret professionnel prévu à l'article L. 511-33 du Code monétaire et financier.

a) Le partage d'informations

L'article 29 de la loi du 6 janvier 1978 dispose en effet que : *« Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés »*. Ainsi, alors que le secret professionnel ne protège que les informations à caractère secret, en interdisant leur divulgation, les règles définies par la loi informatique et libertés s'appliquent à toutes les données directement ou indirectement nominatives.

Ces dispositions viennent conjointement, et de façon complémentaire, assurer une confidentialité certaine aux données portées à la connaissance des organismes financiers.

Si le dispositif légal entourant la lutte contre le blanchiment d'argent autorise un établissement de crédit à lever le secret bancaire au bénéfice de la cellule TRACFIN ou de certaines autorités de contrôle, aucune disposition n'autorisait jusqu'alors cette levée concernant des traitements internes aux établissements de crédit et qui sont, par exemple, mutualisés au sein d'un groupe. Cette question est particulièrement importante pour les établissements bancaires institués en réseau qui n'avaient pas manqué de faire valoir auprès de la CNIL les difficultés rencontrées en l'absence d'éclaircissements du législateur. La loi n° 2003-706 [1] de sécurité financière du 1er août 2003 a néanmoins levé, sur ce point, les incertitudes.

À l'heure où le secret bancaire fait l'objet d'atteintes de plus en plus importantes, la CNIL appelle l'attention sur l'interdiction faite par la loi informatique et libertés de communiquer des informations nominatives à des tiers non autorisés. Elle a d'ailleurs eu l'occasion de s'interroger à plusieurs reprises sur la portée de la faculté offerte au client d'autoriser le banquier à révéler certaines des informations détenues à des tiers désignés. Il lui est apparu que, sous réserve de l'appréciation des tribunaux, la souscription d'une clause particulière, dite de « levée du secret bancaire » pour des conventions ayant le caractère de contrats d'adhésion, ne permet pas d'assurer que la personne a indubitablement donné son consentement, de façon

1 Loi n° 2003-706 du 1er août 2003 article 72 1°*Journal officiel* du 2 août 2003.

libre et éclairée, compte tenu du faible pouvoir de négociation du particulier et de l'impossibilité d'exercer son droit d'opposition.

Le rapport d'étape évoque par ailleurs la question soulevée par les professionnels de la mise en œuvre d'un fichier commun de lutte contre le blanchiment d'argent qui serait mutualisé entre tous les organismes de crédit de la place. La volonté de mettre en œuvre un fichier centralisé constitue une nouvelle illustration de la tendance à la multiplication de « listes noires » mutualisées. Il apparaît que si le renforcement des obligations de vigilance des banquiers au regard de la lutte contre le blanchiment d'argent et le terrorisme rend légitime le souhait des professionnels de s'organiser au mieux pour faire face à ces obligations, seule une intervention législative spécifique paraît de nature à concilier les obligations des professionnels et les droits des personnes concernées, en imposant des règles communes notamment relatives aux garanties et aux conditions minimales d'inscription dans de tels fichiers mutualisés à l'ensemble de la profession.

b) L'information des clients

La Commission a pu constater, dans les dossiers de déclaration récents, une réticence manifeste à faire figurer certaines mentions d'information. Le maintien d'une telle opacité sur les traitements mis en œuvre n'est pas admissible. Tout comme la CNIL l'a déjà indiqué s'agissant d'autres traitements de lutte contre la fraude, en particulier la fraude au crédit [1] ou de traitements relatifs à la fraude aux moyens de paiement [2], le caractère sensible des informations collectées ne devrait pas faire obstacle au droit à l'information des personnes fichées.

3. LA MÉCANIQUE DU SOUPÇON

Aborder la question du blanchiment d'argent et de la mise en œuvre de fichier de surveillance nécessite de resituer cette question, afin d'en comprendre les enjeux, dans le contexte plus général de la gestion du risque par les organismes financiers.

S'alignant d'ores et déjà sur les recommandations du comité de Bâle II qui a renforcé les exigences en matière d'adéquation des fonds propres (ratio de solvabilité Mac Donough), les organismes financiers souhaitent rendre compte de la gestion du risque en l'intégrant dans leur procédure de contrôle interne. À côté des risques traditionnels — le risque de marché, le risque de crédit (supposés être mesurables selon des formules mathématiques), la prise en compte du « risque opérationnel » sera désormais incluse dans le calcul de l'adéquation des fonds propres.

À cet égard, la CNIL est très attentive aux pratiques bancaires nouvelles visant au regroupement, au sein d'une base de données unique, de tous les risques

1 Voir le rapport adopté par la CNIL en novembre 2000 intitulé *Crédit à la Consommation : prévention de la fraude et des impayés et loi « informatique et libertés »*.

2 Voir la délibération de la CNIL n° 03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance.

répertoriés par un organisme financier. Cette pratique a d'ailleurs fait l'objet de déclarations récentes déposées auprès de la CNIL aux termes desquelles certains établissements prévoient d'associer dans un fichier unique de risques des informations à l'origine aussi diverse que des fraudes ou tentatives de fraudes internes, des données issues des fichiers Banque de France, en particulier du FICP, ainsi que des informations relatives à la lutte contre le blanchiment, ceci dans le but de réaliser un *Scoring* de risque sur l'entrée en relation avec un client ou l'attribution au bénéfice de ce dernier de produits ou services divers.

Au-delà, les enjeux relatifs à la lutte contre le blanchiment d'argent et le terrorisme ne sauraient avoir pour conséquence de voir le soupçon, principe-clé du mécanisme réglementaire de la lutte anti-blanchiment en France, devenir le mode privilégié de la gestion du risque et plus généralement de la relation bancaire elle-même.

B. Le droit d'accès

1. UN PARCOURS D'OBSTACLES

Au cours de l'année 2003, la CNIL a été saisie par de nombreuses personnes qui rencontrent des difficultés dans l'exercice de leur droit d'accès auprès d'une banque ou d'un établissement de crédit. Les articles 34 et suivants de la loi du 6 janvier 1978 reconnaissent aux personnes physiques concernées par un fichier, le droit d'obtenir une copie, en langage clair, de l'intégralité des données les concernant (y compris celles figurant en texte libre dans les zones dites « blocs notes » ou « commentaires ») qui seraient enregistrées dans les fichiers, manuels ou informatisés, détenues par une banque, un établissement de crédit ou les services financiers de La Poste.

Les plaintes reçues par la CNIL montrent clairement que la problématique est différente selon que le droit d'accès est exercé par le requérant auprès de l'établissement financier, dont il est client ou d'un établissement de crédit dont il espère devenir client. Tandis que dans le premier cas, les plaintes reçues par la CNIL (plus de 100 en 2003) révèlent que l'intervention de la Commission est nécessaire pour que les clients puissent obtenir l'accès, en langage clair, aux données personnelles détenues par leur banque, celles reçues dans le second cas (plus de 70 en 2003) témoignent de ce que le requérant croit pouvoir, en exerçant son droit d'accès prévu par la loi du 6 janvier 1978, obtenir les motifs ayant conduit un établissement de crédit à lui refuser un prêt.

a) Lorsque le requérant est client

On soulignera que, comme dans de nombreux autres secteurs, si la CNIL était jusqu'alors généralement saisie par des personnes qui ignoraient qu'elles disposaient d'un droit d'accès et de rectification aux données les concernant, la majorité des plaintes reçues en 2003 par la Commission montrent que, désormais, les citoyens connaissent l'existence de ce droit. En effet, les plaignants qui ont saisi la

CNIL durant cette année ont, le plus souvent, déjà exercé leur droit d'accès. S'ils sollicitent l'intervention de la Commission, c'est parce qu'ils n'ont pas reçu de réponse à leur demande ou que la réponse qu'ils ont reçue de leur banque n'est pas satisfaisante.

Afin d'illustrer la nature des plaintes dont a été saisie la CNIL en 2003, prenons le cas d'un M. Dupont, imaginaire s'agissant des données personnelles mentionnées mais, très concret, s'agissant de son exemplarité.

M. Dupont souhaite que sa banque lui communique l'ensemble des informations le concernant, enregistrées dans ses fichiers manuels ou informatisés. À cet effet, il adresse un courrier à sa banque, formulant sa demande sur le fondement des articles 34 et suivants de la loi du 6 janvier 1978.

Quelque temps plus tard, il reçoit de sa banque la réponse suivante :

Monsieur Dupont,
19, rue de la Bonne paie
75015 Paris

Monsieur,

Conformément à votre demande de droit d'accès, j'ai l'honneur de vous indiquer que les informations vous concernant détenues par notre établissement sont celles que vous nous avez communiquées.

Ces informations sont relatives à votre état civil, votre logement, votre vie professionnelle, votre budget et vos comptes bancaires.

Je vous prie d'agréer, Monsieur, l'expression de mes salutations distinguées.

Le directeur

M. Dupont, à juste titre, n'est pas satisfait de cette réponse. Il saisit la CNIL.

La CNIL intervient auprès de sa banque afin de lui rappeler que le droit d'accès prévu par la loi du 6 janvier 1978 impose que soit communiquée à la personne qui exerce ce droit une copie des informations la concernant et non, comme dans le cas de M. Dupont, une liste des catégories de données traitées.

Quelque temps plus tard, M. Dupont reçoit un nouveau courrier de sa banque :

Monsieur Dupont
19, rue de la Bonne Paie
75015 Paris

Monsieur,

Conformément à votre demande, vous voudrez bien trouver ci-après un extrait de fichier reprenant l'ensemble des données vous concernant détenues par notre établissement.

État civil		**Revenus**	
Nom	Dupont	Salaire Monsieur	1 300 euros
Prénom	André	Autres	500 euros (all.)
Date de naissance	1er janvier 1950	Salaire Madame	1 200 euros
Lieu de naissance	Paris XVe	Autres	450 euros (pa.)
Situation familiale	9	***Charges***	
Enfants à charge	2	LOGEMENT	1 000 euros
Identité du conjoint	Jacqueline Durand née le 1er février 1952 à Paris XVIe	Prêts	1
Logement		Impôts	I
Situation	Loc	Comptes bancaires	
Depuis	1996	Banque	CCP Paris
Adresse	19, rue de la Bonne paie (75017) Paris	Code établissement	015698
Téléphone	01 02 03 04 05	Code guichet	4489987
Vie professionnelle		N° de compte	4896 14578 63
Profession	112	Depuis	1986
Employeur	Collège Robespierre, place de la Bastille (75011) Paris	Caractéristiques du dossier Références client	*96*
Téléphone professionnel	I 112 (ID. EMP)	Historique client	
		01/12/1997	TC CT BDF
		02/02/1998	TEL ECH
		06/06/1999	99*
		01/09/1999	TEL ECH2
		01/02/2001	*01 **78 58*

M. Dupont n'est toujours pas satisfait de la réponse de sa banque.

En effet, si la liste détaillée des données le concernant lui est cette fois communiquée, le document comporte de nombreux codes et sigles incompréhensibles. Sa banque s'est contentée de lui adresser une copie des « pages-écrans » de son fichier sans lui fournir d'explications.

Il saisit donc à nouveau la CNIL qui intervient une nouvelle fois auprès de la banque afin de lui rappeler que les données doivent être communiquées en langage clair et qu'ainsi, tout code ou sigle doit être associé à une signification précise.

Quelque temps plus tard, M. Dupont reçoit un troisième courrier de sa banque. Cette fois, la réponse est satisfaisante au regard des articles 34 et suivants de la loi du 6 janvier 1978.

Monsieur Dupont
19, rue de la Bonne Paie
75015 Paris

Monsieur,

Conformément à votre demande, vous voudrez bien trouver ci-après un extrait de fichier reprenant l'ensemble des données vous concernant détenues par notre établissement.

Situation	Locataire	Comptes bancaires	
Depuis	1996	Banque	CCP Paris
Adresse	19, rue de la Bonne paie (75017) Paris	Code établissement	015698
Téléphone	01 02 03 04 05	Code guichet	4489987
Vie professionnelle		N° de compte	4896 14578 63
Profession	Enseignant	Depuis	1986
Employeur	Collège Robespierre, place de la Bastille (75011) Paris	Caractéristiques du dossier Références client	5896 14578 63 Crédit remboursable mensuellement
Téléphone professionnel Conjoint	Inconnu Enseignant Même employeur	Historique client	
		01/12/1997	Transmission de la créance au contentieux à la suite de plus de trois échéances impayées — inscription du client au FICP
Revenus		02/02/1998	Appel du client — établissement d'un échéancier
Salaire Monsieur	1 300 euros	06/06/1999	Non respect de l'échéancier
Autres	500 euros (allocations.)	1er septembre 1999	Appel du client — établissement d'un nouvel échéancier
Salaire Madame	1 200 euros	01/02/2001	Échéancier respecté Remboursement intégral Mainlevée de l'inscription au FICP
Autres	450 euros (pension alimentaire)		
Charges			
Logement	1 000 euros		
Prêts	Inconnu		
Impôts	Inconnu		

Trop souvent, en 2003, la CNIL a eu à intervenir pour que la communication des informations à un client exerçant son droit d'accès auprès de sa banque soit effectuée conformément à la loi. Trop souvent, il faut rappeler à ces établissements que les données doivent être communiquées en langage clair, qu'elles doivent être aisément compréhensibles, de sorte que la personne concernée soit en mesure, et tel est le fondement même du droit d'accès, de maîtriser ses données personnelles et, le cas échéant, de les faire rectifier.

b) Lorsqu'un refus de prêt a été opposé au requérant

La CNIL est par ailleurs saisie par des personnes qui, s'étant vu opposer un refus à une demande de crédit, exercent leur droit d'accès auprès de l'établissement de crédit concerné afin, pensent-ils, de pouvoir connaître les motifs ayant conduit à ce refus. Tel est le cas de M. D. qui veut se porter acquéreur d'un nouveau poste de télévision et qui se voit proposer un paiement par crédit en « trois fois sans frais ». Ou encore, M. V. qui sollicite un prêt pour l'acquisition d'un appartement. Dans les deux cas, leurs demandes sont refusées.

Étonnés de ces refus, car ils estiment que leurs revenus sont suffisants et qu'ils n'ont pas de dettes, M. D. et M. V. demandent aux organismes de crédit de motiver leur décision. Ils reçoivent pour seule réponse, une lettre circulaire leur indiquant que les refus donnés à une demande de crédit n'ont pas à être motivés. M. D. et M. V., non satisfaits et craignant d'être fichés « quelque part », saisissent la CNIL.

La Commission ne peut que leur répondre que le principe de la liberté contractuelle qui résulte de l'article 1101 du Code civil permet à un établissement de crédit de refuser d'accorder un crédit, s'il le souhaite, et qu'aucun texte ne lui fait obligation, dans cette hypothèse, d'avoir à s'expliquer sur les motifs de ce refus. La Commission précise toutefois à M. D. et M. V. qu'elle recommande, lorsqu'un tel établissement tient compte pour refuser un crédit de la présence d'informations relatives au demandeur dans un fichier commun recensant des incidents, qu'il communique à tout requérant la nature et l'origine de ces informations.

Face au nombre important de plaintes de cette nature, la CNIL a édité en 2003 un guide pratique intitulé *Protection des données personnelles et refus de crédit* qui peut être téléchargé sur le site internet de la Commission. Ce guide a pour objet d'expliquer les différentes situations qui peuvent conduire à se voir refuser un crédit. Ainsi en est-il de la technique dite du *Credit-Scoring (cf. supra)* appliquée par les établissements de crédit à toute demande de prêt.

Ce document a également pour objet de guider les citoyens dans les démarches qu'ils peuvent accomplir pour vérifier, par exemple, qu'ils ne sont pas fichés à tort au fichier des incidents de remboursement des crédits aux particuliers (FICP) géré par la Banque de France (*cf.* I. du présent chapitre) ou encore, pour vérifier que l'établissement de crédit ne dispose pas de données erronées les concernant.

2. UN PROGRÈS ATTENDU : LA CONVENTION DE COMPTES

La loi MURCEF adoptée le 21 décembre 2001 a posé le principe de la rédaction obligatoire d'une convention écrite lors de l'ouverture d'un compte bancaire effectué par un client auprès de sa banque, disposition visant à renforcer les droits du consommateur bancaire.

Le ministère de l'Économie, des Finances et de l'Industrie, en novembre 2002, a repoussé de dix-huit mois la publication du décret d'application permettant la mise en œuvre de ces conventions de compte. Mais, le 9 janvier 2003, les représentants de la Fédération bancaire française (FBF) ont pris l'engagement de formaliser dès à présent les relations contractuelles avec leurs clients, en proposant des conventions de compte précisant le fonctionnement au quotidien du compte de dépôt.

Au cours de sa séance plénière du 27 mai 2003, la CNIL s'est félicitée de l'engagement pris par la FBF. Elle a, par communiqué de presse, encouragé les consommateurs à demander communication de leur convention de compte en apportant une attention particulière aux clauses réglementant l'utilisation faite de leurs données personnelles.

La CNIL se félicite à cet égard de la collaboration engagée, dans le cadre de sa mission de conseil aux professionnels, avec certains établissements sur la rédaction des clauses figurant dans les conventions. En effet, celles-ci doivent systématiquement comporter :
— les finalités des traitements mis en œuvre par l'établissement de crédit ;
— les destinataires des données personnelles concernant les clients ;
— le droit de ces clients de s'opposer à un traitement des données à des fins de prospection commerciale ;
— les modalités d'exercice du droit d'accès aux données concernant le client, conformément aux textes relatifs à l'informatique, aux fichiers et aux libertés.

Si les conventions sont remises systématiquement à tout nouveau client, la CNIL relève que les anciens clients, c'est-à-dire la majorité de la clientèle bancaire, ne peuvent en prendre connaissance que sur leur demande expresse. Ces derniers risquent donc d'être insuffisamment informés, en particulier sur leur droit de s'opposer à voir leurs données personnelles utilisées à des fins de prospection commerciale. La CNIL ne peut en conséquence qu'encourager les consommateurs à solliciter de leur banquier que la convention de compte leur soit communiquée et à porter une attention toute particulière aux dispositions contractuelles qui leur sont appliquées concernant les utilisations faites de leurs données personnelles.

Au cours de l'année 2004, la CNIL procédera à une relecture des conventions de comptes émises par principaux établissements de crédit afin de s'assurer de la bonne information des clients.

Chapitre 7

DONNÉES PERSONNELLES ET RELATIONS COMMERCIALES

Conquérir, fidéliser mais aussi rejeter ou même harceler son client : la relation commerciale peut être vécue très différemment selon que l'on se situe d'un côté ou de l'autre. En toutes hypothèses, la contractualisation des relations entre un client et une société commerciale ne justifie pas que cette dernière utilise toutes les informations dont elle dispose sans s'assurer du respect de la loi du 6 janvier 1978, qu'il s'agisse d'un « bon client » ou d'un « mauvais client ». Ce domaine constitue une bonne illustration de la palette de moyens d'action mis à la disposition de la CNIL en attendant la transposition de la directive qui lui conférera de nouveaux pouvoirs.

La méthode de travail de la Commission consiste d'abord à rappeler les règles à respecter pour les nouvelles applications qui voient le jour, tant au travers de l'instruction des dossiers qu'au moyen de recommandations telles celles sur l'utilisation de la carte bancaire par les commerçants ou la gestion de fichiers de personnes à risque par les loueurs de véhicules. Il lui appartient ensuite d'assurer le suivi des applications les plus sensibles, qui ont fait l'objet de vérifications par le passé, comme par exemple le fichier Préventel et de faire de nouvelles missions de contrôle sur place, en 2003 dans le secteur du recouvrement de créances.

Prenant appui sur les travaux menés ces dernières années en matière de « listes noires », la CNIL a également publié en 2003 un rapport d'étude sur ce sujet, qui rappelle ses préconisations en la matière.

La vigilance dont la CNIL fait preuve en la matière n'exclut pas qu'elle facilite pour les professionnels la déclaration de leurs traitements, ce qui l'a conduite à élargir le champ de la norme simplifiée relative à la gestion immobilière à l'analyse de la solvabilité du candidat à la location et au recouvrement de créances notamment.

I. L'EXPLOITATION DU NUMÉRO DE CARTE BANCAIRE

Dans son précédent rapport [1], la CNIL soulignait l'inquiétude des consommateurs à propos de l'utilisation de leur numéro de carte bancaire — un nouvel exemple en est donné ici — et indiquait préparer une recommandation à ce sujet. Elle a été publiée en juin 2003.

A. Un cas d'utilisation contestable

M^me^ Y. a acheté, en ligne sur un site internet de voyagiste, un billet d'avion électronique au bénéfice de M. X., pour un vol Nice/Ajaccio. Il s'agit d'un billet d'avion totalement dématérialisé : le client effectue le règlement et n'a plus qu'à se présenter, au moment de l'embarquement, muni d'une pièce d'identité pour obtenir sa carte d'accès à bord. Elle a payé au moyen de sa carte bancaire (en indiquant le numéro de la carte et sa date de validité).

Lorsque M. X. s'est présenté à l'enregistrement de ce vol Nice/Ajaccio, il ne disposait pas de la carte bancaire de M^me^ Y. Le personnel de la compagnie aérienne lui indique alors que le billet électronique acheté par M^me^ Y. n'est pas valable et qu'un nouveau titre de transport doit être édité au moment de l'embarquement. Ce titre est édité par le personnel de la compagnie aérienne, mais c'est le compte de M^me^ Y. qui est débité, au moyen des références de sa carte bancaire.

M^me^ Y. est choquée de voir que la compagnie aérienne dispose de son numéro de carte de crédit et l'utilise sans son accord, alors qu'elle ne l'a jamais communiqué qu'au voyagiste. Elle saisit donc la CNIL.

La compagnie aérienne, interrogée par la Commission dans ce dossier, lui apporte les précisions suivantes.

Le recours au billet électronique requiert du client, lorsqu'il effectue la réservation sur internet, qu'il fournisse un identifiant qu'il devra présenter au moment de l'enregistrement. Cet identifiant, au choix du client, peut être le numéro de passeport, de carte d'identité, de carte de fidélité ou de carte de crédit. L'identifiant est enregistré dans le dossier de réservation transmis au transporteur pour lui permettre de relier le billet électronique au détenteur de l'identifiant, lors de l'enregistrement du passager.

En l'espèce, M^me^ Y. avait choisi de fournir son numéro de carte bancaire comme identifiant, au moment de l'achat du billet électronique auprès du voyagiste. C'est ce qui explique que la compagnie aérienne en ait eu connaissance.

Bien que les procédures de la compagnie aérienne n'autorisent pas les agents à utiliser le numéro de carte bancaire qui ne constitue qu'un identifiant dans le

1 Voir « L'utilisation du numéro de carte bancaire », 23e rapport d'activité de la CNIL, p. 93.

dossier de réservation, il arrive parfois qu'une telle utilisation soit faite pour « rendre service » au client au moment de l'embarquement. C'est ce qui se serait produit en l'espèce.

La compagnie aérienne a indiqué à la Commission qu'elle effectuerait un rappel des procédures auprès de l'ensemble de ses agents.

B. Recommandation sur le numéro de carte bancaire

L'utilisation des cartes bancaires dépasse aujourd'hui la simple fonction d'un outil monétique de paiement pour devenir un véritable outil de fidélisation, de proximité et d'individualisation dans la relation client — entreprise. Face aux interrogations nombreuses des consommateurs sur ces utilisations nouvelles, à vocations tant commerciales que de lutte contre la fraude, la CNIL a rendu publique le 26 juin 2003 une recommandation sur le stockage et la conservation du numéro de carte bancaire dans le secteur de la vente à distance (délibération n° 03-034 du 19 juin 2003).

1. CONSERVER LE NUMÉRO DANS QUEL BUT ?

La CNIL, tout en rappelant dans sa recommandation que la finalité première de l'utilisation d'un numéro de carte bancaire est la réalisation d'une transaction, qu'elle soit ponctuelle ou à exécutions successives, c'est-à-dire le complet paiement d'un prix en contrepartie de la délivrance d'un bien ou la prestation d'un service, reconnaît pour la première fois le caractère légitime de pratiques relatives à l'identification, sous certaines conditions, des clients à partir de leur moyen de paiement.

S'agissant ainsi de l'identification à des fins commerciales (par exemple les pratiques de « portefeuille électronique »), la CNIL recommande que l'utilisation du numéro de carte bancaire soit subordonnée, lorsque ce numéro est conservé au-delà du temps nécessaire, à la réalisation de la transaction, au recueil du consentement de la personne concernée.

S'agissant par ailleurs de la lutte contre la fraude, la CNIL rappelle dans sa recommandation que l'existence de fichiers de prévention de la fraude, en particulier lorsqu'ils sont mutualisés à l'ensemble d'un secteur d'activité, comporte des risques sérieux d'exclusion et de marginalisation des personnes concernées sur lesquels il convient d'assurer un strict contrôle. Le développement de systèmes experts par les commerçants en ligne afin d'effectuer des contrôles de cohérence sur un paiement effectué par carte bancaire n'est d'ailleurs pas étranger à l'existence de cette problématique.

Il importe en effet que la lutte contre la fraude ne puisse aboutir à une discrimination ou un refus de vente, même si elle peut conduire légitimement le commerçant à refuser un mode de paiement. La CNIL considère en conséquence que l'utilisation du numéro de carte bancaire par un professionnel de la vente à distance dans un fichier ayant pour finalité de lutter contre la fraude au paiement en

conservant la trace d'agissements lui ayant porté préjudice, est légitime, sous la réserve que ce fichier ait fait l'objet d'une déclaration spécifique à la CNIL et soit conforme aux lois et règlements en vigueur.

La CNIL souligne enfin dans sa recommandation que toute utilisation du numéro de carte bancaire, quelle qu'en soit la finalité, doit faire l'objet d'une information complète et claire auprès de la personne fichée. Elle rappelle en particulier qu'il résulte de l'article 10 de la directive 95-46 du 24 octobre 1995 que les personnes fichées doivent être informées de l'identité du responsable du traitement ainsi que des finalités du traitement auquel les données sont destinées.

2. SÉCURITÉ DES PAIEMENTS

S'agissant des questions relatives à la sécurité des paiements, la CNIL rappelle que la multiplication des finalités liées à la collecte du numéro de carte bancaire a par ailleurs pour conséquence la multiplication de bases de données de numéros de cartes bancaires pouvant faire l'objet d'une réutilisation frauduleuse, en particulier lorsqu'elles sont accessibles sur internet.

La recommandation de la CNIL rappelle ainsi que les responsables de traitements doivent prendre les mesures organisationnelles et techniques appropriées afin de préserver la sécurité, l'intégrité et la confidentialité des numéros de cartes bancaires contre tout accès, utilisation, détournement, communication ou modification non autorisés.

La CNIL avance dans sa recommandation plusieurs préconisations pratiques qui pourraient améliorer de façon significative la sécurité des bases de données. Elle préconise par exemple de recourir à des procédés techniques permettant de crypter de manière irréversible le numéro de la carte bancaire dès que la transaction a été réalisée, de masquer les numéros CB des clients sur l'écran des salariés habilités ou de ne pas mémoriser le cryptogramme visuel (chiffres figurant au dos de la carte).

S'agissant plus particulièrement de la mise en place de système d'authentification en ligne, permettant d'accéder directement à un profil client et à des coordonnées bancaires (« portefeuille électronique »), la recommandation de la CNIL invite les commerçants à informer clairement leurs clients sur les risques induits par certains gestionnaires de mots de passe intégrés à des navigateurs internet et leur préciser la méthode permettant de désactiver ces systèmes.

II. LES « LISTES NOIRES » TOUJOURS D'ACTUALITÉ

Une « liste noire » est dans le langage courant un fichier répertoriant des personnes indésirables. Principalement auteurs d'impayés, des personnes étant à l'origine de fraudes, voire de simples « anomalies » ou « incohérences » peuvent se

retrouver fichées. Dans un rapport rendu public en 2003 [1], la Commission alerte au sujet des risques d'exclusion sociale et de marginalisation résultant du développement exponentiel de la mise en œuvre de traitements relatifs à la mutualisation d'informations relatives aux « mauvais payeurs » et aux « fraudeurs ».

En 2003, la CNIL a eu l'occasion de se pencher sur la mise en œuvre de traitements relatifs à des « listes noires » dans le secteur de la location automobile et de la location immobilière qui illustrent de façon exemplaire la problématique posée par les fichiers de mauvais payeurs ou de fraudeurs au regard des libertés publiques et des droits fondamentaux des personnes au-delà de la seule atteinte à la vie privée.

A. Les principes : le rapport de la CNIL sur les « listes noires »

Dans le rapport d'ensemble sur les listes noires, la CNIL rappelle ses préconisations au regard des fichiers, habituellement désignés comme des « listes noires », en dresse le périmètre et les perspectives d'action et formule des propositions visant à un meilleur encadrement de ces fichiers, tout en rappelant l'interdiction posée à l'article 30 de la loi du 6 janvier 1978 de procéder au traitement d'informations relatives à des infractions, mesures de sûreté et condamnation.

1. CLASSIFICATION

La mise en œuvre de traitements susceptibles d'êtres qualifiés de « listes noires » s'effectue dans des contextes et situations juridiques très différents. À côté des fichiers mutualisés encadrés par le législateur figurent ceux qui sont le fruit de regroupements professionnels d'envergure nationale ou locale ou d'initiative privée.

La Commission a cependant entendu dans son rapport faire part de la spécificité du secteur financier et des risques présentés par la mise en commun de « listes noires » par des sociétés privées. Souvent mis en œuvre par de petites structures, des regroupements ad hoc de commerçants ou de certains professionnels, ces traitements ignorent le principe de sectorisation ou ne respectent pas l'ensemble des principes dégagés par la CNIL en matière de « listes noires ». Le développement de ces initiatives, le plus souvent locales, est rendu possible par le faible coût de gestion du développement d'applications permettant d'alimenter et d'accéder à la « liste noire ». Bien souvent rassemblée sur un simple tableur, la « liste noire », quand elle n'est pas diffusée par télécopie, est accessible sur un extranet réservé à des abonnés, voire à tout internaute sous réserve du paiement d'une somme forfaitaire correspondant à une consultation.

La Commission a entendu assimiler aux fichiers mutualisés les fichiers internes à des acteurs incontournables d'un secteur d'activité. En effet, si l'on peut opposer les fichiers dits « internes », c'est-à-dire propres à une entreprise ou un organisme

1 *Les listes noires. Le fichage des « mauvais payeurs » et des « fraudeurs » au regard de la protection des données personnelles*, collection Les rapports de la CNIL, La Documentation française, Paris, édition 2003.

donné, et les fichiers dits « mutualisés » qui sont le fruit d'un regroupement ou d'un croisement de plusieurs fichiers, cette distinction n'est pas suffisante pour cerner la diversité des fichiers de « mauvais payeurs » et de « fraudeurs ». Un fichier interne, du fait de la taille de l'entreprise, de son importance relative en parts de marché dans un secteur d'activité donné, voire de sa situation de monopole ou d'oligopole, trouve sa place dans la présente étude : il s'agit alors d'un « fichier central » qui bien que non mutualisé ou rapproché de celui d'autres entités juridiques doit être régi par les mêmes principes que ceux définis précédemment.

Par contre, sont exclus du périmètre du rapport les fichiers internes mis en œuvre par un organisme afin d'assurer le traitement des impayés, de respecter ses obligations comptables [1] et de procéder au recouvrement de ses créances. Un organisme peut donc légitimement conserver trace des incidents de paiement survenus, sans qu'un tel dispositif ne heurte les principes posés par la loi du 6 janvier 1978. S'agissant du traitement des infractions, les dispositions de l'article 30 de la loi du 6 janvier 1978 n'ont pas entendu priver la victime d'une infraction du droit de conserver trace d'agissements lui ayant causé un préjudice. Dès lors que le traitement de ses informations reste propre à l'organisme et se limite à la préservation de ses droits, telle la poursuite de la réparation du préjudice subi, il est légitime.

2. PRÉCONISATIONS

— *« Les listes noires ne peuvent être tenues secrètes »*

C'est ce que réaffirme le rapport. La nécessaire transparence de ces fichiers doit être assurée par une information des personnes sur les finalités et les destinataires du fichier ainsi que sur l'existence du droit d'opposition. Cette information doit être assurée à trois niveaux : lors de la collecte des informations, lors de la survenance de l'incident pouvant donner lieu à fichage, puis le cas échéant au moment du fichage.

— *« Pas de mise au pilori électronique »*

La CNIL consacre un principe de sectorisation se traduisant par la limitation de la mise en œuvre et de l'accès au fichier à un secteur d'activité et aux seuls professionnels du secteur ce qui exclut par exemple la confusion des impayés trouvant leur origine dans un contrat d'abonnement téléphonique avec ceux d'origine locative. La candidature d'un futur locataire ne saurait être exclue en raison d'impayés relatifs à des prestations de services téléphoniques sans porter atteinte au principe de proportionnalité et générer un risque d'exclusion difficilement compatible avec la protection des libertés individuelles.

Il s'agit de la stricte application du principe de proportionnalité en vertu duquel les données doivent être *« pertinentes, adéquates et non excessives »* par rapport aux finalités pour lesquelles elles sont enregistrées.

1 En application de l'article L. 123-22 du Code de commerce (ancien article 16), les livres et documents créés à l'occasion d'activités commerciales doivent être conservés dix ans. Pour autant, la CNIL ne considère pas cette durée comme étant nécessairement celle de la conservation des données nominatives des clients.

— *« Veiller à la pertinence des informations »*

Les conditions d'inscription dans le fichier centralisé doivent être strictement définies et respectées. S'agissant d'informations relatives aux impayés, il y a lieu de s'assurer de l'existence d'un principe certain de créances et d'assurer en conséquence la gestion des contestations, la Commission préconisant dans le cas de l'existence d'une contestation sérieuse de ne pas procéder à l'inscription. L'inscription d'informations relatives à des manquements à des obligations contractuelles doit reposer sur des critères objectifs et vérifiables, opposables à la personne concernée, faisant abstraction de tout jugement de valeur ou d'appréciation de son comportement. Le responsable du traitement doit notamment s'assurer du respect des conditions d'inscription et procéder à l'examen des contestations et veiller à la création d'instances de médiation et de contrôle. Seuls des incidents présentant une gravité certaine et prédéterminée doivent faire l'objet d'une inscription de telle sorte qu'il appartient à l'organisme centralisateur de définir un seuil d'inscription, selon le cas en fonction d'un niveau de gravité ou d'un montant.

— *« Garantir le droit à l'oubli »*

La fixation de la durée de conservation et l'existence de procédés de mise à jour doivent permettre le respect du principe du « droit à l'oubli ». Pour le fichage d'impayés, ce principe se traduit par la suppression de l'inscription dès régularisation de l'incident. La Commission recommande également que l'obligation de mise à jour soit contractualisée sous la forme d'une obligation à la charge des organismes ayant accès au fichier avec un mécanisme de sanction en cas de manquement allant de la suspension de l'accessibilité aux informations inscrites par cet organisme à la suppression pure et simple de l'ensemble des informations inscrites par l'organisme défaillant.

— *« Assurer la sécurité et la confidentialité »*

Les moyens techniques et humains doivent être à la hauteur des dangers existant en matière d'atteinte à la vie privée. Une gestion rigoureuse des habilitations et contrôles d'accès et la définition d'une politique de journalisation et de gestion des mots de passe afin de se prémunir contre les risques d'intrusion et de détournement de finalité doivent accompagner la mise en œuvre des traitements, de même que la définition d'algorithmes de chiffrement avancés. Par ailleurs, la prise en compte du risque d'homonymie par la collecte des date et lieu de naissance est une préconisation constante de la Commission. Seule l'inscription des personnes identifiée avec certitude devrait être possible. Un traitement spécifique devra permettre de gérer les cas d'usurpation d'identité.

3. OUVERTURE LÉGISLATIVE

L'article 30 de la loi du 6 janvier 1978 réserve, sauf dispositions législatives contraires, aux juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la CNIL, aux personnes morales gérant un service public, la mise en œuvre de traitements automatisés des informations nominatives concernant les infractions, condamnations ou mesures de sûreté.

Cette disposition, bien que pénalement sanctionnée par l'article 226-19 du Code pénal, n'a malheureusement pas empêché la multiplication de fichiers destinés à prévenir la fraude. S'il peut paraître paradoxal, au regard de la protection des droits et libertés, de proposer une dérogation de nature à rendre licite, dans certains cas, la centralisation d'informations relatives à des infractions, la distorsion constatée entre l'interdiction légale et la pratique aboutissant à un développement anarchique d'initiatives non sanctionnées, conduit la CNIL, après une réflexion approfondie, à considérer que seul un aménagement législatif du régime d'interdiction permettrait d'offrir une garantie effective des droits des personnes.

La Commission considère ainsi qu'un fichier commun destiné à la prévention de la fraude devrait faire l'objet d'un encadrement législatif précis relatif aux conditions d'inscription, à la durée de conservation et aux droits des personnes. De plus, un tel fichier, s'il s'avérait indispensable à la profession et socialement admis, devrait être régi par des contraintes de service public, même s'il était exploité par une société privée. La directive du 24 octobre 1995 relative à la protection des données personnelles y invite en précisant dans son article 8 (5) [1] qu'un fichier « d'infractions » peut être mis en œuvre dans le secteur privé, uniquement à la condition que des garanties appropriées soient réunies ou sous le contrôle de l'autorité publique.

La possibilité de tenir des fichiers privés, et *a fortiori* mutualisés, relatifs à des infractions pourrait résulter soit d'une autorisation légale spécifique propre à chaque secteur d'activité, soit d'une autorisation de portée plus générale dans le cadre de la transposition de la directive du 24 octobre 1995 avec l'instauration d'un régime d'autorisation par la CNIL.

L'évolution de la doctrine de la CNIL démontre qu'elle a recherché des solutions pragmatiques lui paraissant répondre à un équilibre délicat à atteindre entre la légitimité des professionnels et la protection des droits des personnes. Une prise de position est attendue de la part du législateur afin d'assurer une protection efficace des citoyens et de reconnaître aux professionnels la possibilité de tenir de tels fichiers, dans des conditions de transparence qui n'existent pas aujourd'hui.

Le législateur a entendu cet appel unique puisque, lors de l'examen en première lecture au Sénat en avril 2003, du projet de loi modifiant la loi du 6 janvier 1978 et transposant la directive de 1995 le rapporteur, M. Alex Türk, a proposé et fait adopter à l'article 9 de la loi de 1978 modifiée une disposition ainsi rédigée : *« Les traitements des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en* œuvre que par : [...] *3° Les personnes morales victimes d'infractions, pour les stricts besoins de la lutte contre la fraude et dans les conditions prévues par la loi ».*

1 *« Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Les États membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique ».*

B. Les « listes noires » des loueurs de véhicules automobiles

1. MISSIONS DE CONTRÔLE

À la suite de plaintes adressées par des personnes s'étant vu refuser la location d'un véhicule automobile en raison de leur inscription sur une « liste noire », la Commission a procédé dans le courant de l'année 2002 à des missions de contrôle auprès des principaux loueurs de véhicules et de leur chambre syndicale, le Conseil national des professions de l'automobile (CNPA) — branche loueurs, afin de contrôler si ces sociétés et organismes respectent l'ensemble des dispositions de la Convention européenne du 28 janvier 1981 et de la loi du 6 janvier 1978.

Les missions de vérifications, effectuées auprès des sociétés Europcar, Avis, Hertz, Budget, Rent-a-Car, Ada et du CNPA, ont permis de constater que chaque société de location de véhicules dispose de sa propre « liste noire » et refuse la location de véhicule aux personnes qui y sont inscrites. Par ce moyen, ces sociétés entendent se prémunir contre des clients dont le comportement peut engendrer d'importants préjudices, d'ordre essentiellement financier. Les motifs d'inscription retenus sont les impayés, les vols et dégradations, les accidents graves ou multiples où la responsabilité du client est engagée, les fraudes diverses, en particulier l'usage de faux documents d'identité. Il arrive également qu'une rubrique à caractère plus général soit créée, parfois sous le nom de « clients suspects ».

Ces missions de vérification ont mis en lumière plusieurs manquements aux dispositions de la loi du 6 janvier 1978.

S'agissant de l'information des personnes, les missions de contrôle ont mis en évidence que la possibilité d'être inscrit sur une liste noire n'était pas visée dans les documents contractuels, ni portée à la connaissance des clients et que, au contraire, la plupart des loueurs de véhicules ne souhaitaient pas indiquer le réel motif du refus de location. Faute d'une information correcte, la personne concernée n'est pas en mesure de se justifier ou de demander la rectification des erreurs, pouvant par exemple résulter d'une homonymie.

Par ailleurs, il est apparu que les conditions d'inscription sur la liste noire n'étaient pas expressément définies, que de surcroît, dans la plupart des cas, l'inscription d'une personne sans aucun motif précis était possible et qu'il n'existait pas toujours de règles claires concernant la suppression des informations enregistrées.

Or, les loueurs de véhicules, désireux de disposer d'instruments permettant de se protéger contre des clients « indélicats », qui créent et gèrent un fichier de personnes à risques doivent le faire en toute transparence. Cette exigence est d'autant plus forte que la création d'un fichier commun à l'ensemble des loueurs de véhicules, sous l'égide du Conseil national des professions de l'automobile, pourrait prochainement être décidée.

La Commission a dès lors décidé de faire part de ses préconisations en adoptant lors de sa séance du 11 mars 2003 une recommandation relative à la

gestion de fichiers de personnes à risques par les loueurs de véhicules (délibération n° 03-012 du 11 mars 2003).

2. LA RECOMMANDATION AUX LOUEURS DE VÉHICULES

La Commission rappelle notamment dans sa recommandation que le respect des dispositions de l'article 2 de la loi du 6 janvier 1978 se traduit par un principe de spécialité pour les agents pouvant procéder à une inscription ou à une consultation (ils doivent être en effet spécifiquement habilités à cet effet et avoir compétence pour vérifier le caractère certain du préjudice subi).

Un accent particulier est porté sur la pertinence du traitement. L'inscription d'une personne dans un fichier spécifique ou l'enregistrement de données la concernant dans un fichier clientèle qui conduit à refuser la location d'un véhicule doit reposer sur des motifs objectifs opposables à la personne concernée, faisant abstraction de tout jugement de valeur ou d'une appréciation de son comportement. La Commission recommande ainsi :
— l'établissement préalable d'une liste des motifs d'inscription ;
— l'exclusion de toute inscription sans indication de motif ;
— l'établissement d'une distinction entre les motifs d'inscription résultant du comportement d'un conducteur employé par une société ou un organisme et les motifs d'inscription imputables à ladite société ou audit organisme.

La sécurité et la confidentialité du traitement doivent également être assurées par la prise en compte du risque d'homonymie, notamment dans des cas signalés d'usurpation d'identité, et en veillant à ce que les données ne soient communiquées qu'aux seuls professionnels de la location de véhicules, et ce par des moyens sécurisés (fichier ou courriel crypté).

La Commission traduit enfin le principe de transparence en recommandant que les personnes soient systématiquement informées par les sociétés ou organismes concernés de l'existence d'un fichier spécifique ou de la possibilité d'enregistrer dans un fichier clientèle des données qui conduisent à refuser la location d'un véhicule, des motifs d'inscription, des destinataires des données, et de leur faculté d'exercer leur droit d'accès, conformément à l'article 34 de la loi du 6 janvier 1978.

3. *WANTED* SUR INTERNET

Saisie d'une demande de conseil portant sur la diffusion sur internet de la photographie et de l'identité des conducteurs de véhicules de location qui n'auraient pas procédé à leur restitution, la Commission a eu l'occasion de rappeler que, quelle que soit la gravité des manquements contractuels, *a fortiori* et même si cela peut paraître paradoxal, lorsqu'il s'agit de la commission d'infractions, telles le vol d'un véhicule, un organisme privé ne pouvait procéder à la « mise au pilori électronique » d'une personne par la diffusion d'avis de recherches sur internet et se substituer ainsi à la puissance publique dans la poursuite des infractions.

Dans le cas soumis à la Commission, un loueur de véhicule envisageait de mettre en œuvre en France un traitement consistant notamment en la diffusion, sous une rubrique dédiée de son site internet, d'appels à témoins portant mention des références des véhicules manquants, ainsi que l'identité et la photographie des locataires ayant un retard de plus de quinze jours au regard de la date convenue de restitution du véhicule. L'organisme concerné se prévalait du fait que ce traitement aurait déjà été mis en œuvre dans d'autres États membres.

L'instruction de la demande de conseil a mis en lumière plusieurs manquements aux dispositions communes de la loi du 6 janvier 1978.

En premier lieu, la Commission a relevé le caractère insuffisant au regard du principe de transparence, de l'information des personnes, qui ne visait à aucun moment la possibilité d'une diffusion sur internet des données personnelles des conducteurs défaillants, en violation des dispositions de l'article 27 de la loi du 6 janvier 1978 en ce qu'elles prévoient l'information des personnes sur les destinataires des données. De surcroît, au regard du seul droit à l'image, le recueil exprès et explicite du consentement, aux termes d'une clause détaillant tous les usages possibles et prévisibles de la photographie, matérialisé le cas échéant par une case à cocher, serait seul de nature à permettre la diffusion de la photographie sur internet.

Par ailleurs, la Commission a estimé qu'une information préalable, aussi complète soit-elle, ne suffisait pas à asseoir la licéïté du traitement et couvrir l'atteinte au principe de proportionnalité.

La CNIL a aussi eu l'occasion de rappeler que la *« divulgation d'informations nominatives portant atteinte à la réputation ou à la considération de la personne auprès de tiers n'ayant pas qualité pour les recevoir »* est une infraction prévue et réprimée par l'article 226-22 du Code pénal d'un an d'emprisonnement et de 15 000 euros d'amende.

Suite aux observations de la Commission, le loueur de véhicule a indiqué renoncer à la mise en œuvre de son projet en France.

S'agissant d'un traitement mis en œuvre dans plusieurs États membres, il importe de noter que cette appréciation ne résulte pas seulement de l'application de dispositions nationales, mais bien du dispositif harmonisé de protection des données, posé par la directive européenne 95/46 du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. L'article 10 de la directive fixant le socle minimal de l'information des personnes inclut l'information sur la finalité du traitement et les destinataires et l'article 6 c) définit le principe de proportionnalité disposant que seules peuvent faire l'objet d'un traitement les informations *« adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement »*.

C. Le fichage des auteurs d'impayés locatifs

La CNIL a été saisie en 2003 d'une déclaration de traitement relative à des impayés de locataires, accessible à tout propriétaire loueur d'immeuble, par internet.

1. LA POSITION DE LA CNIL

a) Précédents corrects

La CNIL a déjà eu à se pencher sur la mutualisation d'informations relatives aux impayés locatifs : elle a ainsi été saisie en 1996 d'une déclaration relative à un système de protection contre les impayés locatifs, dénommé fichier des incidents de paiement locatifs (FIPL) [1] mis en œuvre par une société privée. En 2001, elle a eu à connaître également de l'extension du fichier d'incidents de paiement dénommé « fichier national des incidents de paiement » (FNIP) de la société BGD [2] aux créances civiles en matière de logement, de téléphonie et d'assurances, rendant possible la consultation de l'ensemble des impayés enregistrés dans leur secteur d'activité par les professionnels de chacun de ces secteurs.

Dans les deux cas de figure, le fichier n'était consultable que par des professionnels de l'immobilier identifiés par la possession d'une carte professionnelle. La CNIL avait également obtenu, entre autres garanties, que les impayés ne puissent faire l'objet d'une inscription que si une clause du bail avait expressément prévu cette possibilité. Dans ces conditions, la CNIL avait finalement estimé, s'agissant du FIPL que les dispositions de la loi du 6 janvier 1978 étaient respectées, que le fichier comportait des garanties et notamment que le traitement paraissait licite au regard du droit au logement, le périmètre du fichier, réservé au seul secteur privé locatif et excluant les bailleurs sociaux, ne pouvant faire obstacle à l'attribution d'un logement social (dispositif Besson). Un contrôle sur place avait établi l'absence de caractère réel du traitement, le nombre d'inscriptions étant limité à quelques dizaines. S'agissant du FNIP de la société BGD, une longue instruction suivie également d'un contrôle sur place, a permis de conclure que cette société se conformait aux dispositions de la loi du 6 janvier 1978, tout en relevant le caractère stigmatisant du traitement et les difficultés posées par la référence à un « agrément » de la CNIL ou l'utilisation du terme « national » dans la dénomination du fichier.

b) Impuissance de la CNIL

La déclaration examinée par la Commission en 2003 s'écarte de ces préconisations. En matière de sectorisation, la diffusion d'informations relatives aux locataires auteurs d'impayés n'est pas limitée aux seuls professionnels de l'immobilier mais à tout « *propriétaire loueur d'immeuble* ». Il n'est pas prévu d'insérer une clause

1 17e rapport d'activité 1996 p. 151.
2 22e rapport d'activité 2001 pp. 154 et ss et 23e rapport d'activité 2002 pp. 109 et ss.

spécifique dans le bail d'habitation et il est prévu de porter mention de l'existence de condamnations civiles du débiteur.

La Commission, qui ne dispose pas en l'état de la législation de pouvoir d'autorisation pour les traitements mis en œuvre par le secteur privé, a délivré un récépissé en application des dispositions de l'article 19 de la loi du 6 janvier 1978. Elle a néanmoins indiqué au déclarant que la diffusion des informations relatives aux impayés locatifs à des propriétaires immobiliers qui n'ont pas la qualité de professionnels de l'immobilier n'est pas de nature à assurer le respect de la sectorisation qu'elle demande et à empêcher le détournement de finalité. Elle a souligné qu'en l'absence de clause spécifique du bail d'habitation, la collecte ne pouvait être considérée comme loyale en application des dispositions des articles 25 et 27 de la loi du 6 janvier 1978, infractions prévues et réprimées de 300 000 euros d'amende et de cinq ans d'emprisonnement aux termes des articles 226-18 et 226-21 du Code pénal.

2. LA POSITION DE LA COMMISSION BELGE

Cette position est à rapprocher de l'avis [1] rendu par la Commission de protection de la vie privée, autorité de protection belge, le 19 décembre 2002 relatif au fichier des locataires défaillants mis en œuvre sur l'initiative du syndicat national des propriétaires (SNP) par la société en nom collectif Checkpoint sur le site internet www.check4rent.com.

La Commission belge a estimé que le fichier était doublement illégal (tant du point de vue de la loi sur la vie privée que sur le plan de la garantie constitutionnelle du droit au logement) et qu'un tel type de fichier nécessitait une intervention, préalable et spécifique, du législateur afin de l'autoriser et d'en spécifier les modalités. Le législateur est en effet *« le mieux à même d'appréhender l'opportunité comme la proportionnalité de cet instrument supplémentaire »* concernant *« la location d'immeuble et les relations entre le propriétaire-bailleur et le locataire »*. S'agissant de la proportionnalité du traitement, la Commission se référant à un précédent avis [2] relatif au fichier RSR [3] dans le secteur des assurances, a retenu l'existence d'alternatives au fichage, tel le système des bonus-malus dans l'assurance, le dépôt de garantie et l'assurance contre les impayés locatifs, de nature à rendre le traitement incriminé excessif et non pertinent.

Le syndicat national des propriétaires et la société Checkpoint ont décidé néanmoins de mettre en œuvre le fichier malgré l'avis négatif de la Commission belge. Deux associations flamandes ont porté l'affaire sur le plan judiciaire dans le courant du premier trimestre 2003.

L'avis rendu par la Commission pour la vie privée est intervenu dans un contexte de crise aiguë du logement bruxellois. Tout comme en France, la création

1 Avis n° 52-2002 du 19 décembre 2002 relatif à la constitution d'un fichier externe des locataires défaillants.

2 Avis n° 21-2000 du 28 juin 2000.

3 Fichier de signalement entre compagnies d'assurance des risques spéciaux en assurance incendie, accidents et risques divers géré par le GIE Datassur.

d'un tel fichier s'inscrit en amont des dispositifs légaux encadrant les procédures d'expulsion, la perte du logement étant identifiée comme l'élément déclencheur de l'exclusion sociale.

D. Le fichier Préventel en progrès

Dans son précédent rapport annuel [1], la CNIL faisait un premier bilan des réclamations mettant en cause le fichier Préventel. Ce bilan soulignait que, comparé aux années précédentes, le nombre de ces plaintes était en constante évolution (132 plaintes en 2002, 88 en 2001, 43 en 2000). On rappellera que le fichier Préventel est mis en œuvre par un groupement d'intérêt économique, le GIE Préventel (GIE Prévention Télécommunications) et a pour finalité la prévention des impayés, dans le secteur de la téléphonie mobile, et dans celui de la téléphonie fixe. Ce fichier n'est toutefois, à ce jour, alimenté et consulté que par les opérateurs de téléphonie mobile et par les sociétés qui commercialisent leurs services (Bouygues Télécom, Orange France, SFR, Carrefour, Coriolis Télécom, Débitel France sont membres du GIE Préventel).

1. LES ERREMENTS DU PASSÉ

Peuvent être inscrits dans le fichier Préventel les abonnés débiteurs d'une somme supérieure ou égale à 40 euros [2], ainsi que les personnes qui auraient souscrit irrégulièrement un contrat d'abonnement auprès d'un ou plusieurs opérateurs (par exemple, en produisant des documents d'identité ou bancaires falsifiés).

Les personnes physiques peuvent exercer leur droit d'accès par courrier, auprès du GIE Préventel, service des consultations — TSA n° 90 003, 93588 Saint-Ouen cedex, en joignant la copie d'une pièce d'identité.

La plupart des plaintes reçues par la CNIL en 2002 révélaient des « dysfonctionnements » relatifs aux modalités d'alimentation et de consultation du fichier Preventel par les opérateurs de téléphonie mobile.

a) Alimentation du fichier

S'agissant de l'alimentation du fichier Préventel, de nombreuses plaintes provenaient d'abonnés à un opérateur de téléphonie qui contestaient soit le bien-fondé, soit le montant de la somme qui leur était réclamée ayant donné lieu à leur inscription dans le fichier Préventel. S'il convient de rappeler que les tribunaux judiciaires sont seuls compétents pour apprécier le caractère certain, liquide et exigible d'une créance, la CNIL a recommandé que la situation des clients contestant le montant ou le fondement juridique de la somme dont le paiement leur était réclamé, devait faire

1 *Cf.* 23e rapport d'activité 2002, p. 111.

2 Le seuil de 40 euros s'élevait jusqu'en octobre 2003 à 60 euros. Une déclaration modificative de ce fichier abaissant le seuil à 40 euros a été effectuée par le GIE Preventel auprès de la CNIL qui lui a délivré un récépissé de modification, le 22 octobre 2003.

l'objet, par les opérateurs qui sollicitaient leur inscription dans le fichier Préventel, d'une instruction contradictoire conduite dans un délai raisonnable, de façon non automatisée, assortie de la suspension du processus d'inscription dans le fichier Préventel.

Or, en 2002, la CNIL constatait que malgré ces recommandations exprimées à de nombreuses reprises, les membres du GIE Préventel ne procédaient pas, dans des conditions satisfaisantes, à une telle « instruction ». Ainsi, dans de nombreux cas, les plaintes témoignaient de ce que les requérants avaient tenté à plusieurs reprises de faire valoir leurs observations auprès de leur opérateur (par courriers simples, lettres recommandées, appels téléphoniques) sans jamais obtenir de réponse. C'est donc en dernier recours qu'ils s'adressaient à la Commission.

À l'issue de ce premier bilan, la CNIL ne pouvait qu'observer que les principales difficultés rencontrées par les plaignants résultaient de « dysfonctionnements » des services juridiques, commerciaux ou de recouvrement de leurs opérateurs de téléphonie (absence de gestion et de coordination entre ces services).

b) Consultation du fichier

S'agissant de la consultation du fichier Préventel, des plaintes révélaient que, lors d'une demande de souscription de contrat, les services des opérateurs analysaient mal ou trop rapidement les informations issues de cette consultation. Par exemple, certains opérateurs de téléphonie mobile recevant du GIE Préventel l'information selon laquelle la consultation du fichier permettait d'indiquer qu'il existait des réponses « phonétiquement approchée » du nom du requérant ou, une réponse se rapportant à un « homonyme né le même jour mais dans un autre département », refusait la souscription du contrat ou la subordonnait à la remise d'un dépôt de garantie.

2. UNE NETTE AMÉLIORATION EN 2003

En janvier 2003, la CNIL a « fermement » alerté le GIE Préventel et ses membres sur les défaillances qu'elle avait constatées, qu'il s'agisse de l'alimentation ou de la consultation du fichier Préventel. Dès cette date, le GIE Préventel et ses membres se sont engagés à prendre des mesures afin de mettre un terme à cette situation. En juin 2003, la Commission pouvait déjà observer que ces engagements avaient été respectés et les mesures prises efficaces.

a) Un bilan positif

L'année 2003 marque ainsi une nette baisse des plaintes mettant en cause le fichier Préventel, puisqu'en 2003, la CNIL a reçu soixante-quatorze réclamations concernant le fichier Préventel. Par ailleurs, le grand nombre d'appels téléphoniques qui parvenaient quotidiennement à la Commission en 2002 a très largement chuté en 2003. Ces appels, dans leur grande majorité, provenaient de personnes qui se

voyaient refuser la souscription d'un contrat par le personnel d'un point de vente au motif qu'elles étaient fichées dans Préventel alors qu'elles ne l'étaient pas.

En 2003, la Commission a donc reçu moins de réclamations concernant le fichier Préventel qu'elle n'en avait reçu en 2002 et en 2001.

Ce bilan de l'année 2003, certes positif, aurait pu l'être davantage. En effet, la majorité des réclamations reçues par la CNIL en 2003 a révélé, par leur typologie, que l'automatisation du processus d'inscription dans le traitement Préventel, par les membres du GIE Préventel, soulève toujours des difficultés, même si c'est dans des proportions plus raisonnables qu'auparavant.

Le manque de coordination entre les services des opérateurs, révélé par les réclamations reçues par la CNIL en 2001 et 2002, semble avoir été en partie résolu. Surtout, ce bilan a corroboré le fait que le paramétrage de la fonction dite du « phonétiquement approché » était à l'origine de l'afflux de telles réclamations pendant l'année 2002. Le nouveau paramétrage de cette application informatique, demandé par la Commission, paraît manifestement efficace. Ces résultats tendent également à réfuter l'argument selon lequel il existerait une « part incompressible d'erreurs » qui serait due à la mise en œuvre d'un fichier comportant un nombre important de personnes, en raison, s'agissant du fichier Préventel, de l'accroissement des utilisateurs de téléphonie mobile.

b) Exemples de difficultés persistantes

La majorité des réclamations reçues en 2003 émanent toujours d'abonnés qui contestent soit le bien-fondé, soit le montant de la somme qui leur est réclamée, ayant donné lieu à leur inscription dans le fichier Préventel.

C'est le cas de M. P. qui ouvre une ligne auprès d'un opérateur, en janvier 2003. Dès le lendemain, il constate que sa couverture réseau n'est pas satisfaisante et téléphone aux services de l'opérateur qui reconnaissent qu'il ne peut utiliser sa ligne de téléphone. Ils lui demandent d'adresser un courrier de résiliation sans préavis, ainsi que l'y autorise son contrat, pour ce motif. M. P. envoie ce courrier en recommandé avec accusé de réception, dans les délais qui lui sont impartis, et n'utilise pas sa ligne.

Trois semaines après, il reçoit une première facture avec avis de prélèvement. Il téléphone aux services de l'opérateur qui lui indiquent n'avoir aucune trace de son courrier de résiliation. Il envoie copie de son courrier de résiliation et parallèlement demande à sa banque de faire opposition aux prélèvements bancaires qui se présenteraient. Malgré ces démarches, M. P. reçoit une relance de paiement avant « résiliation de sa ligne pour non paiement ». Las d'écrire en vain et agacé par le prix que lui coûtent ses appels aux services de l'opérateur, M. P. décide d'ignorer cette affaire. Mais, quelque temps après, il reçoit une mise en demeure de l'opérateur l'informant de son inscription dans le fichier Préventel.

M. P. s'adresse donc à la Commission qui intervient auprès de l'opérateur. L'opérateur reconnaît que la demande initiale de résiliation de M. P. n'a pas été prise

en compte par ses services, qu'en tout état de cause la demande de M. P. était légitime et supprime son inscription du fichier Préventel.

Le cas de M. R. mérite également d'être évoqué pour son exemplarité. Il illustre en effet parfaitement l'absence de coordination entre les différents services d'un opérateur.

En décembre 2002, M. R. commande à son opérateur un nouveau téléphone mobile. Après une semaine d'attente, M. R. n'a toujours pas réceptionné l'appareil. Le service client de l'opérateur joint par téléphone lui indique qu'une enquête auprès des services de La Poste serait diligentée. Fin janvier 2003, M. R. n'a toujours pas reçu ce terminal et ne parvient pas à obtenir des explications du service client de l'opérateur. Excédé, il demande à sa banque de rejeter le prélèvement effectué par l'opérateur au titre de l'abonnement du mois de janvier et fait opposition aux prélèvements bancaires qui se présenteraient. En février 2003, M. R. reçoit simultanément une relance de paiement du service recouvrement de l'opérateur, ainsi qu'une facture pour la période du mois de février 2003. Afin d'expliquer la situation, il adresse un courrier recommandé au service recouvrement de l'opérateur, qui demeure sans réponse. Au mois de mars 2003, M. R. reçoit une mise en demeure de payer avec avis d'inscription dans le fichier Préventel.

M. R. écrit à la CNIL qui intervient auprès de l'opérateur. L'opérateur reconnaît que son service recouvrement a lancé une procédure à l'encontre de M. R. sans tenir compte de l'enquête diligentée auprès de la Poste par son service client. L'opérateur annule la facturation des périodes d'abonnement, procède à la mainlevée de l'inscription de M. R. du fichier Préventel et l'invite à retirer un téléphone portable dans l'un de ses points de vente.

Enfin, on soulignera qu'en 2003, la CNIL reçoit toujours autant de réclamations de personnes inscrites dans le fichier Préventel, alors qu'elles ont réglé leur dette auprès de leur opérateur. En outre, la majorité d'entre elles découvrait le maintien de leur inscription dans le fichier Préventel à l'occasion d'une nouvelle souscription de contrat.

Tel est le cas de M^me^ E. qui, en juin 2003, souhaite souscrire un contrat auprès d'un opérateur. On lui oppose un refus au motif qu'elle est inscrite dans le fichier Préventel. Surprise, M^me^ E. écrit au GIE Préventel qui lui répond que ses coordonnées ont été inscrites dans le fichier Préventel le 15 mars 2002 par son ancien opérateur. M^me^ E. a effectivement eu des impayés au titre de son ancien contrat en mars 2002, mais elle les a totalement soldés en juin 2002.

M^me^ E. écrit à la Commission qui interroge l'opérateur. L'opérateur reconnaît que M^me^ E. a soldé ses impayés au mois de juin 2002 et procède à la suppression de son inscription du fichier Préventel.

III. LE RECOUVREMENT DE CRÉANCES

A. Le recouvrement des créances locatives

1. LA NORME SIMPLIFIÉE DE GESTION IMMOBILIÈRE

L'analyse de la solvabilité des locataires est un enjeu important tant pour les propriétaires bailleurs que pour les agences immobilières. Ces dernières peuvent en effet être tenues responsables par les tribunaux du non-paiement du loyer par le locataire qu'elles ont choisi si, selon les termes employés, *« elles ne font pas diligence pour vérifier la solvabilité du locataire »*.

Face à ce risque, les professionnels proposent de plus en plus fréquemment aux bailleurs de souscrire une assurance destinée à se prémunir contre les loyers impayés et souhaitent recueillir et conserver dans leurs fichiers un grand nombre d'informations relatives à leur clientèle. En outre, les nouvelles dispositions relatives à la lutte contre le blanchiment de capitaux imposent aux professionnels une obligation de vigilance.

C'est dans ce contexte que la Commission a souhaité permettre notamment aux agences immobilières de bénéficier de la procédure de déclaration simplifiée prévue par l'article 17 de la loi n° 78-17 du 6 janvier 1978 en mettant à la disposition de la profession une norme simplifiée adaptée à ses nouveaux besoins. On rappellera que la norme simplifiée n° 21, adoptée par la Commission dès 1981, initialement relative à la gestion immobilière, a été élargie, en novembre 1999, aux activités de négociations immobilières, de gestion des associations syndicales libres ou encore des immeubles en jouissance à temps partagé.

À l'issue d'un travail de concertation avec les professionnels, la Commission a adopté, le 18 décembre 2003, la délibération n° 03-067 qui abroge et remplace la norme précédente. Le nouveau texte permet désormais une utilisation de la norme n° 21 dans le cadre de nouvelles finalités ainsi que le recueil d'un plus grand nombre d'informations.

À cette occasion, la norme a été étendue au minitel et à internet. Ces nouvelles technologies, aujourd'hui largement répandues dans le secteur de l'immobilier du fait de la généralisation des sites d'annonces immobilières, de gestion d'immeubles ou encore des services intranet mis en place par des syndicats de copropriétaires, peuvent désormais faire l'objet d'une déclaration simplifiée.

De même, face à l'essor considérable des dispositifs de contrôle d'accès dans les immeubles d'habitation (badges, cartes à puces ou « sans contact »), la Commission a souhaité permettre un allègement des formalités relatives à la mise en œuvre de ces systèmes s'ils ne permettent pas l'enregistrement des traces de passage des occupants. Elle a ainsi autorisé l'application de la norme à la gestion de l'attribution des dispositifs de contrôle d'accès en excluant les systèmes permettant la mémorisation des horaires d'entrée et de sortie des occupants en raison des dangers qu'ils présentent au regard de la vie privée.

2. LES RÈGLES DU RECOUVREMENT DE CRÉANCES ET DE L'ANALYSE DE SOLVABILITÉ

a) La préoccupation légitime de la solvabilité

Dans le secteur locatif social, la finalité « recouvrement de créance » a été admise par la Commission dès 1997 à l'occasion de la modification de la norme simplifiée n° 20. À la demande des professionnels du secteur privé, et compte tenu de la généralisation de tels traitements par les agences immobilières, la norme simplifiée n° 21 est aujourd'hui élargie, selon les termes demandés par les professionnels eux-mêmes, à l'*« analyse de solvabilité et au recouvrement de créance »*. Il s'agit de permettre aux bailleurs mandataires de s'entourer de précautions et de garanties suffisantes pour s'assurer de la capacité de financement du preneur d'un bien immobilier.

Comme cela avait été le cas à l'occasion de l'adoption de la norme simplifiée n° 13 relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit, la Commission a exclu de la norme les traitements relatifs au « calcul automatisé de l'appréciation du risque ».

Les nouvelles informations autorisées sont la conséquence directe des nouvelles finalités envisagées par la norme modifiée : ainsi l'adresse électronique des intéressés résulte de la prise en compte des nouvelles technologies, les coordonnées et l'identifiant des porteurs de badges de l'extension aux dispositifs de contrôles d'accès. Mais la plupart des informations désormais autorisées participent à un renforcement de la sécurité des transactions s'agissant tant du contrôle d'identité des co-contractants que de l'analyse de la solvabilité des preneurs.

Ainsi la Commission a considéré que les informations relatives à la nationalité et aux date et lieu de naissance des candidats locataires et de leur éventuelle caution sont utiles dans le cadre de l'extension de la norme au recouvrement de créance (elles doivent notamment figurer dans l'acte d'assignation). De telles données permettent en outre aux professionnels de s'assurer de l'identité des intéressés selon les obligations qui leur incombent en application des dispositions relatives à la lutte contre le blanchiment de capitaux provenant du trafic de stupéfiants. À cet effet, elles sont aussi recueillies s'agissant du vendeur ou encore de l'acquéreur d'un bien immobilier.

b) Marié ? Pacsé ?

Le régime matrimonial du vendeur, de l'acquéreur, du propriétaire d'un bien immobilier est une information qui peut être recueillie. Il s'agit là encore d'entourer les actes de négociation ou de gestion immobilière de certaines garanties et de s'assurer de la capacité des intéressés à contracter en vérifiant qu'ils disposent de droits sur les biens immobiliers concernés.

La Commission n'a en revanche pas estimé pertinent le recueil du régime matrimonial du locataire ou de sa caution du fait de la solidarité qui pèse sur les deux époux en application de l'article 1751 du Code civil.

La conclusion d'un pacte civil de solidarité par le locataire, l'acquéreur ou le propriétaire d'un bien immobilier pose un problème spécifique. L'information relative à l'engagement du futur locataire dans un pacte civil de solidarité constitue pour les bailleurs une garantie supplémentaire dans la mesure où elle instaure un principe de solidarité s'agissant notamment du paiement du loyer.

Sur le fondement de ce même principe de solidarité qui concerne aussi les charges de copropriétés ou encore les emprunts relatifs à l'achat de la résidence principale, la Commission a autorisé le recueil de cette information s'agissant du copropriétaire, du propriétaire ou encore de l'acquéreur d'un bien immobilier mais l'a refusé s'agissant de la caution du locataire.

La Commission, consciente de la nécessité pour le professionnel de s'entourer de certaines précautions, a néanmoins souhaité en fixer les limites dans le cadre d'une norme simplifiée. Les informations non prévues dans ladite norme peuvent, le cas échéant, être envisagées dans le cadre d'une déclaration ordinaire, sous réserve d'une appréciation au cas par cas de leur pertinence.

B. Bonnes et mauvaises pratiques dans le recouvrement de créances

La CNIL a connaissance des pratiques des sociétés spécialisées dans le recouvrement de créances au travers des plaintes qu'elle reçoit. Pour compléter son information, elle a entrepris une série de contrôles de ces organismes. Elle a examiné dans sa séance 16 décembre 2003 un rapport de synthèse portant sur des missions de vérification sur place réalisées auprès d'organismes procédant au recouvrement de créances pour le compte de tiers qu'il s'agisse de recouvrement amiable ou judiciaire, s'étant déroulées en 2002 et 2003.

Si certains manquements ont pu être relevés, d'une manière générale, les dispositions de la loi du 6 janvier 1978 ont été respectées. Les missions ont toutefois mis en lumière des carences dans l'accomplissement des formalités préalables et une certaine confusion dans la détermination des finalités des traitements et dans les déclarations de conformité à des normes simplifiées adoptées par la CNIL. Les organismes contrôlés ont cependant rapidement mis à jour leur situation au regard des formalités préalables devant être accomplies en application des dispositions de l'article 16 de la loi du 6 janvier 1978 et de ce point de vue la mission pédagogique attachée aux missions de vérification a été remplie.

1. LA TENUE DES FICHIERS DE DÉBITEURS

a) Manquements au droit d'accès et de rectification

Plusieurs particuliers, recevant des courriers d'un cabinet de recouvrement de créances leur réclamant le paiement de sommes d'argent, ont saisi la CNIL car ils n'arrivaient pas à obtenir une copie des informations les concernant détenues par cet

organisme. Ils souhaitaient en effet obtenir des précisions sur la nature et le montant de la créance qui leur était réclamée.

La CNIL a ainsi dû intervenir auprès de plusieurs cabinets de recouvrement de créances afin de leur rappeler que les articles 34 et suivants de la loi du 6 janvier 1978 prévoient que toute personne peut interroger le maître d'un fichier afin de savoir si des informations la concernant font l'objet d'un traitement. Le titulaire du droit d'accès peut en outre obtenir communication des informations le concernant. La communication, en langage clair, doit être conforme au contenu des enregistrements.

La CNIL a également été amenée à intervenir, dans des cas où des cabinets de recouvrement de créances réclamaient à des personnes le paiement d'une dette, alors qu'elles n'étaient pas concernées. Une erreur d'homonymie, commise par le cabinet de recouvrement de créances, était à l'origine de l'envoi de ces multiples courriers.

Les personnes concernées n'arrivant pas à se faire entendre des sociétés de recouvrement, la CNIL a dû intervenir auprès d'elles pour faire rectifier les informations concernant les plaignants, enregistrées dans leurs fichiers.

b) La part prépondérante des zones « bloc-notes »

Les opérations de vérification ont permis d'établir, à une exception près, résultant d'une très forte automatisation de l'application informatique, que la saisie libre dans des zones dites « bloc-notes » est pour beaucoup d'organismes le mode de gestion courante des dossiers de recouvrement : y est consigné l'ensemble des événements affectant l'instruction des dossiers de recouvrement, souvent de façon inutilement exhaustive. Ce mode de saisie linéaire n'est pas sans poser de problèmes au regard de la nécessaire pertinence des données.

La Commission a dû rappeler aux organismes concernés l'obligation de ne traiter que des données pertinentes, adéquates et non excessives au regard de la finalité de recouvrement, ainsi que les limitations nécessaires concernant le traitement de données sensibles.

Il est apparu en outre que les obligations découlant de la loi du 6 janvier 1978 étaient mieux respectées et comprises au sein des organismes ayant formalisé en interne, sous forme de code de déontologie ou tout autre support, le rappel des dispositions applicables et explicite de façon très concrète la déclinaison de ces obligations en les intégrant dans le traitement ordinaire des dossiers de recouvrement dont ils ont la charge.

c) Des durées de conservation souvent excessives

Ces mêmes organismes, dans le cadre d'une externalisation croissante de la gestion de créance, ont parfois en charge les archives du recouvrement : le dossier confié demeure après clôture chez le mandataire qui en assure l'accès à ses clients. La Commission a dû rappeler aux organismes contrôlés l'obligation de ne conserver les informations que le temps nécessaire à l'accomplissement de la finalité pour-

suivie, c'est-à-dire jusqu'à la clôture du dossier de recouvrement quel qu'en soit le motif.

L'extension de la durée de conservation pour répondre à des finalités connexes au recouvrement de créance, telles la mise à disposition du créancier d'un historique des dossiers confiés au travers d'un extranet, paraît admissible dès lors qu'elle ne concerne que des informations limitées au numéro du dossier, à l'identification des parties et montant de la créance recouvrée. Dans un tel cas, la communication de l'historique ne fait que rendre accessible à un destinataire légitime des informations conservées pour des raisons comptables.

Il est apparu en revanche à la Commission que la conservation de l'intégralité des informations relatives aux débiteurs pour faciliter ou orienter le recouvrement d'une créance sur un même débiteur, présente plus de risques de détournement de finalité et de manquement à la sécurité et à la confidentialité. Une telle conservation permet ainsi, comme cela a été constaté pour un organisme, d'effectuer des rapprochements entre plusieurs débiteurs présentant une donnée commune (même adresse, même nom de famille…) et accroît le risque d'erreur. Dans le même temps, la connaissance de l'insolvabilité d'un débiteur peut permettre une action favorable à ce dernier (classement du dossier suite à la délivrance immédiate du certificat d'irrécouvrabilité). Cette utilisation reste cependant marginale et doit être mise en rapport avec l'atteinte à la vie privée qu'elle génère.

Face au développement de l'archivage électronique, qu'il s'agisse de répondre aux obligations légales (responsabilité civile) ou à une externalisation croissante, la Commission a été conduite à attirer l'attention des organismes sur les précautions devant entourer les procédures d'archivage électronique afin de les rendre comptables avec l'obligation de ne conserver les données que pour une finalité déterminée. La Commission a notamment rappelé l'utilité de la séparation physique des bases de données destinées à la gestion courante et celles destinées à l'archivage. Elle a été conduite à évoquer ce que l'on pourrait considérer comme les conditions optimales permettant de concilier le développement de l'archivage électronique avec les principes posés par la loi du 6 janvier 1978, se matérialisant non pas en une copie (même sécurisée) de la base de données à l'identique sur un autre support, mais en une extraction de la base dans un format non indexé ne pouvant être lu que par une application spécifique.

d) La sécurité des traitements

D'une manière générale, la Commission a pu constater le caractère satisfaisant des moyens déployés pour assurer la sécurité des systèmes informatiques et la confidentialité des données enregistrées. En revanche, les échanges d'informations sous forme électronique avec les clients contenant (en pièces jointes ou non) les informations nominatives des débiteurs présentent une vulnérabilité certaine : ils se font en général en mode non crypté. Les représentants des organismes contrôlés, quelle que soit leur taille, ont indiqué ne pas avoir la possibilité d'imposer à leurs clients les formats et moyens de protection des données échangées. Un des organismes a développé un logiciel, fourni gratuitement aux clients, destiné à sécuriser les échanges et à

permettre une meilleure intégration dans l'application. Le développement de services aux clients par internet peut ainsi favoriser l'acceptation par les clients de modes d'échanges sécurisés.

La Commission a appelé toutefois l'attention des organismes sur la vigilance nécessaire dans la définition des conditions d'accès aux données et le contrôle régulier du bon fonctionnement du dispositif de sécurité mis en place.

2. LA RECHERCHE DU DÉBITEUR

La gestion du recouvrement judiciaire par les organismes de recouvrement de créance se limite en général au suivi des contacts avec les auxiliaires de justice, avec plus rarement la rédaction d'actes de procédures ou l'obtention d'une injonction de payer. Cette partie de l'activité des cabinets de recouvrement de créance n'appelle généralement pas de difficulté d'application de la loi du 6 janvier 1978, dès lors que les durées de conservation sont arrêtées et restent attachées à la finalité de recouvrement.

La gestion du recouvrement amiable et la recherche de débiteurs disparus sont plus problématiques. L'essentiel des manquements constatés porte sur la gestion du contact avec les débiteurs et leur entourage, notamment afin de faire pression sur ce dernier dans le cadre d'un recouvrement amiable, et sur la collecte d'informations relatives à la solvabilité du débiteur.

La recherche du contact avec l'entourage élargi du débiteur a souvent pour finalité de réaliser une enquête de solvabilité ou de collecter de nouvelles informations relatives à des débiteurs partis sans laisser d'adresse. L'entourage élargi comprend, en plus des proches du débiteur, le voisinage, l'employeur ou les collègues de travail, les collectivités locales, La Poste, la gendarmerie… Certains organismes, ainsi que l'ont révélé deux plaintes adressées à la CNIL en 2003, n'hésitent pas à prévoir des *scenarii* complets et détaillés d'appels téléphoniques auprès d'organismes publics tels que l'ANPE, l'Assistance publique, les URSSAF, les CAF, etc.

Si l'équilibre en la matière reste encore à trouver, et ce d'autant que les récentes modifications relatives au statut des agents privés de recherche n'ont pas apporté de réponse au problème posé par le caractère déloyal de la collecte et la proportionnalité de l'atteinte à la vie privée, certaines pratiques doivent clairement être écartées.

a) Les contacts avec le débiteur et son environnement

L'établissement d'un contact direct avec le débiteur représente pour le recouvrement amiable l'objectif premier des organismes de recouvrement de créance. Il favoriserait la solution amiable des litiges et la mise en place d'accords de paiement échelonnés. Des excès ont toutefois été constatés : un des organismes contrôlés, dans le cadre du suivi des accords de règlement consentis, a pour règle, dès lors qu'un incident a affecté le respect des accords de paiement, de rappeler systématiquement le débiteur, les jours précédant l'arrivée du terme de l'échéance, pendant les trois

mois suivants, alors que le débiteur respecte à nouveau ses engagements. La pression ainsi exercée permettrait, d'après l'organisme contrôlé, de prévenir tout nouvel incident.

Lorsque les coordonnées téléphoniques du débiteur ne sont pas connues, voire lorsque ce dernier se soustrait aux appels téléphoniques ou ne réagit pas aux courriers qui lui sont adressés, l'organisme de recouvrement de créance s'adresse souvent à l'entourage privé ou professionnel du débiteur, soit à partir de coordonnées connues et communiquées par le débiteur, soit grâce à des informations recueillies auprès de tiers ou par une consultation de l'annuaire afin de rechercher des membres présumés de la famille du débiteur. Cette pratique entraîne de surcroît une collecte déloyale d'informations nominatives relatives à des tiers dont les coordonnées sont associées à celles du débiteur.

Bien que, pour ces contacts, les organismes contrôlés aient bien intégré la nécessité de préserver la confidentialité des informations traitées et ne laissent que des messages ne laissant transparaître ni l'objet de l'appel ni la qualité de l'interlocuteur (« rappeler M. X. pour affaire vous concernant »), leur répétition ou la curiosité de la personne dépositaire du message rend aisée une identification de l'appel. Afin de pallier ce risque, certains agents de recouvrement ont pour instruction de laisser leur numéro de téléphone direct et de répondre aux appels sans présenter l'organisme. Une amélioration de la procédure pourrait être obtenue en proscrivant la répétition du message auprès d'un même interlocuteur.

Ces pratiques ne sont cependant pas acceptables lorsqu'elles se renouvellent avec insistance et sont de surcroît difficilement conciliables avec l'obligation de ne pas divulguer à des tiers des informations et portent ainsi une atteinte disproportionnée à l'intimité de la vie privée de l'intéressé (article 226-22 Code pénal).

b) La collecte d'informations auprès d'EDF

Les services d'EDF-GDF ont appelé l'attention de la CNIL sur les agissements d'un cabinet de recouvrement de créances qui leur adressait régulièrement des questionnaires leur demandant si telle personne avait toujours un abonnement à une adresse donnée et, dans la négative, d'obtenir sa nouvelle adresse.

La CNIL a rappelé à ce cabinet de recouvrement qu'EDF-GDF ne peut lui communiquer de telles informations nominatives sans enfreindre les dispositions de l'article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés aux termes desquelles le maître d'un traitement s'engage *« vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés »*.

En tout état de cause, une telle collecte de données nominatives auprès d'EDF-GDF ne serait pas conforme aux dispositions de l'article 25 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés aux termes duquel *« la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est*

interdite ». Le non-respect de cette interdiction est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 2u Code pénal).

Ce cabinet de recouvrement de créances a en conséquence renoncé à cette pratique.

c) Du recouvrement au « harcèlement »

M^me^ C. a alerté la CNIL à propos des faits suivants. Titulaire d'un crédit permanent auprès d'un établissement bancaire, elle expose que des changements importants sont intervenus dans sa situation professionnelle (congé de longue maladie), et qu'elle a, de ce fait, des difficultés à rembourser deux mensualités de retard, ce dont l'établissement bancaire est informé.

Or, depuis plusieurs mois, les services de recouvrement de l'établissement bancaire procèdent à de multiples appels téléphoniques auprès de la requérante et de son entourage. Ainsi, ces services de recouvrement ont téléphoné à son domicile, mais aussi sur son lieu de travail, dans sa maison de campagne dont le numéro, qu'elle n'a jamais communiqué, figure sur la « liste rouge » et enfin sur son téléphone mobile.

Ces services se seraient en outre présentés au téléphone comme étant un service de recouvrement de créances, révélant ainsi à des tiers la situation financière de M^me^ C. M^me^ C. ajoute que son fils, âgé de 12 ans, a répondu à certains de ces appels, alors qu'elle était sortie. Les propos qui lui auraient été tenus auraient été de nature, par leur insistance, à intimider l'enfant, voire l'inquiéter.

La CNIL est intervenue auprès de l'organisme bancaire en cause et lui a demandé de prendre des mesures pour que cessent de tels agissements. Elle lui a également rappelé, s'agissant de l'origine des informations ayant permis à cet organisme d'obtenir les numéros de téléphone des personnes contactées dans ce dossier, que l'article 25 de la loi interdit la collecte de données nominatives par tout moyen frauduleux, déloyal ou illicite.

3. LES MODIFICATIONS APPORTÉES PAR LES ORGANISMES CONTRÔLÉS

Les missions de contrôle ont été l'occasion pour la CNIL de rappeler aux organismes procédant au recouvrement de créances pour le compte de tiers les principes découlant de la loi du 6 janvier 1978 et leur articulation avec les traitements mis en œuvre. Elles ont permis un rappel pédagogique des conditions d'application de la loi du 6 janvier 1978 qui a été accepté et pris en compte par les modifications apportées aux conditions de mise en œuvre des traitements.

Les constats et observations effectués lors du contrôle ont notamment eu pour effet pour les organismes concernés respectivement :
— de combler les carences constatées en matière d'information des personnes et d'exercice du droit d'accès par la mise en œuvre de procédures propres à assurer l'effectivité du droit d'accès associé à une sensibilisation du personnel ;

— de provoquer un audit des déclarations de traitement effectuées, une régularisation et une mise à plat des méthodes utilisées dans le cadre de la recherche de débiteurs disparus ;
— l'établissement de règles d'archivage et la mise en œuvre de mesures propres à assurer le caractère pertinent, adéquat et non excessif des informations collectées, la vérification du bon fonctionnement du dispositif d'accès aux dossiers par internet ;
— l'effacement des données dénuées de pertinence ou des articles 30 et 31 de la loi du 6 janvier 1978 (données sensibles et informations relatives aux infractions et condamnations) et un renforcement des instruments destinés au contrôle du contenu des zones « bloc-notes » ;
— la remise à plat de l'ensemble du processus de traitement des dossiers de recouvrement afin d'aboutir « à une configuration exemplaire » comprenant une procédure automatisée d'archivage des données, une purge systématique des zones bloc-notes, le renforcement des mesures destinées à assurer la sécurité des traitements, la mise en place d'un code de conduite en interne, d'un code de déontologie à destination des prestataires et de recommandations pour les mandants, et la régularisation des dossiers de formalités préalables ;
— l'interdiction immédiate de l'utilisation des zones bloc-notes à l'ensemble des collaborateurs et la suppression manuelle des informations non pertinentes, dans l'attente de l'intégration d'une solution logicielle permettant de purger les zones bloc-notes des dossiers clôturés et remplaçant les zones bloc-notes par des champs de saisie préformatés.

Chapitre 8

L'EXERCICE DE LA TRANSPARENCE

La loi « informatique et libertés » est une loi de protection du secret de la vie privée. Cette nécessité du secret est particulièrement forte quand elle touche à des données aussi sensibles que les données génétiques dont la collecte même est strictement encadrée ou les informations contenues dans un dossier médical. La loi de 1978 est aussi une loi de transparence puisqu'elle impose l'information des personnes sur l'existence et la mise en œuvre d'un traitement les concernant et qu'elle organise le droit d'accès aux données traitées. Or, l'exercice de la transparence s'avère délicat pour les données relatives à l'intimité de la vie privée ou à l'identité génétique. Ainsi par exemple le secret des origines des enfants « nés sous X » limite leur droit d'accès. De même, l'information individuelle des malades du cancer sur leur insertion dans des registres épidémiologiques est difficile à assurer.

Dans le monde du travail, les règles posées par la loi et par la CNIL sont claires mais l'exemple des dossiers de recrutement montre que les difficultés d'application ne viennent pas seulement de la mauvaise volonté de l'employeur.

I. LES DONNÉES GÉNÉTIQUES

À l'initiative du directeur général de l'UNESCO, le Comité international de bioéthique de l'UNESCO [1] a entamé la rédaction en 2002 d'une déclaration sur les données génétiques qui se situe dans le prolongement de la Déclaration universelle sur le génome humain et les droits de l'homme, adoptée le 11 novembre 1997. Un

1 Le Comité international de bioéthique est à l'heure actuelle la seule instance à caractère international dans le domaine de la bioéthique.

groupe de rédaction a été constitué afin de réfléchir sur le contenu de cet instrument international et d'en élaborer un projet.

C'est dans le cadre de ce travail d'élaboration que le projet de déclaration a fait l'objet d'une très large concertation internationale auprès des États membres, des autorités de protection des données, des organismes non gouvernementaux concernés et des experts. La CNIL a donc été sollicitée par l'UNESCO pour apporter sa contribution à la rédaction de ce texte et pour faire valoir ses observations sur son contenu et son ordonnancement.

Le projet de déclaration internationale sur les données génétiques comporte des dispositions générales rappelant la spécificité des données génétiques, les finalités pour lesquelles elles peuvent être collectées et utilisées et le principe de non-discrimination. Il consacre également plusieurs dispositions à la collecte des données génétiques, aux modalités du consentement de la personne, au traitement et à l'utilisation des données génétiques.

Ce texte s'inscrit dans un contexte particulier marqué par une multiplication de projets visant à accumuler dans des fichiers de population des données génétiques. L'exemple de l'Islande est désormais classique [1] mais on peut également citer l'Estonie, l'île de Tonga dans le pacifique et les projets australien et néo-zélandais. Il semble même, qu'en Europe, au-delà des fichiers d'empreintes génétiques constitués dans des domaines particuliers et encadrés sur le plan juridique, comme par exemple dans le domaine criminel, se dessinent des projets de fichiers de population constitués à partir des données génétiques. Ainsi, le Royaume-Uni aurait un projet de constitution d'une « biobank » qui rassemblerait les échantillons d'ADN de tous les hommes et femmes âgés de 45 à 69 ans afin de mettre à disposition de la communauté scientifique le matériel nécessaire à la recherche. De même on constate la multiplication sur internet d'offres permettant la réalisation de tests génétiques en particulier dans le domaine de l'établissement de paternité. Il semble dès lors nécessaire que des principes communs, en particulier sur le consentement et l'information des personnes, soient affirmés.

A. La reconnaissance d'une spécificité et d'une protection particulière

1. LA SPÉCIFICITÉ DES DONNÉES GÉNÉTIQUES

Les données génétiques présentent en elles-mêmes des caractéristiques qui les rendent singulières en particulier par rapport aux données de santé. Le projet de déclaration définit cette spécificité en disposant que les données génétiques fournissent, ou sont susceptibles de fournir, dans l'avenir une information scientifique, médicale et personnelle pertinente tout au long de la vie d'un individu, que cette information peut également avoir une incidence significative sur la famille de l'inté-

1 Actes de la 23e conférence internationale des commissaires à la protection de données, septembre 2001, Paris, p. 52 et ss.

ressé, sur plusieurs générations et dans certains cas sur l'ensemble du groupe auquel appartient l'individu. Dès lors, ces données doivent être traitées avec une attention particulière.

La reconnaissance de cette spécificité devrait, selon la CNIL, être complétée d'une mention sur le caractère unique de l'identification par l'empreinte génétique. En effet, et c'est une des caractéristiques des données génétiques, elles sont susceptibles de révéler des informations sur plusieurs personnes tout en ne permettant de n'en identifier qu'une seule. Elles révèlent l'unicité de la personne.

Le projet de déclaration sur la portée du texte intègre les échantillons biologiques à partir desquels les données génétiques humaines sont générées et qui sont définis comme toute cellule dont le noyau contient la constitution génétique caractéristique d'un individu.

2. UNE PROTECTION PARTICULIÈRE

La spécificité des données génétiques justifie une protection juridique particulière.

a) Dans les législations sectorielles

C'est d'ores et déjà le cas en droit français où les différentes finalités pour lesquelles les données génétiques peuvent être collectées sont définies et encadrées tant dans le Code de la santé publique que dans le Code civil. Ainsi, le Code civil, dans son article 16-13, interdit toute discrimination en raison des caractéristiques génétiques de la personne. Le Code de la santé publique et le Code du travail comportent également des dispositions encadrant les utilisations possibles des données génétiques.

Dans le secteur de la protection sociale, depuis une loi du 27 juillet 1999, il est interdit aux organismes de sécurité sociale et aux organismes de protection complémentaire en matière de santé de tenir compte des résultats de l'étude génétique d'une personne, même si ceux-ci sont apportés par la personne elle-même. Ces organismes ne peuvent poser aucune question relative aux tests génétiques et à leurs résultats, ni demander à une personne de se soumettre à des tests génétiques avant que ne soit conclu un contrat de protection complémentaire en matière de santé et pendant toute la durée de celui-ci. Toute infraction à ces dispositions est punie d'un an d'emprisonnement et d'une importante amende financière.

Dans le secteur des assurances, il est désormais prévu par la loi (article L. 1141-1 du Code de la santé publique issu de la loi du 4 mars 2002) que les sociétés d'assurance ne doivent pas tenir compte des résultats de l'examen des caractéristiques génétiques d'une personne demandant à bénéficier d'une garantie de risque d'invalidité ou de décès, même si ceux-ci leur sont transmis par la personne concernée ou avec son accord. En outre, ils ne peuvent poser aucune question relative aux tests génétiques et à leurs résultats, ni demander à une personne de se

soumettre à des tests génétiques avant que ne soit conclu le contrat et pendant toute la durée de celui-ci.

Dans le secteur du travail, le Code pénal interdit, sous peine de sanctions pénales, tout refus d'embauche, sanction ou licenciement, fondé sur une discrimination commise à l'égard de personnes à raison notamment de leur origine, de leur état de santé, de leur handicap et de leurs caractéristiques génétiques (loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santés-articles 225-1 et 225-2 du Code pénal).

Des dispositions analogues ont été insérées dans le Code du travail. Ainsi, aucune personne ne peut être écartée d'une procédure de recrutement et aucun salarié ne peut être sanctionné ou licencié en raison de son origine, de son sexe, de ses mœurs, de sa situation de famille et de ses caractéristiques génétiques (article L. 122-45 du Code du travail modifié par la loi précitée du 4 mars 2002).

b) Dans la législation sur la protection des données

Dans la loi « informatique et libertés », les données génétiques ne sont citées qu'au titre des dispositions du chapitre V*bis* sur la recherche dans le domaine de la santé (prélèvements biologiques identifiants) et pour soumettre leur collecte au recueil du consentement exprès de la personne.

Dans la directive européenne du 24 octobre 1995, les données génétiques sont indirectement visées par l'article 2 qui définit les données personnelles comme toute information concernant une personne physique identifiée ou identifiable… directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Dans le projet de loi informatique et libertés tel qu'il a été adopté en première lecture par l'Assemblée nationale et par le Sénat, si les données génétiques ne sont pas explicitement citées au titre des données sensibles de l'article 8 — qui cite toutefois les données de santé —, elles le sont de façon explicite à l'article 25 qui énumère la liste des traitements soumis à un régime d'autorisation préalable.

La Commission a estimé que le projet de déclaration devrait préciser que les études de génétique de population de grande envergure, ayant vocation à concerner l'ensemble d'une population, doivent s'inscrire dans le respect des principes de protection des données à caractère personnel et que les autorités de protection des données personnelles doivent également être consultées sur les règles ou les normes destinées à encadrer l'utilisation des données génétiques.

Le projet de déclaration rappelle également la nécessité de fournir à la personne dont le consentement est recherché des informations claires, objectives et détaillées qui doivent préciser les finalités pour lesquelles les données génétiques humaines et les échantillons biologiques sont collectés ainsi que la raison de leur traitement et de leur éventuelle conservation. Ces dispositions sont importantes à rappeler à l'heure où se développent des tests de paternité sur internet sans qu'aucune garantie particulière ne soit prise pour assurer l'information et le recueil du

consentement de toutes les personnes susceptibles d'être concernées par de tels tests. Elles rejoignent le souci déjà exprimé par la CNIL d'un consentement dit « libre et éclairé » qui doit être impérativement précédé d'une information claire et détaillée.

La référence, à l'article 10 du projet de déclaration, au droit de ne pas savoir dans le cadre d'une recherche ou d'un dépistage d'une maladie déterminée, visée à l'article 9 du projet de déclaration, mérite une attention particulière. Confrontée, dès 1987, à cette délicate question lors de l'examen de projets de recherches sur certains marqueurs génétiques rares (8e rapport annuel, p. 301), la Commission, après une longue réflexion et de nombreuses consultations, avait estimé, sans contester la légitimité de la prévention, particulièrement opportune dans le cas des maladies — telle le glaucome — où il existe un traitement, qu'il n'était pas opportun de prévenir systématiquement les familles des patients porteurs du gène d'une maladie incurable et de générer ainsi chez elles une angoisse permanente sans qu'il en résultât un réel bénéfice direct pour elles. Cette préconisation de la CNIL avait d'ailleurs été renforcée par un avis du Comité national d'éthique français du 30 octobre 1995 (intitulé « Génétique et médecine : de la prédiction à la prévention »), qui a réaffirmé le droit pour le patient « de ne pas savoir », estimant que le secret médical devait être préservé vis-à-vis des tiers, y compris des membres de la famille, et qu'il incombait en conséquence non pas au médecin, mais au patient porteur du gène d'une maladie.

B. Des finalités encadrées

1. L'IMPORTANCE DU PRINCIPE DE FINALITÉ

Énumérées à l'article 5 du projet de déclaration, ces finalités sont similaires à celles déjà admises en France et dans la plupart des pays dotés d'une législation en la matière. Ainsi, les données génétiques peuvent être utilisées dans le cadre de l'établissement d'un diagnostic et de soins de santé, pour la recherche médicale et toute autre recherche scientifique, y compris les études de génétique des populations et les études épidémiologiques ou anthropologiques, en médecine légale, dans le cadre de procédures civiles ou pénales et pour toute autre fin compatible avec la Déclaration universelle sur le génome humain et les droits de l'homme et avec le droit international des droits de l'homme.

Le projet de déclaration dispose que les données génétiques collectées en vue d'une finalité spécifique ne doivent pas être utilisées en vue d'une autre finalité, sauf si le consentement préalable, libre, éclairé et exprès de la personne concernée, a été obtenu ou s'il en est ainsi décidé par la loi ou la réglementation nationale.

Dans le domaine de l'utilisation des données génétiques et des prélèvements biologiques attachés à une personne, le respect de la finalité apparaît essentiel au regard des potentialités informatives que revêt l'information génétique. Une donnée collectée dans le cadre d'une consultation de génétique médicale ne devrait pas pouvoir être utilisée dans le cadre d'une recherche criminelle. De même, une prise de sang effectuée dans le cadre de la conduite d'un essai de pharmacogénétique

destiné à évaluer l'efficacité d'un médicament au regard du profil génétique ne devrait pas pouvoir être utilisée ultérieurement pour déterminer l'empreinte génétique de la personne dans le cadre d'une recherche de paternité. Si le matériel est le même, les finalités et les utilisations sont très différentes et doivent être distinguées.

Le respect du principe de finalité constitue dès lors une garantie importante de nature à prévenir des utilisations non prévues. Ainsi, le fait que la loi du 18 mars 2003 pour la sécurité intérieure ait prévu que les empreintes génétiques réalisées dans le cadre de la recherche de certaines infractions limitativement énumérées, ne soient réalisées qu'à partir de segments d'ADN non-codants — c'est-à-dire non susceptibles, en l'état de la science, de révéler d'éventuelles prédispositions génétiques —, à l'exception du segment correspondant au marqueur du sexe, est de nature à prévenir toute utilisation par exemple à des fins de dépistage de certaines maladies. À cet égard, la Commission a considéré que les dispositions du projet de déclaration qui concernent la destruction des données génétiques collectées au cours d'une enquête criminelle devraient être complétées de façon à ce que les empreintes génétiques conservées à des fins criminelles ne puissent être réalisées qu'à partir de segments non-codants de l'ADN à l'exception du marqueur correspondant au sexe.

2. LES LIMITES DU CONSENTEMENT

Admettre comme le propose le projet de déclaration, que les données génétiques puissent être utilisées à des fins autres que celles pour lesquelles elles ont été collectées, au motif que la personne aurait donné son accord exprès à une autre utilisation n'est pas de nature à la protéger contre des utilisations abusives et pourrait permettre par exemple à des services de police, au seul motif qu'ils auraient obtenu le consentement de l'intéressé, de procéder à la collecte et au traitement des données génétiques ou des prélèvements biologiques collectés et conservés à des fins d'identification génétique.

La Commission a estimé ainsi qu'il serait également utile que le texte proposé par l'UNESCO soit modifié de façon à préciser que le seul consentement de la personne ne suffit pas à permettre l'utilisation des données génétiques à des fins autres que celles pour lesquelles elles ont été initialement collectées. Seule une loi peut autoriser la collecte et le traitement de telles données même si la personne a donné son consentement exprès.

C'est ainsi qu'aux termes de l'article L. 1141 du Code de la santé publique, il est expressément prévu que les sociétés d'assurance ne doivent pas tenir compte des résultats de l'examen des caractéristiques génétiques d'une personne demandant à bénéficier d'une garantie de risque d'invalidité ou de décès, même si ceux-ci leur sont transmis par la personne concernée ou avec son accord.

La conférence générale de l'UNESCO a adopté le 16 octobre 2003, au cours de sa 32e session, la déclaration internationale sur les données génétiques humaines. Ce texte de principe reste général et, dans la mesure où il ne revêt pas de valeur contraignante, laisse aux États participants une marge de manœuvre importante pour la mise en application des principes qu'il contient.

II. LES ORIGINES PERSONNELLES

La loi du 22 janvier 2002 relative à l'accès aux origines des personnes adoptées et pupilles de l'État a introduit dans le Code de l'action sociale et des familles plusieurs dispositions visant à favoriser le rapprochement des enfants « nés sous X » de leurs parents de naissance. Afin de faciliter la réalisation de cet objectif, cette loi a notamment créé un Conseil national pour l'accès aux origines personnelles (CNAOP), chargé d'assumer un rôle actif dans les recherches entamées par les personnes « nées sous X » ou par leurs parents de naissance.

Le législateur a prévu qu'un décret pris après avis de la CNIL devait fixer les conditions dans lesquelles seraient traitées et conservées les informations susceptibles de révéler l'identité des parents biologiques ou des éléments non nominatifs de leur histoire personnelle.

La CNIL a donc été amenée à se prononcer sur les garanties apportées par le projet de décret qui lui a été soumis par le ministère de la Santé, de la Famille et des Personnes handicapées, mais également sur les dispositions de ce projet de texte relatives au suivi informatique des dossiers traités par le CNAOP. La CNIL a recherché, dans sa délibération n° 03-007 du 4 février 2003, la définition d'un cadre sécurisé et respectueux de l'équilibre établi par la loi du 22 janvier 2002 reconnaissant à la fois le droit pour l'enfant « né sous X » à la recherche de ses origines personnelles et le droit pour les parents de naissance au secret de leur identité.

Avant tout, la CNIL s'est attachée à ce que soit défini un cadre sécurisé pour le traitement, informatisé ou non, des données personnelles recueillies par le CNAOP, compte tenu de la sensibilité de ces données. Celles-ci sont en effet susceptibles de révéler l'identité de parents de naissance d'enfants « nés sous X », information couverte par le secret et qui ne peut être communiquée, via le CNAOP, à l'enfant concerné qui en aurait fait la demande qu'avec l'accord de ces parents.

Au-delà, ces informations — recueillies par le CNAOP auprès des établissements de santé, des services départementaux, des organismes autorisés et habilités pour l'adoption, de l'autorité centrale pour l'adoption ou de la mission pour l'adoption internationale — peuvent porter sur la santé des parents, les origines de l'enfant et les circonstances de la naissance, à la condition que les parents de naissance aient souhaité l'intégration de ces informations dans le dossier de leur enfant.

Ainsi, des mesures de sécurité particulières ont été retenues dans le cadre du projet de décret afin que soit garantie la confidentialité des données communiquées au CNAOP, tant au moment de leur transmission qu'à l'occasion de leur conservation dans les locaux du Conseil, et ce quel que soit leur support.

S'agissant plus particulièrement des données enregistrées sur support informatique, seule l'identité des personnes ayant saisi le CNAOP, des parents adoptifs du demandeur d'accès et des correspondants départementaux du CNAOP, apparaît dans l'application informatique. Les autres informations enregistrées se limitent aux données nécessaires au suivi administratif des dossiers et des échanges de

correspondances avec les structures publiques ou privées en rapport avec le CNAOP, et à la production de statistiques d'activité anonymes.

Aucune information sensible au sens de la loi du 6 janvier 1978 — telle que l'origine raciale, les mœurs ou la religion des parents — n'est traitée informatiquement. L'identité supposée des parents de naissance susceptible d'être communiquée au CNAOP n'est en aucun cas enregistrée sur support informatique.

En outre, le CNAOP est amené, pour l'accomplissement de ses missions, à contacter des tiers (services départementaux, organismes sociaux, organismes d'adoption, personne mandatée pour les recherches, procureur de la République) pour obtenir des informations. Là encore, la CNIL a été attentive à ce que ces tiers ne reçoivent du CNAOP que les données nécessaires à l'identification du dossier concerné par la structure dépositaire.

De même, la CNIL a veillé à ce que le décret prévoie que le titulaire du droit d'accès ne puisse accéder qu'aux informations relatives à sa demande ou à la déclaration, ainsi qu'à son suivi, sous réserve que l'exercice de ce droit ne porte pas atteinte à la vie privée d'autrui. En d'autres termes, le droit d'accès prévu par la loi du 6 janvier 1978 ne peut en aucun cas constituer un fondement juridique suffisant pour obliger le CNAOP à transmettre des données couvertes par le secret des origines.

III. LES DONNÉES MÉDICALES

A. Le réajustement des instruments d'investigation épidémiologique

Saisie du projet de loi relatif à la politique de santé publique, la Commission a souhaité faire part au ministre de la Santé d'un certain nombre d'observations [1] sur les dispositions du texte rassemblées dans le chapitre consacré aux systèmes d'information et intéressant l'application de la loi informatique et libertés. Ces dispositions ont pour objectif principal d'élargir les cas dans lesquels des données personnelles de santé peuvent être transmises et utilisées à des fins de santé publique.

1. LES NOUVELLES CONDITIONS DE TRANSMISSION DE DONNÉES DE SANTÉ À L'INSEE

a) Évolution législative

L'article 13-I du projet de loi prévoit une modification des deux premiers alinéas de l'article 7 bis de la loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistique. L'objectif poursuivi est de permettre à l'INSEE et aux

1 Le projet de loi a fait l'objet d'une adoption en première lecture à l'Assemblée nationale le 14 octobre 2003 et au Sénat, le 19 janvier 2004.

services statistiques ministériels d'accéder aux données à caractère personnel relatives à la santé, à l'exclusion des données relatives à la vie sexuelle, et ce dans le cadre d'établissement de statistiques sur l'état de santé de la population, les politiques de santé publique ou les dispositifs de prise en charge par les systèmes de santé et de protection sociale en lien avec la morbidité des populations concernées.

Jusqu'à présent, l'INSEE et les services statistiques ministériels pouvaient être destinataires d'informations relatives aux personnes physiques recueillies, dans le cadre de sa mission, par une administration, un établissement public, une collectivité territoriale ou une personne morale de droit privé gérant un service public à des fins exclusives d'établissement de statistiques, à l'exclusion cependant des données relatives à la santé ou à la vie sexuelle. C'est en 1986 (loi du 23 décembre 1986) que les dispositions de l'article *7bis* ont été insérées dans la loi du 7 juin 1951 afin de donner un fondement juridique à la communication à l'INSEE ou aux services statistiques ministériels d'informations nominatives et de documents recueillis par les administrations sous le couvert du secret professionnel dans l'exercice quotidien de leurs missions de gestion.

Au cours de l'examen du projet de loi qui lui avait alors été soumis, la Commission avait exprimé certaines réserves vis-à-vis de l'absence de garanties prévues en ce qui concerne les conditions de transmission des données relatives à la santé et à la vie sexuelle.

Le Gouvernement avait à l'époque, tenu compte des réserves de la CNIL puisque la loi du 23 décembre 1986 a finalement exclu les données de santé et celles relatives à la vie sexuelle.

Le projet de loi actuel revient donc sur ces dispositions au motif que cette interdiction limiterait les possibilités de mise en œuvre d'outils statistiques en matière de santé publique.

Il convient de noter que l'alinéa 3 de l'article *7bis* — que le projet de loi relative à la politique de santé publique laisse inchangé — précise que ces cessions d'informations doivent s'effectuer dans le respect des dispositions de la loi du 6 janvier 1978 et, qu'en particulier, une convention entre le cédant et le cessionnaire précise les modalités de la transmission, la finalité du traitement envisagé et le sort des informations après leur utilisation aux fins de traitement statistique.

b) Quels services destinataires ?

La référence aux services statistiques ministériels en général a soulevé des objections de la Commission. Certes, ces services ministériels sont, en vertu du décret du 17 juillet 1984 modifié relatif au Conseil national de l'information statistique, définis précisément comme étant des services producteurs rattachés à l'INSEE mais on peut s'interroger, nonobstant la protection apportée par la loi informatique et libertés, sur la légitimité qu'auraient d'autres services statistiques ministériels à être destinataires de données personnelles relatives à la santé des personnes. La Commission a considéré qu'il convenait de limiter la possibilité de transmettre des données

personnelles de santé aux seuls services qui participent à la définition et à la conduite de la politique de santé publique.

La Commission a également estimé que le projet de loi devait être complété pour préciser les garanties prévues afin d'assurer la confidentialité des données.

Le Gouvernement a suivi dans une large mesure ces recommandations. Le projet de loi a en effet été complété pour préciser, comme l'avait suggéré la CNIL, que seuls des « […] *services statistiques des ministères participant à la définition, à la conduite et à l'évaluation de la politique de santé publique* » pourront avoir connaissance de données de santé. L'avis du Conseil national de l'information statistique est également ajouté comme préalable à toute cession de données à l'INSEE.

L'article 13-I est également complété, comme l'avait souhaité la CNIL, de trois alinéas rappelant que les données ne doivent être cédées que sous une forme ne permettant pas l'identification des personnes concernées et que toute dérogation à ce principe devra s'inscrire dans le respect des dispositions de la loi informatique et libertés. Des garanties sont en outre prévues pour s'assurer de la qualité des personnes appelées à recevoir et à traiter les données.

2. AUTRES MESURES DU PROJET DE LOI RELATIF À LA POLITIQUE DE LA SANTÉ PUBLIQUE

a) La communication de données par l'assurance maladie

La rédaction de l'article 13-II a pour objet de compléter l'article L. 161-29 du Code de la sécurité sociale pour reconnaître la possibilité au personnel non médical des organismes d'assurance maladie soumis au secret professionnel de déroger à ce secret afin de permettre la transmission de données identifiantes dans le cadre de recherches dans le domaine de la santé conduites conformément aux dispositions de la loi du 6 janvier 1978.

Cette disposition n'a pas appelé d'observation particulière de la part de la Commission.

b) L'exploitation des données des services publics départementaux de protection maternelle et infantile

L'article 13 — IV prévoit de compléter l'article L. 2132-3 du Code de la santé publique par une disposition prévoyant la transmission par chaque service public départemental de protection maternelle et infantile au ministre chargé de la Santé de données de santé issues des examens obligatoires donnant lieu à l'établissement d'un certificat de santé, sous forme agrégée et sous forme personnelle, à l'exclusion dans ce dernier cas du nom et du prénom, du jour de naissance et de l'adresse détaillée. Il est prévu que les conditions de cette transmission sont fixées par arrêté pris après avis de la CNIL.

La Commission a estimé que la nécessité de disposer de données personnelles n'était pas démontrée, aucune justification précise n'étant avancée sur ce point.

En tout état de cause, les modalités d'une telle transmission d'informations devront être précisées et, tout particulièrement, la manière dont l'anonymat des enfants sera respecté.

La rédaction retenue aux termes de la première lecture précise la finalité de suivi statistique et épidémiologique de la santé des enfants et les garanties prévues pour préserver la confidentialité des données.

c) Une finalité supplémentaire pour le SNIIRAM

Aux termes de l'article L. 161-28 du Code de la sécurité sociale, le système national d'information interrégimes de l'assurance maladie (SNIIRAM) a été créé pour améliorer la connaissance des dépenses de l'ensemble des régimes d'assurance maladie et permettre la transmission en retour aux prestataires de soins d'informations sur leur activité. Une seule base de données, préservant l'anonymat des assurés, est gérée par la CNAMTS et comporte les données issues des fichiers des caisses d'assurance maladie et en particulier les informations résultant des traitements des feuilles de soins ainsi que les données sur l'activité hospitalière, issues du programme de médicalisation des systèmes d'information [1].

L'article 13 du projet de loi prévoit de compléter l'article L. 161-28-1 du Code de la sécurité sociale d'une disposition étendant la finalité du système à la définition, à la mise en œuvre et à l'évaluation de politiques de santé publique.

Ces dispositions seraient justifiées par l'impossibilité actuelle d'utiliser des échantillons extraits du SNIIRAM pour mener des études spécifiques en matière de santé publique.

La CNIL a observé que l'utilité de cet ajout n'apparaissait pas clairement dans la mesure où l'arrêté du 11 avril 2002 relatif à la mise en œuvre du SNIIRAM prévoit d'ores et déjà la possibilité pour un chercheur d'accéder à des données individuelles relatives aux bénéficiaires dans les conditions prévues aux articles 40-11 à 40-15 de la loi du 6 janvier 1978.

d) La transmission des certificats de décès

Face aux difficultés rencontrées cet été pour obtenir des informations sur les décès liés à la canicule, le gouvernement a souhaité modifier l'article L. 2223-42 du Code général des collectivités territoriales afin d'élargir l'accès de ces certificats, qui indiquent la ou les causes de décès, aux organismes (dont la liste est fixée par décret en Conseil d'État pris après avis de la CNIL) et préciser les utilisations possibles de ces données.

Cette disposition qui n'a pas soulevé d'observation particulière de la part de la Commission, a fait l'objet d'une nouvelle rédaction à la fin de l'été afin de prévoir l'utilisation des données du certificat de décès à des fins de veille et d'alerte par l'État et par l'Institut de veille sanitaire.

1 22e rapport annuel de la CNIL p. 62 et ss.

B. L'information des malades

1. L'APPLICATION DE LA LOI SUR LES DROITS DU MALADE

La loi du 4 mars 2002 a posé le principe d'un droit d'accès direct, par le patient, à l'ensemble des données personnelles de santé [1]. On rappellera qu'avant l'adoption de cette loi, l'accès à ces données ne pouvait s'effectuer que par l'intermédiaire d'un médecin.

Le principe du droit d'accès direct aux données personnelles de santé, rapidement connu des citoyens, s'exerce d'ores et déjà assez régulièrement auprès des professionnels de santé. Ainsi, la Commission a pu constater que les réclamations qui lui sont adressées ont été plus nombreuses en 2003 en cette matière.

a) CADA et CNIL

Les réclamations émanent principalement des patients qui, ayant exercé le droit d'accès auprès d'un établissement public hospitalier, d'une clinique ou de leur médecin traitant, n'ont pas obtenu de réponse ou ont obtenu une réponse qu'ils estiment incomplète.

Or, il convient d'emblée de souligner, qu'en cette matière, la CNIL n'est compétente que dans l'hypothèse où le patient souhaite accéder à son dossier médical détenu par un établissement de santé privé ou un professionnel de santé exerçant à titre libéral.

En effet, lorsque le droit d'accès est exercé auprès d'un établissement de santé public ou participant au service public hospitalier, ou encore, lorsque les données de santé concernent une personne décédée auxquelles les ayants droit peuvent accéder, la réclamation, qui découle de l'absence de réponse à de telles demandes, doit être adressée à la Commission d'accès aux documents administratifs (CADA), instaurée par la loi du 17 juillet 1978 modifiée par la loi du 4 mars 2002.

Cette « double » compétence entre la CNIL et la CADA, n'est bien sûr, pas, ou peu, connue des citoyens qui, lorsqu'ils n'ont pas de réponse à leur demande d'accès à leurs données personnelles de santé, s'adressent parfois à tort à la CNIL. Il est vrai que la CNIL elle-même, dans son précédent rapport d'activités, n'avait pas mis en lumière cette complication.

Tel est le cas, entre autres exemples, de M. P. qui, cherchant à obtenir son dossier médical, s'est adressé, en vain, au service des urgences d'un groupe hospitalier où il avait été admis. M. P. saisit la CNIL qui transmet le dossier à la CADA.

M^me^ L. cherche à comprendre les circonstances du décès de sa mère dans un centre hospitalier régional universitaire. Elle demande donc à cet établissement de santé de lui communiquer le dossier médical de sa mère. Estimant que la réponse qui lui a été adressée n'est pas satisfaisante M^me^ L. saisit la CNIL qui, là encore, transmet le dossier à la CADA.

1 *Cf.* 23e rapport d'activité 2003, p. 134 à 137.

b) La médecine libérale

La CNIL a eu à instruire, en 2003, des plaintes émanant de patients qui, ayant été suivis par des praticiens d'exercice libéral, avaient exercé sans succès leur droit d'accès auprès de ces praticiens.

Ainsi, M^me^ M. a demandé au directeur de la clinique où elle a subi deux interventions chirurgicales son dossier médical constitué par le chirurgien qui l'a opérée. Ses demandes réitérées demeurant vaines, elle saisit la CNIL.

M^me^ C., quant à elle, s'est adressée au praticien qui l'avait opérée, mais aussi au Conseil départemental de l'ordre où il est inscrit, afin d'obtenir une copie de son dossier médical. Trois mois après sa première demande elle n'a reçu aucune réponse et saisit la CNIL.

Tant dans le cas de M^me^ M. que dans celui de M^me^ C., la Commission a dû s'adresser aux praticiens concernés pour que les requérants puissent obtenir la communication de leur dossier médical.

La loi du 4 mars 2002 a « bousculé » les habitudes des professionnels de santé, puisque désormais un patient n'a, sauf exceptions particulières, plus à demander l'intervention d'un médecin pour accéder aux données de santé le concernant. Ce principe de la maîtrise de ses données personnelles par le patient est un « défi » pour les professionnels de santé qui doivent désormais accéder directement à leurs demandes.

2. LES PROGRÈS DANS L'INFORMATION DES MALADES DU CANCER

Vingt ans après l'étude menée au début des années 1980 sur les registres du cancer ayant notamment abouti à la recommandation du 19 février 1985 relative aux traitements automatisés d'informations médicales nominatives, utilisés à des fins de recherche médicale, la Commission a souhaité procéder à une nouvelle étude des règles de fonctionnement des registres, en particulier s'agissant des mesures de confidentialité et des modalités d'information des personnes concernées.

La possibilité désormais reconnue par la loi d'accéder directement à ses données médicales et la volonté des patients d'être davantage associés aux traitements médicaux — évolution que la CNIL a pu mesurer depuis plusieurs années — [1], modifient la situation qui prévalait lors de la constitution des fichiers des registres du cancer. Alors que la loi impose une information individuelle des personnes dont les données sont transmises aux registres, force est de constater qu'en pratique, celle-ci n'est pas toujours réalisée. La CNIL a souhaité en procédant à un « état des lieux » de la situation des registres du cancer, en particulier dans le domaine de l'information, à la fois rappeler le respect de la loi et recommander les moyens les plus appropriés pour y parvenir.

1 *Cf.* 21^e^ et 22^e^ rapports annuels de la CNIL.

Dans un premier temps, la Commission a procédé à deux missions de vérification sur place auprès du registre des tumeurs digestives du Calvados à Caen et du registre général du cancer de l'Isère à Grenoble en février et mars 2003. Puis, en concertation avec l'association FRANCIM, réseau français des registres du cancer elle a diffusé au mois d'août 2003 auprès de l'ensemble des responsables des registres du cancer un questionnaire sur la sécurité et l'information afin d'obtenir un « état des lieux » de la situation des registres et d'adapter en conséquence ses éventuelles recommandations notamment en matière de sécurité. Des réunions de concertation se sont également tenues avec les représentants de la profession d'anatomo-cyto-pathologistes et du Conseil national de l'ordre des médecins. [1]

Ces différents travaux ont permis, en mesurant les évolutions intervenues depuis vingt ans d'adopter une nouvelle recommandation relative aux traitements de données à caractère personnel mis en œuvre par les registres du cancer.

a) Les registres du cancer : état des lieux

Les registres du cancer permettent de recenser, dans une zone géographique déterminée, les cas de cancer à partir de données nominatives transmises volontairement à l'organisme de recherche par les professionnels de santé concernés. Les fichiers épidémiologiques ainsi constitués doivent permettre de connaître avec précision le nombre, l'incidence et l'étiologie des cancers dans une population donnée et d'envisager le cas échéant des actions générales de dépistage ou de prévention. C'est à partir d'estimations sur l'incidence du cancer dans les départements disposant d'un registre et de l'analyse de la mortalité du cancer au niveau national qu'il est ainsi possible d'extrapoler à la France entière et aux départements ne disposant pas de registres, des politiques adaptées en matière de soins et de prévention.

Actuellement, vingt et un registres ont été qualifiés par le Comité national des registres [2]. Sur ce nombre, treize sont des registres généraux du cancer, les autres étant spécialisés dans des cancers spécifiques (tumeurs digestives, cancers de la thyroïde, hémopathies malignes, tumeurs solides de l'enfant). Aujourd'hui, on considère que les registres du cancer couvrent 13 % de l'ensemble de la population française. La volonté du Gouvernement affirmée dans le Plan cancer en mars 2003 est de porter cette couverture à 15 %.

Les sources d'alimentation des registres du cancer sont de plus en plus variées et permettent ainsi, par un travail de recoupement de l'ensemble des informations collectées, de sélectionner les pathologies qui relèvent de l'enregistrement.

1 Le rapport du CNOM sur le recueil des données par les registres du cancer et la situation au regard de la loi informatique et libertés a été adopté lors de la session de décembre 2003.

2 Aux termes de l'arrêté du 6 novembre 1995 relatif au Comité national des registres (CNR), ce dernier rend un avis d'opportunité au vu des priorités nationales de santé publique et compte tenu des registres déjà existants, sur la création ou le maintien d'un registre et atteste de la qualification au vu des avis rendus par le comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé et de la CNIL. La qualification conditionne l'accès à un financement national. Dix autres registres ont également été qualifiés mais ne concernent pas des cancers (cardiopathies ischémiques, malformations congénitales, accidents vasculaires cérébraux, victimes corporelles d'accidents de la circulation routière…).

Le rôle et la place des médecins anatomo-cyto-pathologistes dans le fonctionnement des registres du cancer sont essentiels et tous les registres du cancer interrogés font appel à leurs données. Ce sont eux qui, après biopsie, confirment la réalité d'une tumeur de nature cancéreuse. Les dossiers médicaux détenus par les médecins de ville et par les établissements de soins constituent l'autre source principale d'alimentation des registres du cancer, le recueil des données s'effectuant par des enquêtes sur place, réalisées par le personnel des registres. Dans la moitié des cas, les données sont également transmises par disquette ou Cédérom.

La nécessité pour les registres du cancer de disposer de données exhaustives sur les cas de cancer dans une zone déterminée et de suivre ces cas les conduit à solliciter les services médicaux des caisses d'assurance maladie afin d'obtenir la liste des personnes bénéficiant pour une affection de nature cancéreuse comprise dans la liste des affections de longue durée (ALD 30) d'une prise en charge à 100 %. Ils sollicitent également de la part des médecins responsables des départements d'information médicale la communication d'informations issues du programme de médicalisation des systèmes d'information (PMSI).

Par ailleurs, le suivi des cas enregistrés dans les bases de données des registres du cancer nécessite de mener des études de survie afin de connaître le statut vital de la personne. La plupart des registres obtiennent aujourd'hui cette information en interrogeant les communes de naissance, ce qui est très lourd à gérer. À cet égard, il doit être rappelé que les organismes de recherche peuvent obtenir auprès de l'INSEE des informations relatives au décès des personnes inscrites au Répertoire national des personnes physiques, après autorisation de la CNIL [1].

b) Comment assurer l'information individuelle ?

Il convient de rappeler qu'aux termes de l'article 40-5 de la loi du 6 janvier 1978, les personnes dont les données sont transmises aux registres du cancer doivent être, avant le début du traitement de ces données, individuellement informées de la nature des informations transmises, de la finalité du traitement des données, des personnes physiques ou morales destinataires des données et des modalités d'exercice du droit d'accès, de rectification et de leur droit d'opposition.

En matière d'information des personnes concernées la situation n'apparaît pas actuellement très satisfaisante. Une minorité de registres déclare procéder à une information individuelle, c'est-à-dire à la remise au malade, lors d'un entretien personnalisé d'une note l'informant de l'objet du recueil de données, des modalités de fonctionnement du registre, des destinataires des données et des droits ouverts au titre de la loi « informatique et libertés ». En revanche, dans la majorité des cas, les registres indiquent avoir pris les dispositions nécessaires pour que le public accueilli dans les établissements de soins soit informé de l'activité et des modalités de fonctionnement du registre, notamment en procédant à des publications régulières dans la

1 Conformément aux dispositions du décret n° 98-37 du 16 janvier 1998 autorisant l'accès aux données relatives au décès des personnes inscrites au Répertoire national d'identification des personnes physiques dans le cadre des recherches dans le domaine de la santé.

presse locale. À cet effet, les registres diffusent le modèle de note d'information précité, à charge pour les médecins exerçant dans les établissements de soins de diffuser effectivement l'information.

Or, le décret du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 définit des obligations particulières dans ce domaine à la charge des responsables de traitement, en l'occurrence les registres du cancer. Ainsi, le dossier de demande d'autorisation présenté par le registre doit comporter les mesures envisagées pour communiquer individuellement aux personnes concernées par le traitement les informations figurant au premier alinéa de l'article 40-5 de la loi. L'article 25-20 III du décret précise que, dans le cas où les données nominatives ont été initialement recueillies pour un autre objet que le traitement automatisé envisagé — ce qui est le cas des registres du cancer — l'établissement ou le professionnel de santé détenteur des données informe par écrit les personnes concernées.

La recommandation adoptée par la CNIL le 27 novembre 2003 [1] rappelle ainsi que les transmissions de données nominatives nécessaires aux registres du cancer pour disposer, dans le cadre de leur système d'information, de données fiables et exhaustives sont autorisées par les dispositions des articles 40-1 et suivants de la loi du 6 janvier 1978 et que dès lors, les médecins qui participent au diagnostic et à la prise en charge des patients peuvent transmettre des informations nominatives sans violer le secret professionnel tel que défini par l'article 226-13 du Code pénal. Dès lors, ce même secret professionnel ne peut être invoqué par des professionnels de santé pour refuser de transmettre des données aux registres. Il apparaît toutefois essentiel que les registres du cancer informent régulièrement leurs correspondants des résultats obtenus. C'est là d'ailleurs un des aspects d'une surveillance épidémiologique efficace.

La question des modalités pratiques de l'information individuelle des patients est à l'origine des difficultés rencontrées par certains registres du cancer, confrontés au refus de certains anatomo-pathologistes de transmettre au registre des données nominatives sur leurs patients au motif que, n'étant jamais en contact direct avec ceux-ci, ils ne sont pas assurés de l'effectivité de cette information individuelle et considèrent ainsi que la loi n'étant pas respectée, leur responsabilité pourrait dès lors être engagée.

La Commission a d'ailleurs attiré l'attention du ministre de la Santé et du président du Conseil national de l'ordre des médecins sur cette situation de blocage préjudiciable aux registres.

Aux termes d'échanges fructueux avec des responsables de registres, des représentants des anatomo-cyto-pathologistes et du Conseil national de l'ordre des médecins, la Commission a proposé dans sa recommandation de prendre avant tout en compte l'intérêt du patient et de consacrer le rôle central du médecin en contact direct avec le patient pour l'information.

1 Délibération n° 03-053 du 27 novembre 2003.

Ainsi, la Commission considère que les données transmises aux registres du cancer ayant été, à l'origine, collectées pour un autre objet que celui poursuivi par la surveillance épidémiologique et, le personnel des registres de cancer n'étant jamais en contact avec le patient, seul le médecin, responsable de la prise en charge thérapeutique, en contact direct avec le patient est en mesure de procéder, au moment, qu'il estimera le plus opportun et en conscience à cette information. [1]

Dès lors il convient de prendre en compte la situation particulière d'un patient à qui il vient d'être annoncé un diagnostic de cancer. Même si les traitements aujourd'hui proposés sont plus performants, l'annonce du diagnostic de cancer constitue toujours un traumatisme majeur. Les professionnels de santé sont eux-mêmes formés à ces consultations « d'annonce » qui doivent tout à la fois informer le patient de sa maladie, lui exposer les différentes alternatives thérapeutiques proposées, les risques thérapeutiques que ces traitements comportent et les éléments de pronostic.

L'information sur l'activité des registres ne peut évidemment pas être imposée dès ce stade. Il appartient au médecin chargé de la prise en charge thérapeutique de déterminer le moment adéquat pour expliquer au patient que ses données sont susceptibles, sauf opposition de sa part, d'être transmises à un registre du cancer et lui faire comprendre l'intérêt de santé publique que revêt cette transmission.

La possibilité désormais reconnue au médecin par la loi du 4 mars 2002 sur les droits des malades de recommander la présence d'une tierce personne — qui peut ne pas appartenir à la famille — pour accompagner le patient lors de la consultation de certaines informations délicates permet également de procéder à cette information sur les registres du cancer.

La note d'information individuelle remise à l'appui de cette explication par le médecin doit indiquer précisément le nom du registre du cancer ainsi que son adresse. Elle doit comporter l'indication précise de la finalité du système d'information crée et géré par le registre du cancer. La nature des informations transmises aux registres doit être précisée, de même que l'assurance que ces données seront, conformément à la loi du 6 janvier 1978, transmises à des personnes nommément désignées et astreintes au secret professionnel.

Les modalités d'exercice du droit d'accès de la personne concernée doivent être décrites, avec l'indication des personnes auprès desquelles peut être formulée la demande de l'intéressé. Le droit d'opposition, reconnu à toute personne dont des données nominatives sont susceptibles d'être transmises aux registres du cancer doit pouvoir s'exercer auprès du registre et de tout professionnel de santé sollicité pour transmettre des données au registre. L'indication selon laquelle l'opposition de la personne et, le cas échéant, sa demande de suppression des données, aura été prise en compte, doit être précisée.

1 Il serait ainsi souhaitable de modifier en ce sens l'article 25-20 III du décret n° 78-774 du 17 juillet 1978 de façon à indiquer que, c'est l'établissement ou le professionnel de santé en contact direct avec le patient et effectivement chargé de la prise en charge thérapeutique qui procède à l'information exigée par la loi.

Il est donc recommandé aux registres du cancer de mettre en place une procédure de rappel systématique aux professionnels de santé de la nécessité d'informer individuellement les personnes tout en leur laissant le choix de déterminer le moment qu'ils estimeront en conscience le plus opportun pour le patient. À cet effet, les registres pourraient utilement organiser avec l'ensemble des professionnels de santé concernés des réunions permettant de définir localement les modalités pratiques de cette information. En outre, dans les régions où sont implantés des registres du cancer et des réseaux de soins en cancérologie, le réseau de soins constitue un relais supplémentaire d'information.

IV. LES DONNÉES LIÉES AU MONDE DU TRAVAIL

L'année 2003 a été marquée, dans le secteur du travail, par un nombre important de plaintes de salariés et de personnes recherchant un emploi rencontrant des difficultés dans l'exercice de leur droit d'accès auprès de leurs employeurs ou d'un cabinet de recrutement.

D'autres plaintes témoignent du manque d'information des salariés lorsque leur employeur met en œuvre un système de contrôle et de surveillance (internet, messagerie, vidéosurveillance, autocommutateurs, badgeuses...).

En règle générale, on peut observer que, hormis les cas où elle est saisie par une organisation syndicale, les plaintes reçues par la Commission dans le secteur du travail s'inscrivent souvent dans le cadre d'un litige déjà existant entre le requérant et son employeur ou son employeur potentiel (rupture du contrat de travail ou procédure de licenciement en cours, candidat à un emploi qui n'a pas obtenu le poste). Cette particularité, qui se retrouve dans d'autres secteurs comme, par exemple, celui du logement, s'explique notamment par le fait que, tant qu'elle se trouve dans une relation de subordination ou en situation de demande, la personne concernée par le fichier hésite à saisir la CNIL craignant qu'une telle démarche ait des conséquences dans sa vie professionnelle et ses relations avec son employeur.

Dès lors, il convient d'emblée de souligner que l'instruction de ces plaintes, alors qu'un contexte conflictuel entre le requérant et l'organisme mis en cause existe déjà lorsque la CNIL est saisie, apportera difficilement une réponse de nature à satisfaire pleinement le plaignant dont les principales difficultés relèvent plus du droit du travail que de la protection des données personnelles. Très concrètement, si l'intervention de la Commission permettra la régularisation d'une situation souvent irrégulière au regard des règles protectrices des données personnelles, elle n'aura pas pour effet, en revanche, de stopper une procédure de licenciement ou d'interférer dans l'octroi d'un emploi.

A. L'exercice du droit d'accès dans le secteur du travail

Jusqu'à présent, la CNIL était généralement saisie par des personnes qui ignoraient qu'elles disposaient d'un droit d'accès et de rectification aux données les concernant enregistrées dans un fichier (articles 34, 35 et 45 de la loi du 6 janvier 1978) et, *a fortiori*, les modalités selon lesquelles s'exerce ce droit. On constate désormais que, lorsqu'un salarié saisit la CNIL, il a le plus souvent, déjà exercé son droit d'accès. Ainsi, s'il sollicite aujourd'hui l'intervention de la Commission c'est parce qu'il n'a pas reçu de réponse à sa demande ou qu'il estime que la réponse qu'il a reçue n'est pas satisfaisante.

1. L'ACCÈS DES SALARIÉS AUX DONNÉES PERSONNELLES DÉTENUES PAR LES EMPLOYEURS

La plainte de M. X. illustre les difficultés auxquelles peuvent se heurter les salariés en matière de droit d'accès aux dossiers du personnel.

Après avoir tenté, à plusieurs reprises et sans succès, d'obtenir une copie des informations le concernant enregistrées dans les fichiers manuels ou informatisés du service du personnel de son employeur, M. X. saisit la CNIL. La plainte de M. X. ne constitue pas un cas isolé. La Commission est très régulièrement saisie par de nombreux salariés de faits similaires.

Dans de pareils cas, la Commission intervient auprès des employeurs, afin que les requérants obtiennent, dans les meilleurs délais (articles 34, 35 et 45 de la loi du 6 janvier 1978), une copie, en langage clair, de l'ensemble des informations les concernant figurant dans les fichiers des organismes mis en cause.

Afin d'aider les plaignants dans leur démarche, une action pédagogique est également menée par la Commission qui adresse aux requérants des documents pratiques (lettres-type, par exemple) leur rappelant les droits qu'ils tiennent de la loi du 6 janvier 1978.

Ces documents étant également disponibles en ligne sur le site de la CNIL, les requérants — s'ils disposent des moyens nécessaires — sont invités à s'y connecter. Ce moyen d'information est notamment très apprécié des représentants du personnel.

2. L'ACCÈS DES DEMANDEURS D'EMPLOI AUX DONNÉES DÉTENUES PAR UN CABINET DE RECRUTEMENT

Le cas de M^{me} A., qui recherche un emploi, est très illustratif des difficultés auxquelles peuvent être confrontés les demandeurs d'emploi quand ils veulent avoir accès aux données détenues par un cabinet de recrutement.

M^{me} A. s'est adressée à un cabinet de recrutement qui, pour constituer son dossier de candidature, lui fait remplir un formulaire et passer différents tests

(psychotechniques, graphologiques...). M^me^ A. doit, par ailleurs, se prêter à un entretien d'évaluation.

M^me^ A., qui n'a pas été retenue pour le poste, demande l'intégralité des informations la concernant, détenues par ce cabinet de recrutement. Elle souhaite, en particulier, connaître les résultats des tests et du bilan qu'elle a passé. Le cabinet de recrutement lui communique les informations contenues dans sa « fiche candidat », mais lui précise qu'il n'est pas en mesure de lui adresser la copie des résultats de ses tests et de son entretien d'évaluation. Il estime que ces éléments sont confidentiels et restent la propriété du cabinet.

Étonnée de cette réponse, M^me^ A. saisit la CNIL.

L'exercice du droit d'accès dans ce domaine peut s'avérer d'application délicate. La CNIL a adopté le 21 mars 2002 une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opération de recrutement [1] qui rappelle clairement qu'« en application des articles 34 et suivants, 45 de la loi du 6 janvier 1978, et L. 121-7 du Code du travail, *» tout candidat peut obtenir communication des informations le concernant «* , et recommande que *» tout candidat soit clairement informé des modalités d'exercice du droit d'accès et puisse obtenir sur sa demande toutes les informations le concernant y compris les résultats des analyses et des tests ou évaluations professionnelles éventuellement pratiqués «* .

S'agissant des modalités selon lesquelles une telle communication doit être effectuée la Commission, dans cette recommandation, a estimé nécessaire d'opérer une distinction selon que la communication se rapporte aux données contenues dans la fiche du candidat ou aux résultats des tests et autres évaluations. La CNIL a en effet considéré que les données contenues dans la fiche du candidat devaient être communiquées à l'intéressé par écrit, tandis que les résultats aux tests ou autres évaluations auxquels le candidat a été soumis devaient être communiqués *« par tout moyen approprié au regard de la nature de l'outil utilisé »*.

Il est en effet apparu que de nombreux tests ou outils d'évaluation ne débouchaient pas sur des résultats aisément communicables sans interprétation (un entretien passé avec un psychologue, par exemple) et sans explication au regard du poste à pourvoir et, qu'en outre, aucun texte ne prévoyait une obligation de communiquer par écrit les résultats des tests. Dès lors, les personnes chargées du recrutement doivent informer préalablement, par écrit, individuellement ou collectivement, les candidats des méthodes et techniques qui seront utilisées pour les évaluer. Dans l'hypothèse où certains résultats ne pourraient être communiqués que sous forme orale en raison des méthodes utilisées pour les mettre en œuvre, le consentement exprès de ces personnes doit être recueilli.

La Commission, saisie du refus de communication sous forme écrite des résultats aux tests passés par les personnes, s'assure que les modalités d'information ont été respectées par le cabinet de recrutement et que la nature des outils utilisés justifie que la communication des résultats soit effectuée oralement.

1 Rapport annuel 2002 p. 297.

S'agissant de la plainte de M^me A., ces règles ont été rappelées par la Commission au cabinet de recrutement auquel elle s'était adressée. L'intervention de la Commission a finalement permis à M^me A. d'obtenir la copie des résultats de ses tests (pour certains, dans la mesure où la nature des outils utilisés le justifiait, sous forme orale), ainsi que la copie du compte rendu de son entretien d'évaluation.

B. Le défaut d'information lié à la mise en place de dispositifs de contrôle et de surveillance

Les dispositifs de contrôle et de surveillance sur les lieux de travail demeurent un sujet de préoccupation des salariés qui saisissent régulièrement la CNIL, lors de la mise en œuvre d'un tel dispositif (badgeuse, autocommutateur, internet, messagerie électronique, vidéosurveillance…) au sein de leur entreprise.

En effet, que ce soit à partir des connexions à internet, de l'utilisation de la messagerie électronique, du contrôle d'accès par badges…, les salariés laissent immanquablement des « traces » et ne sont pas toujours avertis des conséquences éventuelles qui peuvent en découler. C'est pourquoi les salariés interrogent la Commission afin de savoir dans quelles conditions ces dispositifs peuvent être régulièrement mis en œuvre par leur employeur.

M. H. est employé dans une PME et utilise internet, dans le cadre de ses fonctions, environ quatre heures par jour. M. H. saisit la CNIL car son employeur lui reproche une utilisation abusive d'internet à des fins personnelles. Or, l'employeur de M. H. n'a ni déclaré la mise en place du traçage des accès à Internet, ni informé ses salariés de la mise en place de ce dispositif.

M^me S., membre du comité d'entreprise de son entreprise, souhaite quant à elle, attirer l'attention de la Commission sur la mise en œuvre, par son employeur, d'un système de contrôle par badges des salariés de l'entreprise, sans information préalable des salariés et des membres du CE.

Ou encore, M. T. appelle l'attention de la CNIL sur l'installation par son employeur d'une dizaine de « webcams » dans l'entreprise, sans en avoir préalablement informé les salariés. L'une d'elles est même dirigée sur le système d'accès par badges.

Dans tous les cas, la Commission rappelle à l'employeur les règles applicables à la mise en œuvre de tels traitements dans l'entreprise : information préalable des salariés (article 27 de la loi du 6 janvier 1978 — L. 121-8 Code du travail), consultation et information du comité d'entreprise (L. 432-2-1 du Code du travail) et respect du principe de proportionnalité (article L. 120-2 Code du travail), obligation de déclarer tout traitement automatisé d'informations nominatives (article 16 loi du 6 janvier 1978).

Il convient de souligner, s'agissant de la question relative à l'appréciation de la proportionnalité de la mise en œuvre de ces dispositions, qui relève en dernier ressort des juridictions compétentes, que cette notion est codifiée par le Code du travail sous l'article L. 120-2 qui dispose que : *« Nul ne peut apporter aux droits des*

personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

La Commission rappelle régulièrement aux salariés qui la saisissent que l'ordinateur, mis à la disposition du salarié ou d'un agent public, est la propriété de l'entreprise ou de l'administration. Il peut être protégé par un mot de passe et un « login » mais il s'agit d'une mesure de sécurité qui n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé et c'est seulement, à titre subsidiaire, qu'il peut comporter des informations relevant de l'intimité de la vie privée.

Mais la notion de proportionnalité, appliquée au traitement des données personnelles à des fins autres que techniques, signifie également que l'information préalable des salariés ou des agents publics ne peut, en soi, permettre à une entreprise ou une administration d'employer tous les modes de surveillance et de contrôle. Ces éléments doivent également être régulièrement rappelés aux employeurs par la Commission.

LES DÉLIBÉRATIONS 2003 PAR SECTEUR D'ACTIVITÉ

Administration électronique

Délibération n° 03-054 du 27 novembre 2003 portant avis sur les dispositions relatives au développement de l'administration électronique de l'avant-projet de loi habilitant le Gouvernement à simplifier le droit par voie d'ordonnances

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis des dispositions du titre relatif au développement de l'administration électronique, contenues dans l'avant-projet de loi habilitant le Gouvernement à simplifier le droit par voie d'ordonnances ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret nº 78-774 du 17 juillet 1978 ;

Après avoir entendu Monsieur Marcel Pinet, commissaire, en son rapport, et Madame Catherine Pozzo di Borgo, commissaire-adjoint du Gouvernement, en ses observations ;

Émet l'avis suivant :

Les dispositions figurant sous le titre « développement de l'administration électronique » ont pour objet de définir le cadre juridique adéquat pour assurer le développement de l'administration électronique et améliorer ainsi le service public au bénéfice de l'usager.

L'article premier autorise ainsi le Gouvernement à fixer par voie d'ordonnance les règles nécessaires pour, respectivement :
– assurer la sécurité et la fiabilité des informations échangées entre les usagers et l'administration ;
– permettre aux usagers d'effectuer leurs démarches administratives par voie électronique dès lors que de tels services sont disponibles ;
– offrir la possibilité pour les administrations d'effectuer tout ou partie des procédures de contrôle dont elles ont la charge par voie électronique ;
– mettre à disposition des usagers un dispositif leur permettant de stocker sous forme électronique les documents et données les concernant pouvant être transmis aux destinataires de leur choix, en particulier dans le cadre de démarches administratives ;
– offrir aux usagers la possibilité de déclarer, en une seule opération, leur changement d'adresse aux autorités administratives, et le cas échéant à des partenaires privés.

Cet article précise enfin son champ d'application en ce qui concerne tant les acteurs intéressés que les traitements de données visés.

L'article 2 autorise le Gouvernement à fixer par voie d'ordonnance les conditions de nature à permettre la signature électronique des actes administratifs.

L'article 3 autorise le Gouvernement à prendre par voie d'ordonnance, dans le respect des principes posés en matière de protection des libertés individuelles et de la vie privée, les mesures de nature à permettre l'accès et la diffusion des données publiques produites ou collectées par les administrations de l'État, les collectivités ter-

ritoriales, les établissements publics à caractère administratif, les organismes de Sécurité sociale et les autres organismes chargés de la gestion d'un service public administratif.

Enfin, l'article 4, d'application directe, vise à ajouter à l'article 21 de la loi nº 82-610 du 15 juillet 1982 un second alinéa afin de permettre la constitution, au niveau national comme au niveau local, de groupements d'intérêt public pour exercer pendant une durée limitée une activité liée au développement technologique ou gérer des équipements d'intérêt commun nécessaires à ces activités.

La Commission considère qu'en l'état, l'ensemble de ces dispositions qui énonce de simples orientations de caractère général n'appelle pas d'objection de principe au regard des principes de protection des données à caractère personnel mais qu'elle devra être consultée sur les dispositions des ordonnances qui préciseront les mesures envisagées et qui seront susceptibles d'intéresser la protection des droits et libertés des personnes à l'égard des traitements de données à caractère personnel.

Il ne lui appartient pas d'apprécier si l'encadrement juridique ainsi défini par le projet de loi est suffisant au regard des exigences de la jurisprudence du Conseil constitutionnel ni si les mesures envisagées, telles qu'elles ressortent de l'exposé des motifs, sont de nature législative ou réglementaire. Elle estime cependant devoir formuler des observations sur les points suivants.

Sur la sécurité et la fiabilité des échanges de données entre usagers et administrations

La Commission suggère que le texte précise que les informations échangées le sont « par voie électronique ».

La Commission approuve l'orientation prise par le Gouvernement de permettre aux administrations de disposer de systèmes d'information dont la sécurité réponde aux exigences posées en particulier par l'article 17 de la directive européenne nº 95/46/CE du 24 octobre 1995 et par l'article 29 de la loi du 6 janvier 1978.

La Commission estime que, dans la mesure où cette disposition a pour objet de renforcer la sécurité non seulement des téléprocédures effectuées par les usagers mais également des échanges d'informations entre administrations, il y a lieu de transférer dans un article spécifique le dernier paragraphe de l'article premier qui prévoit que *« les dispositions du présent article s'appliquent également aux échanges entre autorités administratives »*.

Sur la possibilité pour les administrations, prévue par le 3° de l'article 1er « d'effectuer tout ou partie des procédures de contrôle dont elles ont la charge par voie électronique »

La Commission estime que, dans la mesure où le 3° de l'article 1er a uniquement pour objet de permettre aux autorités administratives, dans le cadre des procédures de contrôle dont elles ont la charge, d'obtenir des usagers concernés, par voie électronique, les informations requises sur demande préalable et également d'accomplir par voie électronique des actes de procédure liés à l'exercice des contrôles, la rédaction de cette disposition devrait être complétée de façon à délimiter son champ d'application.

La Commission considère également que les dispositions de l'ordonnance devraient indiquer précisément les procédures de contrôle concernées et fixer les modalités d'interrogation et de transmission des informations.

Sur la mise à disposition de l'usager d'un dispositif de stockage des données

La Commission relève la proposition de doter l'usager d'un dispositif de stockage de données ou de documents dont il serait le gestionnaire.

La Commission estime toutefois qu'au regard des principes de protection des données à caractère personnel, l'institution d'un tel dispositif suppose de définir précisément ses conditions exactes d'accès et d'utilisation par l'usager et par l'administration, les contraintes de sécurité, s'agissant en particulier de la possibilité pour l'usager de chiffrer les informations et de déterminer la validité juridique des informations y figurant ainsi que les responsabilités respectives de l'usager, de l'administration destinataire et de l'hébergeur, au regard de l'enregistrement des données, de leur conservation et de leur transmission.

La Commission estime dès lors que la référence faite au 4° de l'article premier à la seule responsabilité des usagers mérite d'être complétée et précisée.

La Commission prend acte de ce que, aux termes de l'exposé des motifs, la liste des données susceptibles d'être conservées dans ce dispositif de stockage sera fixée par décret en Conseil d'État pris après avis de la CNIL.

Elle relève également que selon l'exposé des motifs, les dispositifs de stockage seraient gérés par des prestataires privés qui devraient être agréés selon des modalités analogues à celles prévues par l'article L. 1111-8 du Code de la santé publique pour l'hébergement de données personnelles de santé.

Sur le service de changement d'adresse

La Commission estime que les objectifs de simplification poursuivis par la création du service de changement d'adresse sont légitimes dès lors d'une part que l'inscription à ce service et la décision de transmettre à telle autorité administrative ou tel partenaire privé les informations relatives au changement d'adresse relèvent de la seule volonté de l'usager et, d'autre part, que toutes garanties sont prises afin que ne soit pas constitué, à l'occasion de telles démarches, un fichier national de domiciliation. Elle observe en outre que les termes de *« partenaires privés »* pourraient être remplacés par une expression mieux adaptée à l'objet de la disposition énoncée.

La Commission prend acte des assurances qui lui ont été données qu'il n'est pas envisagé de recourir au fichier des changements d'adresse de La Poste.

Elle estime également que pour assurer le respect des règles de protection des données à caractère personnel, il y aura lieu de prévoir, dans l'ordonnance, l'obligation pour le service assurant la gestion de ce service de n'enregistrer que les données d'identification et d'adresse strictement nécessaires pour assurer la transmission de celles-ci aux seuls destinataires désignés par l'usager et habilités à connaître de ces informations, au titre de leurs missions, et de ne conserver ces données que le temps strictement nécessaire pour permettre leur bonne réception technique par les destinataires précités et l'envoi par leurs soins d'un accusé de réception.

Sur la signature électronique des actes administratifs

La Commission estime que dans la mesure où, aux termes de l'exposé des motifs, l'article 2 a non seulement pour objet de permettre la signature électronique des actes administratifs mais également de déterminer les effets juridiques, en particulières vis-à-vis des usagers, des accusés de réception émis sous forme électronique par l'administration, il y aurait lieu de compléter en ce sens cet article.

Sur l'accès et la diffusion des données publiques

Aux termes de l'exposé des motifs, cet article permettra de transposer la directive concernant la réutilisation et l'exploitation commerciale des documents du secteur public, en cours d'adoption. Le champ de l'article 3 est cependant plus vaste que la seule exploitation commerciale et englobe notamment la mise à disposition par les organismes visés des données publiques diffusables.

La Commission rappelle, ainsi qu'elle l'a précisé notamment dans son avis du 3 mai 2001 sur le projet de loi sur la société de l'information et ainsi que l'a souligné le groupe de travail de l'article 29 de la directive européenne n° 95/46/CE du 24 octobre 1995 dans son avis du 3 mai 1999, que les règles de protection des données à caractère personnel s'appliquent aux données rendues publiques, s'agissant tout particulièrement des principes de finalité et de légitimité et du droit de toute personne de s'opposer à la diffusion des données la concernant.

La Commission observe à cet égard que seul l'article 1er fait référence à la législation relative à l'informatique, aux fichiers et aux libertés et estime en conséquence que l'article 3 devrait être complété également en ce sens.

Affaires étrangères

Délibération n° 03-028 du 27 mai 2003 portant avis sur le projet d'arrêté du ministre des Affaires étrangères modifiant l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère des Affaires étrangères d'un projet d'arrêté modifiant l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires ;

Vu la délibération nº 01-019 du 15 mai 2001 relative à un projet d'arrêté portant création d'un traitement informatique de délivrance des visas dans les postes diplomatiques et consulaires mis en œuvre par le ministère des Affaires étrangères ;

Vu le projet d'arrêté du ministre des Affaires étrangères ;

Après avoir entendu Monsieur François Giquel, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère des Affaires étrangères a saisi la Commission d'un projet d'arrêté modifiant l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires appelé Réseau Mondial Visas 2 (RMV 2).

Cette modification vise à ajouter à l'article 5 de cet arrêté le ministère de la Défense au titre des destinataires des informations traitées.

La Commission prend acte que la mise en place de cet accès ne conduira pas le ministère de la Défense à exploiter les données auxquelles il aura accès par un traitement spécifique ou associé à ses propres fichiers informatiques.

Les communications générées par cet accès seront protégées contre toute intrusion et l'accès au poste permettant cet accès, relié au réseau interne du ministère des Affaires étrangères, bénéficiera des mêmes procédures de protection que celles déjà mises en œuvre s'agissant du RMV 2.

Émet un avis favorable au projet d'arrêté modifiant l'arrêté du 22 août 2001 du ministre des Affaires étrangères portant création d'un traitement informatisé

d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires ayant pour objet d'ajouter le ministère de la Défense aux destinataires des informations nominatives enregistrées et traitées dans le RMV 2.

Délibération n° 03-066 du 18 décembre 2003 portant avis sur un projet de décret du ministre des Affaires étrangères relatif à l'inscription au registre des Français établis hors de France

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministre des Affaires étrangères d'un projet de décret relatif à l'inscription au registre des Français établis hors de France ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention de Vienne du 24 avril 1963 sur les relations consulaires ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le Code civil, notamment ses articles 30, 103, 104 et 105 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 78-753 du 17 juillet 1978 modifiée portant diverses mesures d'améliorations des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal ;

Vu le décret n° 55-1397 du 22 octobre 1955 modifié instituant la carte nationale d'identité ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le décret n° 79-433 du 1er juin 1979 relatif aux pouvoirs des ambassadeurs et à l'organisation des services de l'État à l'étranger, notamment son article 1er ;

Vu le décret n° 99-176 du 9 mars 1999 relatif à l'immatriculation consulaire dans les postes diplomatiques et consulaires ;

Vu le décret n° 2000-1277 du 26 décembre 2000 portant simplification de formalités administratives et suppression de la fiche d'état civil ;

Vu le décret n° 2001-185 du 26 février 2001 relatif aux conditions de délivrance et de renouvellement des passeports ;

Vu le décret n° 2002-701 du 29 avril 2002 relatif à la protection des citoyens de l'Union européenne par les représentations diplomatiques et consulaires de la France ;

Vu le projet de décret du ministre des Affaires étrangères ;

Après avoir entendu Monsieur François Giquel, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministre des Affaires étrangères a saisi la Commission d'un projet de décret relatif à l'inscription au registre des Français établis hors de France. Ce projet de décret abroge le décret du 9 mars 1999 relatif à l'immatriculation consulaire dans les postes diplomatiques et consulaires.

Conformément à l'article 2 du projet de décret, cette procédure est destinée à améliorer la connaissance que le chef de poste consulaire a de la communauté de ressortissants français installés dans sa circonscription, à faciliter l'exercice de la protection consulaire et à permettre l'établissement et la mise à jour du plan de sécurité propre au poste.

Pour l'intéressé, la nouvelle procédure a pour objet de faciliter l'accomplissement de formalités administratives, de lui permettre d'accéder à certaines procédures ou prestations liées à sa résidence à l'étranger et, enfin, de recevoir des informations d'ordre général du poste consulaire dont il dépend.

La réforme envisagée a pour objet de faciliter et de simplifier l'accomplissement de cette démarche en permettant d'une part, de l'effectuer par différents moyens, et notamment par voie électronique, d'autre part, de l'effectuer, de façon automatique, à l'occasion de l'accomplissement au poste consulaire concerné, d'une autre formalité exigeant la justification de l'état civil, de la nationalité et de la résidence, telle que notamment la délivrance ou le renouvellement d'une carte nationale d'identité ou d'un passeport ou l'inscription sur les listes électorales.

Dans un même souci de simplification, l'article 14 du projet de décret prévoit que plusieurs registres peuvent être tenus conjointement par plusieurs chefs de poste consulaire, l'inscription au registre des Français installés hors de France pouvant alors permettre de s'inscrire, le cas échéant, dans un poste consulaire proche de sa résidence.

La Commission relève que l'objectif de simplification des démarches administratives qui est poursuivi est légitime et que les caractéristiques fondamentales de l'inscription consulaire, en particulier son caractère facultatif, ne sont pas modifiées.

Elle observe que le ministère des Affaires étrangères souhaite également, dans le cadre de cette réforme, attribuer à chaque Français inscrit au registre des Français établis hors de France un numéro d'identification personnel unique qui permettrait, à terme, à l'intéressé d'effectuer des formalités administratives à partir de son lieu de travail ou de son domicile. En outre, l'attribution de ce numéro faciliterait le transfert du dossier de l'intéressé en cas de changement de domicile dans une autre circonscription consulaire.

La Commission prend acte que, conformément à l'article 11 du projet de décret, la composition et les modalités d'utilisation de ce numéro seront définis par un arrêté du ministre des Affaires étrangères pris après avis de la CNIL.

La Commission estime qu'elle devrait être également consultée sur l'arrêté du ministre des Affaires étrangères, prévu en application de l'article 11 du projet de décret, qui définira les caractéristiques de la carte d'immatriculation consulaire.

La Commission prend acte que le projet de décret prévoit expressément qu'un relevé des informations recueillies est remis à l'intéressé à l'occasion de son inscription, ainsi que lors de chaque modification de l'enregistrement le concernant et impose au chef de poste concerné de prendre toute mesure pour garantir la confidentialité de la transmission, par le poste consulaire des informations aux intéressés.

La Commission relève que cette réforme doit se traduire par une refonte du système informatique de gestion consulaire du ministère des Affaires étrangères qui fera l'objet de dispositions réglementaires ultérieures qui lui seront soumises pour avis.

La Commission estime opportun, enfin, de préciser la rédaction du dernier alinéa de l'article 4 du projet de décret afin qu'il apparaisse sans ambiguïté que l'enregistrement, à l'occasion de l'inscription au registre d'un Français de l'étranger, des informations concernant son conjoint ou ses enfants mineurs de nationalité étrangère sera effectué à la demande de ce dernier.

Émet au bénéfice des observations qui précèdent, **un avis favorable** au projet de décret relatif à l'inscription au registre des Français établis hors de France abrogeant le décret du 9 mars 1999 relatif à l'immatriculation consulaire dans les postes diplomatiques et consulaires.

Banque et crédit

Délibération n° 03-018 du 24 avril 2003 portant avertissement à Fortis banque

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par un particulier inscrit, par Fortis banque, au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 modifié ;

Vu les articles L. 333-4 et suivants du Code de la consommation ;

Vu l'article L. 613-21 du Code monétaire et financier ;

Vu le règlement n° 90-05 du 11 avril 1990 du Comité de la réglementation bancaire, modifié, relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-29 du 6 mars 1990 portant avis sur le projet de règlement du Comité de la réglementation bancaire relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-72 du 29 mai 1990 portant avis sur la mise en œuvre, par la Banque de France, d'un traitement automatisé d'informations nominatives relatif à la gestion d'un fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 87-25 du 10 février 1987 fixant le règlement intérieur de la CNIL, et notamment son article 54 ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'instruction de la plainte dont a été saisie la CNIL a permis d'établir que le plaignant a été inscrit par Fortis banque au FICP le 31 août 2001, pour une durée de cinq ans.

Après plusieurs lettres de relance, Fortis banque a finalement indiqué à la CNIL que l'inscription de son client au FICP résultait du « débit de son compte courant » et lui a transmis un jugement du tribunal d'instance de Versailles du 26 août 1996 « relatant la chronologie des faits » sur lesquels cette inscription serait fondée.

Il ressort de ce jugement que le compte bancaire du plaignant a présenté un solde débiteur continu (découvert) de plus de quatre-vingt-dix jours pendant la période 1993-1994.

La CNIL a, le 9 avril 2003, adressé un courrier à Fortis banque lui demandant, d'une part, de procéder à la mainlevée de l'inscription du requérant au FICP et, d'autre part, de faire valoir ses observations sur ce dossier dans un délai de quinze jours, lui indiquant en outre que la Commission examinerait s'il convenait, en l'espèce, de faire application de l'article 21-4° de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Fortis banque a indiqué en réponse qu'elle procédait à la mainlevée de l'inscription de son client au FICP, précisant toutefois que cette inscription, effectuée le 31 août 2001 : *« En application de l'article 3 du règlement ° 90-05 du 11 avril 1990 avait pour objet, en conformité aux objectifs de la loi Neïertz, de prévenir tout risque de surendettement du débiteur et de prévenir les établissements de crédit du non respect par M. L. de ses obligations contractuelles à l'égard d'un établissement bancaire ».*

L'article 3 b) du règlement n ° 90-05 du 11 avril 1990 relatif au FICP prévoit que constitue un incident de paiement caractérisé justifiant une inscription au FICP *« pour un même crédit ne comportant pas d'échéance échelonnée, le défaut de paiement des sommes exigibles plus de 90 jours après la date de mise en demeure du débiteur d'avoir à régulariser sa situation, dès lors que le montant des sommes impayées est au moins égal à 500 euros (anciennement 3 000 francs) ».*

L'article 4 du règlement n ° 90-05 relatif au FICP prévoit que : *« Dès qu'un incident de paiement caractérisé est constaté, l'établissement de crédit informe le débiteur défaillant que l'incident sera déclaré à la Banque de France à l'issue d'un délai d'un mois à compter de la date d'envoi de cette information ».*

L'article 5 bis du règlement n ° 90-05 relatif au FICP prévoit que *« lorsqu'un incident caractérisé ayant affecté le remboursement d'un crédit donné est enregistré dans le fichier, il n'est procédé à aucune nouvelle déclaration au titre du même crédit en cas de survenance d'autres incidents ou de prononcé de la déchéance du terme ou d'engagement d'une procédure judiciaire ».*

En adoptant la loi n° 89-1010 du 31 décembre 1989, dite « loi Neïertz », qui a créé le fichier national des incidents de remboursement des crédits aux particuliers (FICP), le législateur a entendu mettre en place un dispositif de prévention et de traitement des situations de surendettement.

Le fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, constitue un instrument de lutte contre le surendettement des particuliers et qu'il n'a pas pour finalité la mise en commun entre les banques, les établissements de crédits et les établissements financiers de La Poste, d'informations relatives à leurs débiteurs, sauf dans les cas prévus par les dispositions du règlement n° 90-05 précité.

Dans le cas d'espèce, Fortis banque, en inscrivant son client au FICP le 31 août 2001, pour un incident de paiement caractérisé au plus tard en 1996, n'a pas respecté les dispositions du règlement n° 90-05 modifié relatif au FICP, pris après avis de la CNIL.

Bien qu'ayant procédé à la mainlevée de l'inscription du requérant du FICP, Fortis banque continue d'affirmer que cette inscription a été réalisée dans le respect des dispositions du règlement n° 90-05 relatif au FICP et conformément aux objectifs de la loi Neiertz.

Dès lors, la réponse de Fortis banque ne permet pas de garantir à la Commission que cet établissement respectera, à l'avenir, les règles de fonctionnement du FICP.

En conséquence, la Commission nationale de l'informatique et des libertés :

Demande à Fortis banque de prendre des mesures afin de rappeler, au sein de ses services, les règles de fonctionnement du FICP et d'être tenue informée des dispositions prises à cet effet.

Décide, faisant application des dispositions de l'article 21.4° de la loi du 6 janvier 1978, d'adresser à cet effet **un avertissement** à la société Fortis banque, sise 56, rue de Chateaudun à Paris.

Décide que, conformément aux dispositions de l'article 15 du règlement n° 90-05 relatif au fonctionnement du FICP et de l'article L. 613-21 du Code monétaire et financier, le présent avertissement sera porté à la connaissance de la Commission bancaire.

Délibération n° 03-033 du 19 juin 2003 portant avertissement à la Caisse régionale du Crédit agricole mutuel du Nord

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par un particulier inscrit, par la Caisse régionale du Crédit agricole mutuel du Nord, au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 modifié ;

Vu les articles L. 333-4 et suivants du Code de la consommation ;

Vu l'article L. 613-21 du Code monétaire et financier ;

Vu le règlement n° 90-05 du 11 avril 1990 du Comité de la réglementation bancaire, modifié, relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-29 du 6 mars 1990 portant avis sur le projet de règlement du Comité de la réglementation bancaire relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-72 du 29 mai 1990 portant avis sur la mise en œuvre, par la Banque de France, d'un traitement automatisé d'informations nominatives relatif à la gestion d'un fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu les courriers adressés par la Commission à la Caisse régionale du Crédit agricole mutuel du Nord les 9 avril, 2 mai et 12 juin 2003 ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'instruction de la plainte dont a été saisie la CNIL a permis d'établir que le plaignant a été inscrit par la Caisse régionale du Crédit agricole mutuel (CRCAM) du Nord au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, le 31 août 2002.

Or, il ressort d'un arrêt rendu par la cour d'appel de Douai, sur un litige opposant le plaignant à cet organisme bancaire, que l'incident de paiement qui lui est imputable, relatif au défaut de remboursement d'un crédit, est caractérisé depuis le 15 février 1994, date à laquelle une mise en demeure a été adressée au plaignant, ayant entraîné la déchéance du terme.

Après trois mois d'instruction par la CNIL – période au cours de laquelle la CRCAM du Nord a procédé à la mainlevée de l'inscription du plaignant au FICP – et plusieurs lettres de relance, la CRCAM du Nord a, dans un premier temps, indiqué à la CNIL qu'elle ne retrouvait aucune trace de fichage de ce client.

Dans un second temps, la CRCAM a indiqué qu'après avoir procédé à des investigations approfondies, le motif du fichage du plaignant au FICP, intervenu le 31 août 2002, serait vraisemblablement lié à un découvert bancaire. Or, depuis 1994, le plaignant n'utilise plus les comptes qu'il détient dans cet établissement.

Comme l'inscription au FICP paraissait avoir été faite en violation du règlement FICP, la CNIL a, par courrier du 9 avril 2003, demandé à la CRCAM du Nord de lui faire part de ses observations dans un délai de quinze jours, lui indiquant en outre que la Commission examinerait s'il convenait, en l'espèce, de faire application de l'article 21-4° de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Bien que ce courrier soit resté sans réponse, la CNIL a décidé, lors de sa séance plénière du 24 avril 2003, de ne pas adresser d'avertissement à cet établissement, dans la mesure où il avait procédé à la mainlevée de l'inscription au FICP du requérant, mais de lui adresser un courrier portant rappel à l'observation de la loi rappelant à cet établissement les dispositions du règlement n° 90-05 du 11 avril 1990 relatif au FICP et lui demandant les mesures qu'il ne manquerait pas de prendre pour assurer, à l'avenir, le respect de ces dispositions.

Le 4 juin 2003 le requérant a informé la CNIL que le 31 mars 2003, la CRCAM du Nord, qui n'a par ailleurs pas répondu aux courriers de la CNIL des 9 avril et 2 mai 2003, avait procédé à une nouvelle inscription au FICP du requérant.

Un courrier a été adressé à la CRCAM du Nord le 12 juin 2003 lui indiquant que la CNIL envisageait, une nouvelle fois, de faire application des dispositions de l'article 21-4° de la loi du 6 janvier 1978 et lui demandant de faire valoir ses observations.

Par courrier du 17 juin 2003, la CRCAM du Nord a fait part à la CNIL des observations suivantes. Elle expose qu'ayant été condamnée, par décision judiciaire, à restituer au requérant une somme d'argent correspondant au montant de son plan d'épargne populaire, ses services ont versé cette somme sur le compte courant du requérant qui a obtenu un chèque de banque de son agence le 2 décembre 2002.

La banque ajoute que cette opération, qui a eu pour conséquence de générer un « *apparent nouveau débit en compte* », dont elle ne précise pas le montant, a entraîné une nouvelle inscription du plaignant au FICP, effectuée par traitement automatisé.

La CRCAM du Nord, en précisant que cette inscription est en cours d'annulation auprès de la Banque de France, « *puisqu'il ne s'agit pas véritablement d'un nouveau débit en compte* », reconnaît ne pas avoir respecté les dispositions du règlement n° 90-05 du 11 avril 1990 du Comité de la réglementation bancaire.

Il convient de rappeler que l'article 4 du règlement n° 90-05 relatif au FICP prévoit que : « *Dès qu'un incident de paiement caractérisé est constaté, l'établissement de crédit informe le débiteur défaillant que l'incident sera déclaré à la Banque de France à l'issue d'un délai d'un mois à compter de la date d'envoi de cette information* ».

L'article 5 bis du règlement n ° 90-05 relatif au FICP prévoit par ailleurs que : « *Lorsqu'un incident caractérisé ayant affecté le remboursement d'un crédit donné est enregistré dans le fichier, il n'est procédé à aucune nouvelle déclaration au titre du même crédit en cas de survenance d'autres incidents ou de prononcé de la déchéance du terme ou d'engagement d'une procédure judiciaire* ».

En adoptant la loi n° 89-1010 du 31 décembre 1989, dite « loi Néiertz », qui a créé le fichier national des incidents de remboursement des crédits aux particuliers (FICP), le législateur a entendu mettre en place un dispositif de prévention et de traitement des situations de surendettement.

Le fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, constitue un instrument de lutte contre le surendettement des particuliers et ne saurait être utilisé à d'autres fins par les banques, les établissements de crédits et les établissements financiers de La Poste.

Dans le cas d'espèce, la CRCAM du Nord a commis plusieurs irrégularités.

Elle a d'abord inscrit son client au FICP le 31 août 2002, pour un motif non prévu par le règlement n° 90-05 du 11 avril 1990 relatif au FICP, et en a d'ailleurs convenu, au moins implicitement, en procédant à la mainlevée de cette inscription.

Cet établissement a en outre reçu plusieurs courriers de la CNIL lui rappelant les dispositions du règlement n° 90-05 du 11 avril 1990 relatif au FICP qui sont restés sans réponse.

Cet établissement a enfin procédé à une nouvelle inscription du requérant au FICP le 31 mars 2003.

Ce faisant, la CRCAM du Nord n'a respecté ni les dispositions de l'article 36 de la loi du 6 janvier 1978 relatives à l'exercice du droit de rectification, ni celles relatives au fonctionnement du FICP fixées par le règlement n° 90-05 du 11 avril 1990, modifié, pris après avis de la CNIL.

En conséquence, la Commission nationale de l'informatique et des libertés :

Demande à la CRCAM du Nord de prendre des mesures afin de rappeler, au sein de ses services, les règles de fonctionnement du FICP.

Demande à être tenue informée des dispositions prises à cet effet.

Décide, faisant application des dispositions de l'article 21.4° de la loi du 6 janvier 1978, d'adresser **un avertissement** à la Caisse régionale de Crédit agricole mutuel du Nord, sise 10 avenue Foch à Lille.

Décide que, conformément aux dispositions de l'article 15 du règlement n° 90-05 relatif au fonctionnement du FICP et de l'article L. 613-21 du Code monétaire et financier, le présent avertissement sera porté à la connaissance de la Commission bancaire.

Délibération n° 03-050 du 20 novembre 2003 portant avis sur le projet de règlement modifié n° 90.05 du 11 avril 1990 du Comité de la réglementation bancaire relatif au fichier des incidents de remboursement des crédits aux particuliers

La Commission nationale de l'informatique et des libertés ;

Saisie par le Comité de la réglementation bancaire et financière d'un projet de modification du règlement n° 90.05 relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) qui comprend également les mesures, conventionnelles et judiciaires, prises dans le cadre de la procédure de traitement des situations de surendettement ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2003-710 du 1er août 2003 d'orientation et de programmation pour la ville et la rénovation urbaine ;

Vu le Code de la consommation, titre III du livre III ;

Vu le Code de commerce ;

Vu le Code monétaire et financier ;

Vu le Code pénal ;

Vu le Code de procédure pénale ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le règlement n° 90.05 du Comité de la réglementation bancaire et financière du 1er avril 1990 relatif au fichier national des incidents de remboursement des crédits aux particuliers, modifié par les règlements n° 93.04 du 19 mars 1993, n° 96.04 du 24 mai 1996, n° 2000-04 du 6 septembre 2000, n° 2000-10 du 8 décembre 2000, n° 2003-02 du 16 mai 2003 ;

Vu la délibération n° 89-108 du 26 septembre 1989 portant avis sur un projet de loi relatif à la prévention et au règlement judiciaire des difficultés liées au surendettement des ménages ;

Vu la délibération n° 90-29 du 6 mars 1990 portant avis sur le projet de règlement du Comité de la réglementation bancaire et financière du 1er avril 1990 relatif au fichier national des incidents de remboursement des crédits aux particuliers ;

Vu les délibérations n° 93-019 du 2 mars 1993, n° 96-019 du 19 mars 1996 et n° 99-053 du 18 novembre 1999 portant avis sur les projets de règlement modifié du Comité de la réglementation bancaire relatif au fichier national des incidents de remboursement des crédits aux particuliers ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La loi d'orientation et de programmation pour la ville et la rénovation urbaine n° 2003-710 du 1er août 2003 a apporté plusieurs modifications à la procé-

dure de traitement des situations de surendettement. Les articles du Code de la consommation relatifs au FICP (articles L. 331-1 et suivants du Code de la consommation) relatifs au surendettement des particuliers et L. 628-1 et suivants du Code de commerce relatifs à la faillite civile applicable en Alsace-Moselle sont modifiés. Ces modifications rendent nécessaires, sur divers points, une mise à jour du règlement n° 90-05 précité.

Il résulte de la loi du 1er août 2003 une nouvelle définition des situations de surendettement entraînant une modification du règlement 90.05 du Comité de la réglementation bancaire et financière.

L'essentiel des modifications introduites transcrit purement et simplement les mesures adoptées par le législateur ou en constitue l'application directe. La procédure d'enregistrement des données dans le FICP est ainsi modifiée du fait de l'introduction de la procédure de rétablissement personnel, de l'augmentation de la durée des mesures conventionnelles ou judiciaires dont peuvent bénéficier les personnes surendettées, de l'enregistrement des dossiers de surendettement dès la saisine des commissions du surendettement, des nouvelles conditions de radiation de ces inscriptions, de l'inscription sous certaines conditions des informations relatives aux situations de surendettement et des jugements de faillite civile prononcés en Alsace-Moselle et de la réduction, de trois à deux ans, de la durée d'inscription des mesures visant à suspendre l'exigibilité des créances autres qu'alimentaires mentionnées à l'article L. 331-7-1 du Code de la consommation.

Ces modifications n'appellent pas d'observations de la Commission dès lors que l'information préalable des débiteurs est clairement effectuée.

D'autres dispositions du projet de modification relèvent d'une initiative réglementaire et sont motivées par le souci d'améliorer l'efficacité du dispositif en matière de lutte contre le surendettement.

Le projet de règlement prévoit ainsi que les déclarations d'incidents de paiement et la consultation du FICP pourront être effectuées par échanges sécurisés sur internet aussi bien que par remise ou télétransmission d'un fichier informatique sécurisé.

Les modalités pratiques de l'accès par internet et les mesures de sécurité ont été décrites et examinées à l'occasion de la demande d'avis relative à un portail sécurisé d'accès aux fichiers tenus par la Banque de France, dénommé « POBI », qui a fait l'objet d'un avis tacite du 2 octobre 2003 (demande d'avis n° 866088).

Cette modification a notamment pour effet de rendre accessible en temps réel l'information contenue dans le FICP et de prendre en compte l'obligation de sécurité et de mise à jour résultant de l'article 29 de la loi du 6 janvier 1978.

Elle n'appelle en conséquence pas d'observations particulières.

L'aménagement essentiel du dispositif consiste en une redéfinition des seuils à partir desquels l'incident de paiement est considéré comme caractérisé.

Ainsi, l'inscription des incidents de paiement intervient désormais dès la deuxième échéance impayée (au lieu de la troisième) pour les crédits remboursables mensuellement et dès le soixantième jour de retard (au lieu du quatre-vingt-dixième) d'une échéance dans les autres cas. Lorsque le crédit ne comporte pas d'échéances échelonnées (cas d'une autorisation de découvert), le retard caractérisant l'incident de paiement est ramené de quatre-vingt-dix jours à soixante jours, après la date de mise en demeure du débiteur d'avoir à régulariser la situation, sans pour autant que soit augmenté le seuil du montant ouvrant lieu à inscription qui reste fixé à 500 euros.

S'il n'appartient pas à la Commission de fixer le seuil permettant de caractériser l'incident de paiement, elle constate cependant que ces mesures auront des

répercussions certaines sur le nombre de personnes fichées et potentiellement le nombre de contestations dont la Commission est saisie, alors que dans le même temps est noté un accroissement des plaintes relatives au non-respect des conditions d'inscription au FICP par les établissements de crédit. La redéfinition des conditions d'inscription appelle donc encore plus de rigueur dans la gestion du fichier.

En conséquence, la Commission rappelle que :
– la proportionnalité et la pertinence du traitement doivent être préservées ;
– le nombre de plaintes reçues justifie son inquiétude quant aux conditions de respect par les établissements de crédit du règlement du CRBF ;
– elle fera preuve d'une vigilance particulière sur les suites données à l'instruction des réclamations dont elle est saisie.

Attire l'attention des autorités de contrôle des activités financières sur ce point ainsi que sur l'intérêt de la mise en place, au sein de la Banque de France, d'une instance de médiation chargée notamment, en liaison avec les médiateurs des établissements de crédit, de faciliter l'exercice des droits de rectification et d'opposition des personnes inscrites au FICP.

Demande à être saisie d'une demande d'avis modificative de la Banque de France relative aux modalités de fonctionnement du FICP afin d'apprécier les mesures prises pour assurer le respect des dispositions du règlement du CRBF, tout particulièrement les mesures destinées à prévenir le détournement de finalité.

Émet un avis favorable au projet de modification du règlement n° 90.05 du 11 avril 1990 du Comité de la réglementation bancaire.

Délibération n° 03-051 du 20 novembre 2003 portant avertissement au Crédit immobilier de France

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par un particulier inscrit, par le Crédit immobilier de France – Ile-de-France, au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 modifié ;

Vu les articles L. 333-4 et suivants du Code de la consommation ;

Vu l'article L. 613-21 du Code monétaire et financier ;

Vu le règlement n° 90-05 du 11 avril 1990 du Comité de la réglementation bancaire, modifié, relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-29 du 6 mars 1990 portant avis sur le projet de règlement du Comité de la réglementation bancaire relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-72 du 29 mai 1990 portant avis sur la mise en œuvre, par la Banque de France, d'un traitement automatisé d'informations nominatives relatif à la gestion d'un fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 87-25 du 10 février 1987 fixant le règlement intérieur de la CNIL, et notamment son article 54 ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'instruction de la plainte dont a été saisie la CNIL a permis d'établir que le plaignant a été inscrit par le Crédit immobilier de France au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, le 31 août 2002 pour une durée de cinq ans.

Le plaignant indique avoir tenté, à plusieurs reprises, depuis le mois de décembre 2002, d'obtenir de cet établissement la mainlevée de cette inscription dont il conteste le bien-fondé, démarche demeurée infructueuse.

Dans un courrier adressé à une association de consommateurs, saisie par le requérant, le Crédit immobilier de France indique que l'inscription de son client au FICP résultait *« d'un incident de remboursement caractérisé ayant conduit à l'exigibilité anticipée de son prêt en 1991 »*, ajoutant que *« tant que la totalité de* [la]

créance n'est pas intégralement remboursée, [il a] *l'obligation de maintenir le fichage des époux C. ».*

La CNIL a, le 16 octobre 2003, adressé un courrier au Crédit immobilier de France lui demandant, d'une part, de procéder à la mainlevée de l'inscription du requérant au FICP et, d'autre part, de faire valoir ses observations sur ce dossier, lui indiquant en outre que la Commission examinerait s'il convenait, en l'espèce, de faire application de l'article 21-4° de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le Crédit immobilier de France a indiqué en réponse qu'il procédait à la mainlevée de l'inscription de son client au FICP, sans autre précision.

L'article 4 du règlement n ° 90-05 relatif au FICP prévoit que : *« Dès qu'un incident de paiement caractérisé est constaté, l'établissement de crédit informe le débiteur défaillant que l'incident sera déclaré à la Banque de France à l'issue d'un délai d'un mois à compter de la date d'envoi de cette information ».*

En adoptant la loi n° 89-1010 du 31 décembre 1989, dite « loi Néiertz », qui a créé le fichier national des incidents de remboursement des crédits aux particuliers (FICP), le législateur a entendu mettre en place un dispositif de prévention et de traitement des situations de surendettement.

Le fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, constitue un instrument de lutte contre le surendettement des particuliers et n'a pas pour finalité la mise en commun entre les banques, les établissements de crédits et les établissements financiers de La Poste, d'informations relatives à leurs débiteurs, sauf dans les cas prévus par les dispositions du règlement n° 90-05 précité.

Dans le cas d'espèce, le Crédit immobilier de France, en inscrivant son client au FICP le 31 août 2002, pour un incident de paiement caractérisé datant de 1991, n'a pas respecté les dispositions du règlement n° 90-05 modifié relatif au FICP, pris après avis de la CNIL.

En outre, cet établissement bancaire, en ne faisant pas droit aux demandes de mainlevée de cette inscription formulées par le requérant et en ne procédant pas à la rectification d'une information erronée transmise à la Banque de France, n'a pas respecté les dispositions des articles 36, 37 et 38 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Bien qu'ayant répondu qu'il procédait à la mainlevée de l'inscription du requérant du FICP, le responsable du service contentieux du Crédit immobilier de France n'a transmis à la Commission aucune autre observation relative au courrier qu'elle lui avait adressé.

En conséquence la Commission **demande** au Crédit immobilier de France de prendre des mesures afin de rappeler, au sein de ses services, les règles de fonctionnement du FICP et d'être tenue informée des dispositions prises à cet effet.

Décide, faisant application des dispositions de l'article 21.4° de la loi du 6 janvier 1978, d'adresser à cet effet **un avertissement** au Crédit immobilier de France – Ile-de-France, dont le siège social est situé 59, rue de Provence à Paris.

Décide que, conformément aux dispositions de l'article 15 du règlement n° 90-05 relatif au fonctionnement du FICP et de l'article L. 613-21 du Code monétaire et financier, le présent avertissement sera porté à la connaissance de la Commission bancaire.

Délibération n° 03-052 du 20 novembre 2003 portant avertissement au Crédit mutuel du grand Cronenbourg

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par un particulier inscrit, par le Crédit mutuel du grand Cronenbourg, au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 modifié ;

Vu les articles L. 333-4 et suivants du Code de la consommation ;

Vu l'article L. 613-21 du Code monétaire et financier ;

Vu le règlement n° 90-05 du 11 avril 1990 du Comité de la réglementation bancaire, modifié, relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-29 du 6 mars 1990 portant avis sur le projet de règlement du Comité de la réglementation bancaire relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 90-72 du 29 mai 1990 portant avis sur la mise en œuvre, par la Banque de France, d'un traitement automatisé d'informations nominatives relatif à la gestion d'un fichier national des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 87-25 du 10 février 1987 fixant le règlement intérieur de la CNIL, et notamment son article 54 ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

L'instruction de la plainte dont a été saisie la CNIL a permis d'établir que la plaignante a été inscrite par le Crédit mutuel du grand Cronenbourg au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, le 31 octobre 2000 pour une durée de cinq ans, pour un incident de paiement relatif à un prêt personnel.

Par jugement en date du 10 mai 2001, la plaignante a été condamnée à rembourser au Crédit mutuel du grand Cronenbourg les sommes de 6 785,85 euros au titre d'un prêt personnel et de 655,49 euros, augmentée des intérêts légaux, au titre du solde débiteur sur son compte courant.

Il convient de relever que la plaignante n'a été inscrite au FICP que pour l'incident de paiement relatif au non-remboursement des échéances de son prêt person-

nel et qu'elle n'a fait l'objet d'aucune inscription de la part du Crédit mutuel du grand Cronenbourg pour le solde débiteur de son compte courant.

La plaignante indique avoir réglé l'intégralité des sommes dues au titre du prêt personnel contracté auprès du Crédit mutuel du grand Cronenbourg au mois de janvier 2002.

Or, le Crédit mutuel du grand Cronenbourg a maintenu son inscription au FICP jusqu'au mois de juin 2003.

Elle indique avoir tenté, à plusieurs reprises, d'obtenir de cet établissement la mainlevée de cette inscription, démarche demeurée infructueuse.

Saisi par la CNIL dans ce dossier le 15 mai 2003, le Crédit mutuel du grand Cronenbourg a finalement indiqué à la Commission avoir procédé à la mainlevée de l'inscription de sa cliente du FICP le 13 juin 2003 dans la mesure où la créance pour laquelle elle avait fait l'objet d'une condamnation avait été réglée par la requérante le 4 avril 2003 puisqu'il subsistait un reliquat sur son compte courant.

Toutefois, et dans la mesure où seule la date de régularisation de l'impayé relatif au prêt personnel de la requérante devait déterminer la date de mainlevée de son inscription au FICP, la CNIL a demandé des informations complémentaires sur ce point à cet établissement bancaire.

Le Crédit mutuel du grand Cronenbourg a finalement indiqué que la plaignante avait réglé sa dette relative au prêt personnel « avant le 7 juin 2002 ».

La CNIL a, le 16 octobre 2003, adressé un courrier au Crédit mutuel du grand Cronenbourg lui demandant de faire valoir ses observations sur ce dossier, lui indiquant en outre que la Commission examinerait s'il convenait, en l'espèce, de faire application de l'article 21-4° de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Par courrier du 18 novembre 2003, le directeur du Crédit mutuel du grand Cronenbourg indiquait à la CNIL que le maintien de l'inscription de la requérante au FICP résultait d'une erreur d'interprétation des règles relatives au fonctionnement du FICP et ajoutait qu'il présentait ses excuses pour ce *« fâcheux incident »*.

L'article 6 du règlement n° 90-05 du 11 avril 1990 modifié relatif au FICP prévoit que l'établissement de crédit signale à la Banque de France *« le paiement intégral des sommes dues »*.

En adoptant la loi n° 89-1010 du 31 décembre 1989, dite « loi Néiertz », qui a créé le fichier national des incidents de remboursement des crédits aux particuliers (FICP), le législateur a entendu mettre en place un dispositif de prévention et de traitement des situations de surendettement. Le fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France, constitue un instrument de lutte contre le surendettement des particuliers et n'a pas pour finalité la mise en commun entre les banques, les établissements de crédits et les établissements financiers de La Poste, d'informations relatives à leurs débiteurs, sauf dans les cas prévus par les dispositions du règlement n° 90-05 précité.

Dans le cas d'espèce, le Crédit mutuel du grand Cronenbourg, en ne procédant pas à mainlevée de l'inscription de sa cliente au FICP dès le règlement intégral des sommes dues au titre de l'incident ayant généré l'inscription, n'a pas respecté les dispositions du règlement n° 90-05 modifié relatif au FICP, pris après avis de la CNIL.

En outre, cet établissement bancaire n'a pas fait droit aux demandes de mainlevée de cette inscription formulées par la requérante et a maintenu son inscription pendant près de dix-huit mois. Le Crédit mutuel du grand Cronenbourg aurait en

effet dû procéder à la mise à jour de l'information relative à l'inscription de la requérante auprès de la Banque de France dès le règlement intégral des sommes dues au titre du prêt personnel souscrit par la plaignante.

Dès lors, cet établissement n'a pas respecté les dispositions des articles 36, 37 et 38 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En conséquence, la Commission **demande** au Crédit mutuel du grand Cronenbourg de prendre des mesures afin de rappeler, au sein de ses services, les règles de fonctionnement du FICP et d'être tenue informée des dispositions prises à cet effet.

Décide, faisant application des dispositions de l'article 21,4° de la loi du 6 janvier 1978, d'adresser à cet effet **un avertissement** au Crédit mutuel du grand Cronenbourg, dont le siège social est situé 90, route de Mittelhausbergen à Strasbourg.

Décide que, conformément aux dispositions de l'article 15 du règlement n° 90-05 relatif au fonctionnement du FICP et de l'article L 613-21 du Code monétaire et financier, le présent avertissement sera porté à la connaissance de la Commission bancaire.

Biométrie

Délibération n° 03-027 du 22 mai 2003 portant avis sur le projet d'arrêté du ministre de la Justice portant création d'une application informatique destinée à vérifier l'identité des détenus en établissement par reconnaissance de la morphologie de la main

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère de la Justice d'un projet d'arrêté portant création d'un traitement automatisé de données nominatives destiné à vérifier l'identité des détenus en établissement par reconnaissance biométrique de la morphologie de la main ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le projet d'arrêté du ministre de la Justice ;

Après avoir entendu Monsieur Patrick Delnatte, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministre de la Justice a saisi la Commission d'un projet d'arrêté portant création d'un traitement automatisé de données nominatives destiné à vérifier l'identité des détenus en établissement par reconnaissance biométrique de la morphologie de la main.

Cette application permettra en outre d'éditer, dès l'entrée dans l'établissement concerné, une carte d'identité intérieure, support plastifié sur lequel figurent le nom et la photographie du détenu et une piste magnétique sur laquelle est enregistré son numéro d'écrou, à l'exclusion de toute autre catégorie d'informations nominatives, notamment le gabarit de la main.

Cette application a pour objet de lutter contre d'éventuelles tentatives d'évasion par substitution à l'occasion des déplacements des détenus aux parloirs.

Elle repose sur la constitution d'une base centrale, propre à chaque établissement et reliée à une ou plusieurs bornes qui permettront de l'interroger au moyen de la carte d'identité intérieure du détenu.

Dès l'arrivée d'un détenu en établissement, les personnels du greffe procèdent à l'enregistrement dans la base centrale des informations relatives à son identité (nom, prénom, numéro d'écrou, photographie numérisée), ainsi qu'à celui d'un gabarit de son empreinte palmaire.

Pour procéder à la vérification de l'identité d'un détenu à l'intérieur de l'établissement, tout particulièrement avant et après un déplacement au parloir, le personnel pénitentiaire procède à une vérification de la mesure ponctuelle de la

morphologie de la main du détenu par rapport au gabarit enregistré dans la base de l'établissement.

Le numéro d'écrou, encodé dans la piste magnétique de la carte d'identité intérieure du détenu, permet d'interroger la base centrale. Si la mesure de la main est identique à celle enregistrée dans la base et associée au numéro d'écrou, les informations relatives à l'identité du détenu ainsi que sa photographie s'affichent à l'écran. Si le gabarit et la mesure ponctuelle ne correspondent pas, l'absence d'affichage de l'identité du détenu et de sa photographie, pouvant laisser supposer une tentative d'usurpation d'identité, alerte le surveillant.

S'agissant du recours à l'identification par reconnaissance de la morphologie de la main, la Commission a souligné à plusieurs reprises que cette technique ne soulevait pas de difficulté particulière au regard des dispositions de la loi du 6 janvier 1978 en ce qu'il n'est pas possible d'y recourir à l'insu des personnes concernées, contrairement à la technique des empreintes digitales.

Si la Commission a exprimé sa préférence pour les techniques n'impliquant pas la constitution d'une base centrale regroupant des gabarits biométriques d'individus, il convient de relever ici, outre les impératifs de sécurité, que la base centrale qui sera créée sera propre à chaque établissement et ne sera pas interconnectée avec d'autres traitements.

Les informations nominatives enregistrées et traitées dans la base de l'établissement sont, pour des raisons de sécurité, effacées dès que le détenu concerné quitte l'établissement, que ce soit à l'occasion de sa libération ou d'un transfèrement dans un autre établissement en cours de peine. Lors de sa levée d'écrou, le détenu doit également remettre sa carte d'identité intérieure.

Cette durée de conservation apparaît pertinente au regard de la finalité du traitement.

Les seuls destinataires des informations nominatives relatives aux détenus qui sont collectées et traitées au moyen de cette application sont les surveillants de l'établissement pénitentiaire concerné.

La base centrale dans laquelle ces informations seront enregistrées sera, dans tous les cas, installée au greffe de l'établissement pénitentiaire concerné, bâtiment faisant déjà l'objet de mesures de sécurité physiques renforcées.

De plus, seuls les personnels du greffe de l'établissement disposent des mots de passe leur permettant d'accéder à la base.

Les détenus bénéficient d'un droit d'accès direct aux informations les concernant qui figurent dans la base de leur établissement d'incarcération et en sont informés par une affiche présente dans les locaux du greffe.

Émet un avis favorable au projet d'arrêté du ministre de la Justice portant création d'un modèle-type de traitement de données nominatives relatif à l'identité des détenus, avec production d'une carte d'identité infalsifiable et contrôle biométrique de la morphologie de la main.

Délibération n° 03-032 du 5 juin 2003 portant avis sur le projet d'arrêté du ministre de la Justice portant création dans certains établissements pénitentiaires d'un traitement automatisé de données nominatives ayant pour objet la gestion des personnes placées sous surveillance électronique

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère de la Justice d'un projet d'arrêté portant création, dans les établissements pénitentiaires participant à l'expérimentation, d'un traitement automatisé de données nominatives ayant pour objet la gestion des personnes placées sous surveillance électronique ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le Code de procédure pénale, notamment ses articles 138, 723-7 à 723-17 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu l'arrêté du 1er juillet 2002 portant homologation du procédé de surveillance électronique pris pour l'application du décret n° 2002-479 du 3 avril 2002 portant modification du Code de procédure pénale ;

Vu le projet d'arrêté du ministre de la Justice ;

Après avoir entendu Monsieur Patrick Delnatte, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministre de la Justice a saisi la Commission d'un projet d'arrêté portant création, dans les établissements pénitentiaires participant à l'expérimentation, d'un traitement automatisé de données nominatives destiné à assurer la gestion des personnes placées sous surveillance électronique.

Cette modalité particulière d'exécution du contrôle judiciaire, d'une peine privative de liberté (ou de son reliquat) ou d'une mesure de liberté conditionnelle consiste à assigner, en permanence ou pendant certaines plages horaires, le condamné ou la personne astreinte à un contrôle judiciaire dans un lieu fixé par le juge et à vérifier à distance que l'intéressé respecte les obligations de présence qui lui ont été imposées.

Ce dispositif repose sur un bracelet-émetteur, que l'intéressé doit porter en permanence pendant toute la durée de la mesure, un émetteur/récepteur qui décode les signaux radio du bracelet-émetteur et un centre de surveillance, installé au greffe de l'établissement pénitentiaire dont dépend la personne concernée, qui reçoit les éventuels messages d'alerte envoyés par l'émetteur/récepteur lorsque ce dernier ne détecte plus la présence du bracelet-émetteur pendant les plages horaires d'assignation.

Le traitement mis en œuvre dans chacun des établissements pénitentiaires concernés permet à son personnel de vérifier que les personnes placées sous surveil-

lance électronique respectent les obligations de présence imposées par le juge, de modifier, le cas échéant, leurs plages horaires d'assignation et d'éditer périodiquement des rapports et des statistiques non nominatives.

À cette fin, sont enregistrées dans le traitement des informations nominatives relatives à l'identité des personnes placées sous surveillance électronique (nom, prénoms, date de naissance, sexe et situation familiale), au lieu d'assignation fixé par le juge (numéro, rue, code postal, ville et numéros de téléphone), aux modalités particulières d'exécution de la mesure (dates et heures des mouvements au lieu d'assignation, type de mouvement – sous la forme : « entrée » ou « sortie »), au rapport de la personne concernée avec la justice (numéro d'écrou, catégorie pénale, plages horaires journalières de sortie, dates et heures de début et de fin de la période de placement, fin normale ou retrait de la mesure, périmètre d'assignation, dates et heures des alarmes, types), ainsi qu'aux coordonnées des différents responsables du suivi de la personne placée sous surveillance électronique (nom, prénom et numéro de télécopie du magistrat ; nom, prénom et numéro de télécopie du travailleur social ; numéro de téléphone du surveillant d'astreinte).

Les destinataires des informations nominatives traitées sont, chacun en ce qui le concerne, les magistrats du tribunal de grande instance dont dépend l'établissement pénitentiaire concerné, le chef de cet établissement pénitentiaire, le directeur du service pénitentiaire d'insertion et de probation et les agents dûment habilités du service chargé de la surveillance électronique.

Les informations nominatives traitées sont effacées dès la fin de la mesure, puis conservées à titre d'archive pendant douze mois sur un support magnétique différent dédié uniquement à cette fonction.

Le traitement mis en œuvre et les postes informatiques permettant d'y accéder sont installés au greffe de chacun des établissements pénitentiaires concernés, dont la sécurité et l'accès font l'objet de mesures de protection particulières.

En outre, la base et les postes permettant d'y accéder sont reliés par un réseau local propre qui ne sera pas interconnecté à un autre réseau.

L'accès aux postes est réservé aux agents de l'établissement pénitentiaire dûment habilités, qui disposent de mots de passe à cette fin. Un dispositif d'enregistrement des accès au traitement permet d'identifier l'auteur et le poste de travail à partir duquel il a été accédé à la base.

En cas de panne matérielle ou logicielle, il est prévu que les prestataires techniques peuvent assurer des opérations de maintenance à distance à partir de deux centres situés à l'étranger.

La Commission prend acte que le recours à une telle procédure revêt un caractère temporaire et que, préalablement à la généralisation du placement sous surveillance électronique prévue en 2004, le ministère de la Justice recommandera aux prestataires techniques choisis de se doter d'un centre de maintenance situé en France.

Elle observe aussi que le ministère de la Justice, outre la mise en place de mesures de sécurité physiques et logiques renforcées, conclura avec chacun des deux prestataires concernés un contrat reprenant les principales dispositions protectrices de la loi du 6 janvier 1978.

Ce contrat prévoit notamment les cas précis dans lesquels ces sociétés peuvent agir à distance sur le traitement, prohibe toute réutilisation des données, rappelle que les informations transmises sont couvertes par le secret professionnel et impose à ces sociétés de prendre des mesures de sécurité particulières pendant les

transferts d'informations. Ce contrat prévoit en outre que le contrôle du respect des engagements des parties pourra être effectué sur place par la personne déléguée à la protection des données désignée par le ministère de la Justice, par un membre de la Commission ou par une société de contrôle spécialisée ou un organisme d'audit désigné par la CNIL.

La Commission considère toutefois que ces mesures doivent être renforcées par la formalisation dans ce modèle de contrat des précisions suivantes :
– l'indication que la procédure de télémaintenance ne sera engagée qu'en dernier recours et, en tout état de cause, après que tous les autres moyens de remédier à la panne détectée ont été employés ;
– l'indication des cas dans lesquels cette procédure de télémaintenance, qui dans la plupart des cas prend la forme d'un accès à distance au traitement, peut impliquer un transfert de données nominatives et les mesures de sécurité particulières qui seront adoptées dans cette hypothèse ;
– une typologie sommaire des pannes éventuelles susceptibles d'affecter les matériels comme le logiciel utilisé et, dans la mesure du possible, la précision selon laquelle la résolution de chacune d'entre elles implique ou non le recours à la télémaintenance.

Les personnes placées sous surveillance électronique, comme les différents acteurs chargés du suivi de cette mesure, disposent d'un droit d'accès direct aux informations nominatives les concernant. Elles sont informées personnellement de l'existence du traitement, ainsi que de leurs droits d'accès et de rectification par le document leur notifiant les obligations qui leur incombent dans le cadre de leur placement. En outre, un document d'information est affiché au greffe de l'établissement pénitentiaire concerné.

Émet au bénéfice des observations qui précèdent, **un avis favorable** au projet d'arrêté du ministre de la Justice portant création, dans les établissements pénitentiaires participant à l'expérimentation, d'un traitement automatisé de données nominatives destiné à assurer la gestion des personnes placées sous surveillance électronique.

Demande que lui soit soumis le modèle de contrat de protection des données en matière d'opérations de maintenance ainsi modifié.

Délibération n° 03-043 du 7 octobre 2003 portant avis sur un projet de décret modifiant le Code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques

Saisie par le ministère de la Justice d'un projet de décret en Conseil d'État modifiant le Code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 2003-495 du 18 mars 2003 pour la sécurité intérieure ;

Vu le Code de procédure pénale, notamment ses articles 706-54 à 706-56 et R. 53-9 à R. 53-21 ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu ensemble les délibérations nº 99-052 du 28 octobre 1999 et 02-008 du 7 mars 2002 de la Commission portant avis sur le fichier national des empreintes génétiques ;

Vu le projet de décret présenté par le ministre de la Justice ;

Après avoir entendu Monsieur François Giquel en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère de la Justice a saisi la CNIL d'un projet de décret en Conseil d'État modifiant le Code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques.

Ce projet de décret est prévu par l'article 706-54 du Code de procédure pénale qui, dans sa rédaction issue de la loi du 18 mars 2003, élargit, d'une part, la liste des personnes dont l'empreinte génétique est susceptible de faire l'objet d'un enregistrement dans le FNAEG et, d'autre part, celle des infractions concernées, telles qu'elles résultent de la rédaction de l'article 706-55 du Code de procédure pénale.

Ce projet de texte a pour objet de préciser les nouvelles conditions d'alimentation et de consultation du FNAEG, ainsi que les règles de conservation et d'effacement des informations nominatives qui y sont enregistrées.

La Commission estime que l'extension très importante du champ d'application du fichier national des empreintes génétiques, tant en ce qui concerne les infractions visées que les personnes concernées, nécessite des garanties sérieuses destinées à prévenir tout enregistrement non contrôlé, erroné ou abusif des personnes et tout usage d'un tel fichier à des fins étrangères à celles pour lesquelles il a été constitué.

Les catégories de personnes concernées

D'une part, seront enregistrées dans le fichier les empreintes génétiques résultant des traces biologiques de personnes inconnues, recueillies dans le cadre d'une enquête de flagrance, préliminaire ou d'une instruction concernant l'une des infractions visées par l'article 706-55 du Code de procédure pénale, ainsi que les échantillons biologiques prélevés sur des cadavres non identifiés et les traces biologiques issues de personnes inconnues dans le cadre d'une enquête sur les causes de la mort ou sur une disparition inquiétant et suspecte.

D'autre part, la liste des personnes identifiées désormais susceptibles de voir leur empreinte génétique enregistrée dans le FNAEG, fixée par l'article 3 du projet de décret, comprend :
– les personnes condamnées pour l'une des infractions mentionnées à l'article 706-55 du Code de procédure pénale, sur décision du procureur général ou du procureur de la République ;
– les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, dans le cadre d'une enquête préliminaire ou de flagrance ou d'une instruction, sur décision de l'officier de police judiciaire agissant soit d'office soit sur demande du procureur de la République ou du juge d'instruction ;
– les personnes disparues pour lesquelles des échantillons biologiques auraient pu être recueillis dans le cadre d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte ;
– avec leur accord, les ascendants ou descendants d'une personne disparue, dans le cadre d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte.

La Commission relève que la loi ne prévoit pas l'enregistrement dans le FNAEG de l'empreinte génétique de cette dernière catégorie de personnes. Toutefois, à supposer que cette nouvelle catégorie puisse être introduite par décret, la Commission prend acte de la proposition du ministère de la Justice de compléter l'article 3 du projet de décret (R. 53-10, I, 5° nouveau du Code de procédure pénale) afin qu'il précise que l'accord des ascendants ou descendants d'une personne disparue doit être recueilli par procès-verbal.

La Commission estime en outre que les empreintes génétiques de ces personnes ne devraient pouvoir être exploitées et conservées que pour répondre à la seule finalité de recherche de la personne disparue et considère en conséquence que la proposition du ministère de la Justice d'exploiter les empreintes génétiques de ces personnes et de les conserver dans le FNAEG jusqu'à la découverte de la personne disparue ou à défaut pendant quarante ans, y compris à des fins d'identification et de recherche d'auteurs d'infractions, est de nature à faire naître un risque de confusion entre les différentes finalités du fichier.

La Commission prend acte de la proposition complémentaire d'offrir la possibilité aux ascendants et descendants d'une personne disparue d'autoriser, par une mention expresse à ce même procès-verbal, l'utilisation de leurs empreintes génétiques à des fins d'identification et de recherche des auteurs d'infractions, mais estime que le FNAEG devrait être structuré de telle façon que les données concernant les ascendants et les descendants de personnes disparues ayant limité l'utilisation de leurs empreintes génétiques aux seules fins de recherche de la personne disparue concernée puissent être traitées et consultées de façon distincte.

Les informations enregistrées

L'article 4 du projet de décret énumère les informations (numéro de la procédure, autorité judiciaire ou officier de police judiciaire ayant demandé l'enregistrement au fichier, date de la demande d'enregistrement dans le fichier ou celle à laquelle la condamnation est devenue définitive, nom de la personne physique ou morale habilitée ayant réalisé l'analyse, nature de l'affaire) qui, dans tous les cas, doivent accompagner les empreintes génétiques résultant de l'analyse soit de prélèvements, soit de traces biologiques, et font l'objet d'un enregistrement dans le FNAEG.

Dans le cas des personnes inconnues ou disparues et des cadavres non identifiés, seront en outre enregistrées des informations relatives au scellé contenant les traces ou échantillons biologiques ayant servi à l'analyse.

Dans le cas des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, seront en outre enregistrés les nom, prénoms, date et lieu de naissance et filiation des personnes dont sont enregistrées les empreintes génétiques.

Dans le cas des échantillons prélevés sur des ascendants et descendants d'une personne disparue, seront enregistrés : les nom, prénoms, date et lieu de naissance de la personne disparue et l'indication du lien de parenté avec celle-ci de la personne dont sont enregistrées les empreintes génétiques.

L'enregistrement et le traitement de ces informations apparaissent pertinents au regard de la finalité que le législateur a donnée au fichier.

S'agissant plus particulièrement de l'information relative à la nature de l'affaire qui, aux termes de l'article 4 du projet de décret, ne peut être exploitée qu'en vue d'un traitement à des fins statistiques quand il s'agit des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale ou des personnes condamnées, la Commission prend acte de la proposition du ministère de la Justice de préciser dans le projet de décret que cette information ne peut apparaître en cas de consultation, ni servir de critère de recherche nominative dans le fichier.

La Commission estime qu'une telle disposition est de nature à garantir que le FNAEG ne sera utilisé que pour faciliter l'identification et la recherche des auteurs d'infractions et non pour connaître les antécédents judiciaires des personnes qui y figurent.

La durée de conservation des informations

La durée de conservation des informations nominatives enregistrées dans le FNAEG est fixée par l'article 8 du projet de décret à une durée maximale de quarante années. Dans le cas des cadavres non identifiés ou de la recherche de personnes disparues, les empreintes génétiques correspondantes seront effacées après identification définitive de la personne décédée ou dès réception d'un avis de découverte de la personne.

Le ministère de la Justice a fait connaître que par cohérence avec la durée de conservation des informations nominatives enregistrées dans le fichier automatisé des empreintes digitales, il pourrait être prévu de réduire à vingt-cinq ans la durée de conservation des informations dans le FNAEG pour les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles

aient commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, mais que cette réduction soulèverait d'importantes difficultés, au regard de l'efficacité du fichier, spécialement concernant les auteurs d'infractions sexuelles.

Le ministère de la Justice propose en conséquence une nouvelle rédaction de l'article 8 du projet de décret réduisant à vingt-cinq ans la durée maximale de conservation des informations concernant les personnes visées au 2° du I de l'article R. 53-10, sauf si la personne a fait l'objet d'une décision de classement sans suite, de non-lieu, de relaxe ou d'acquittement exclusivement fondée sur l'existence d'un trouble mental, en application de l'article 122-1, premier alinéa, du Code pénal, décision dont la gestionnaire du fichier aura été informée par le procureur de la République, les données étant alors conservées pendant quarante ans à compter de la date de la décision.

La Commission prend bonne note de la proposition du ministère de la Justice de réduire à vingt-cinq ans la durée de conservation maximale dans le fichier des informations concernant les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, mais estime en tout état de cause excessif, au regard de la finalité du fichier et vu la diversité des situations générant l'enregistrement des empreintes génétiques de personnes identifiées, que les durées de conservation des informations qui y figurent soient fixées de façon uniforme, sans tenir compte de la gravité et de la nature de l'infraction ni de la situation juridique des personnes concernées.

En effet, peuvent être enregistrées dans le fichier les empreintes génétiques :
– de personnes condamnées, de personnes soupçonnées, des ascendants ou descendants de personnes disparues ;
– pour des infractions de nature très différente, dont la sanction peut aller de la réclusion criminelle à perpétuité à une simple amende, selon qu'il s'agit d'infractions de nature sexuelle, d'actes de terrorisme, de crimes et délits d'atteintes volontaires à la vie de la personne, etc. ou de certains délits d'atteintes aux biens, tels que des appels téléphoniques malveillants ou la dégradation d'un véhicule par inscriptions, signes ou dessins.

La Commission demande par conséquent que soit prévue une modulation des durées de conservation des données, qu'il s'agisse des personnes condamnées ou de celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55.

Elle demande enfin qu'aucune exception à la durée de conservation maximale de vingt-cinq ans ne puisse être faite, s'agissant par exemple des personnes atteintes, au moment des faits, d'un trouble psychique ou neuropsychique ayant aboli leur discernement ou le contrôle de leurs actes.

La procédure d'effacement des informations enregistrées dans le fichier

L'article 7 du projet de décret fixe les modalités pratiques de la procédure d'effacement, mais ne contient aucune disposition facilitant l'application de la loi quant aux cas dans lesquels *« la conservation des empreintes n'apparaîtrait plus nécessaire compte tenu de la finalité du fichier »*.

Le ministère de la Justice a indiqué que si les critères d'effacement des informations enregistrées au FNAEG relèvent de l'appréciation souveraine des faits par

les magistrats compétents, une circulaire donnera des indications aussi précises que possible sur l'application de ces dispositions, indications qui auront valeur d'instruction générale pour les magistrats du parquet et constitueront un élément d'information utile pour ceux du siège.

Ainsi, dans les cas où la procédure judiciaire aura permis de mettre totalement hors de cause une personne à l'encontre de laquelle il existait des indices graves ou concordants rendant vraisemblable qu'elle ait commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, l'effacement des informations la concernant sera ordonné, y compris d'office.

Le ministère de la Justice précise qu'en revanche une décision de classement sans suite, de non-lieu, de relaxe ou d'acquittement ne devra pas donner lieu à effacement s'il apparaît dans la procédure que la personne a bien commis les faits reprochés et que la décision judiciaire la concernant est fondée sur d'autres motifs que sa mise hors de cause (par exemple en cas de classement sans suite en opportunité, de prescription ou de trouble mental).

Enfin le ministère de la Justice indique que dans les cas où la décision de classement sans suite, de non-lieu, de relaxe ou d'acquittement est intervenue au bénéfice du doute, par application justifiée du principe de la présomption d'innocence, une analyse détaillée des différents éléments de la procédure (éléments à charge, personnalité de l'intéressé, nature et gravité des faits reprochés, temps écoulé depuis leur commission) interviendra pour apprécier si, compte tenu de la finalité du fichier, l'effacement des informations relatives à l'intéressé doit être ou non ordonné.

La Commission prend note de ces orientations mais estime qu'elles devraient recevoir une traduction juridique dans le projet de décret, l'article 7 étant complété au moins afin de préciser que si la procédure judiciaire a mis hors de cause la personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, notamment en permettant l'identification du coupable des faits dont elle était soupçonnée, l'effacement des informations la concernant dans le FNAEG devra être ordonné, y compris d'office.

La Commission demande qu'en tout état de cause lui soit soumise, ainsi que l'a proposé le ministère de la Justice, la circulaire d'application de ces dispositions réglementaires.

À la question posée par le ministère de la Justice de savoir si, dans les cas exceptionnels d'infractions d'une particulière gravité, il ne pourrait toutefois pas paraître justifié de conserver au FNAEG l'empreinte d'une personne poursuivie, puis mise judiciairement mise hors de cause, si les éléments de la procédure font apparaître des éléments objectifs pouvant faire craindre que cette personne ne passe un jour à l'acte, la Commission ne peut répondre que négativement, une telle règle ayant pour effet de faire figurer dans le FNAEG, à côté de celles de personnes condamnées et de celles de personnes mises en cause, les empreintes génétiques de « suspects potentiels ».

Les destinataires

L'article 9 du projet de décret détermine les personnes qui seules pourront accéder directement au fichier, à savoir les personnels de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire de la police nationale et ceux de la gendarmerie nationale, spécialement affectés dans le service mettant en œuvre le traitement et dûment habilités, ainsi que, pour certaines

opérations relatives aux scellés, les personnels affectés au service central de préservation des prélèvements biologiques et dûment habilités.

La Commission estime qu'il conviendrait de compléter cette disposition du projet de décret par la mention des officiers de police judiciaire agissant au titre de l'article 706-56 I, premier alinéa, du Code de procédure pénale, en précisant les informations accessibles à ces personnels lors de l'interrogation du fichier qui doit se faire au vu du seul état civil de l'intéressé.

La nature de l'ADN utilisé

La Commission prend acte de ce que le ministère de la Justice ne voit aucune objection à ce que l'article 6 du projet de décret renvoie expressément, dans un souci de lisibilité, au cinquième alinéa de l'article 706-54 du Code de procédure pénale qui prévoit que les empreintes génétiques inscrites dans le fichier ne peuvent êtres réalisées que sur la partie non codante de l'ADN.

Les mesures transitoires

L'article 13 du projet de décret prévoit que les résultats des analyses d'identification par empreintes génétiques prévus à l'article 3 de ce même texte (article R. 53-10, I et II) qui auraient été obtenus avant l'entrée en vigueur de ces dispositions dans le cadre de procédures judiciaires puissent être enregistrés dans le FNAEG.

Cette disposition, qui figurait déjà dans le décret du 18 mai 2000, n'appelle pas d'observation particulière de la part de la Commission, mais nécessite cependant d'être complétée par l'énumération des catégories de personnes, officiers de police judiciaire ou magistrats, habilités à demander l'enregistrement de ces empreintes génétiques.

Les mesures de sécurité physiques et logiques

Les moyens informatiques permettant de faire fonctionner le FNAEG sont installés dans les locaux de la Sous-direction de la police scientifique et technique, qui font l'objet de mesures strictes de sécurité physique.

Chaque utilisateur dispose d'un code d'accès personnel et les consultations du FNAEG font l'objet d'un suivi informatique, conformément à l'article R. 53-18, dernier alinéa, du Code de procédure pénale. En outre, les demandes de rapprochement à l'initiative des officiers de police judiciaire seront effectuées par l'intermédiaire des réseaux privés sécurisés des ministères de l'Intérieur et de la Défense.

La Commission considère que ces mesures apparaissent de nature à garantir la sécurité et la confidentialité du fichier comme des donnés qui y sont enregistrées.

Prend acte des propositions du ministère de la Justice :
– de préciser à l'article 3 du projet de décret (article R. 53-10 I 5°nouveau du Code de procédure pénale) que l'accord des ascendants ou descendants d'une personne disparue doit être recueilli par procès-verbal et que ceux-ci peuvent autoriser, par une mention expresse à ce même procès-verbal, l'utilisation de leurs empreintes génétiques à des fins d'identification et de recherche des auteurs d'infractions ;
– de préciser à l'article 4 du projet de décret (article R. 53-11 I 5°nouveau du Code de procédure pénale) que l'information relative à la nature de l'affaire justifiant l'enregistrement au fichier d'une empreinte génétique ne peut apparaître en cas de consultation ni servir de critère de recherche nominative ;

– de compléter l'article 6 du projet de décret (article R. 53-13 nouveau du Code de procédure pénale) pour prévoir expressément que les empreintes génétiques inscrites dans le fichier ne peuvent êtres réalisées que sur la partie non codante de l'ADN.

Demande que :

– le FNAEG soit structuré de telle façon que les données concernant les ascendants et les descendants de personnes disparues ayant limité l'utilisation de leurs empreintes génétiques aux seules fins de recherche de la personne disparue concernée puissent être traitées et consultées de façon distincte ;

– soit prévue une modulation des durées de conservation des informations dans le fichier, qu'elles concernent les condamnés ou les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55, tenant compte de la gravité et de la nature de l'infraction concernée ;

– s'agissant de cette dernière catégorie de personnes, la durée de conservation des informations enregistrées dans le fichier ne puisse excéder vingt-cinq ans, y compris pour les personnes ayant fait l'objet d'une décision de classement sans suite, de non-lieu, de relaxe ou d'acquittement exclusivement fondée sur l'existence d'un trouble mental ;

– l'article 7 (article R. 53-13-1 nouveau du Code de procédure pénale) du projet de décret soit complété afin de préciser que si la procédure judiciaire a mis hors de cause la personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait commis l'une des infractions visées à l'article 706-55 du Code de procédure pénale, notamment en permettant l'identification du coupable des faits dont elle est soupçonnée, l'effacement des informations la concernant dans le FNAEG devra être ordonné, y compris d'office ; que la circulaire d'application de ces dispositions réglementaires lui soit soumise ;

– l'article 9 du projet de décret (article R. 53-18 nouveau du Code de procédure pénale) soit complété par la mention des officiers et des agents de police judiciaire agissant au titre de l'article 706-56 I du Code de procédure pénale, dans le cadre et les limites des procédures qu'ils diligentent, et par l'indication de la nature des seules informations accessibles à ces personnels ;

– l'article 13 du projet de décret soit complété de façon à préciser que les résultats des analyses d'identification par empreintes génétiques obtenus avant l'entrée en vigueur du décret ne peuvent être enregistrées, selon les cas visés à l'article R. 53-10, que sur décision de l'officier de police judiciaire, agissant soit d'office soit à la demande du procureur de la République ou du juge d'instruction, ou encore sur décision du procureur de la République ou du procureur général.

Émet dans ces conditions **un avis favorable** au projet de décret modifiant le Code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques.

Délibération n° 03-065 du 16 décembre 2003 portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par la mairie de Levallois-Perret, destiné à contrôler l'accès au « roller-parc » par la reconnaissance des empreintes digitales

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le député-maire de Levallois-Perret, en application de l'article 15 de la loi du 6 janvier 1978, d'un projet d'arrêté portant création d'un traitement de gestion des accès au « roller-parc » ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu M. Maurice Benassayag, commissaire en son rapport et Mme Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

La direction des sports de la mairie de Levallois-Perret met en œuvre un traitement automatisé d'informations nominatives de contrôle de l'accès des abonnés au « roller-parc », recourant à un dispositif de reconnaissance des empreintes digitales.

La mairie fait valoir que l'utilisation d'un procédé biométrique permet d'éviter les difficultés liées à l'utilisation de cartes d'accès, lesquelles sont généralement oubliées, perdues, volées, échangées et ainsi d'assurer la sécurité des équipements récemment installés.

Le système repose sur la création d'une part d'un fichier des abonnés au « roller-parc » comportant les nom, prénom, date de naissance, adresse, numéro de téléphone ainsi qu'un numéro d'ordre chronologique, d'autre part, d'une base de données contenant l'enregistrement des caractéristiques des empreintes d'un doigt de la personne associé au numéro d'ordre chronologique.

Cette base de données biométriques est centralisée à la direction des sports et reliée, via le réseau téléphonique commuté, à un boîtier de stockage situé à l'entrée du « roller-parc ». En pratique, l'abonné désireux d'accéder aux équipements doit poser son doigt sur le lecteur d'empreintes digitales associé au boîtier. La reconnaissance de l'empreinte déclenche l'ouverture du tourniquet à l'entrée.

Les empreintes digitales sont des données biométriques qui « laissent des traces » pouvant ensuite être exploitées à des fins d'identification de personnes. Dès lors la constitution et l'utilisation de bases de données nominatives associées à des empreintes digitales, même limitée à la comparaison des empreintes aux seules fins de contrôle d'accès à des locaux ou à des services, comportent un risque d'atteinte aux libertés individuelles dans la mesure où elle est susceptible d'être utilisée à des fins étrangères à la finalité initialement poursuivie.

La Commission estime en conséquence que la constitution de bases de données d'empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles de ces bases de données, ne peut être admise que dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse.

Or, en l'espèce, l'objectif invoqué par la mairie de se doter d'un dispositif évitant la manipulation de cartes pour gérer les accès ne justifie pas la conservation dans une base de données des empreintes digitales des personnes fréquentant le « roller-parc ». En conséquence, le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné à l'objectif poursuivi.

Émet un avis défavorable au projet d'arrêté présenté par la mairie de Levallois-Perret.

Collectivités locales

Délibération n° 03-030 du 27 mai 2003 relative à la demande d'avis présentée par la communauté urbaine de Lyon concernant la constitution d'un traitement automatisé de données nominatives ayant pour finalité l'envoi d'informations aux Lyonnais habitant Paris et la région parisienne

La Commission nationale de l'informatique et des libertés ;

Saisie par la communauté urbaine de Lyon d'un projet d'arrêté relatif à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité l'envoi d'informations sur les manifestations économiques et culturelles organisées par la communauté urbaine de Lyon aux personnes d'origine lyonnaise domiciliées à Paris et en région parisienne ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil de l'Union européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret nº 78-774 du 17 juillet 1978 ;

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La communauté urbaine de Lyon a mis en œuvre une application dénommée « Lyopar » qui a pour objectif de gérer les contacts créés avec les personnes originaires de l'agglomération lyonnaise qui sont domiciliées à Paris et en Ile-de-France dans le but de les informer de toutes les manifestations culturelles et économiques réalisées sur le territoire du grand Lyon.

Les noms et adresses figurant dans le fichier sont communiqués par les personnes elles-mêmes, préalablement informées par des encarts dans la presse ou par une information diffusée dans certaines grandes entreprises.

Les noms et adresses proviennent également de la liste électorale de Paris obtenue auprès de la préfecture de police de Paris et d'annuaires d'établissements d'enseignement supérieur privés, contactés à cet effet par la délégation parisienne.

À partir de la liste électorale, la délégation parisienne procède à un tri informatique en fonction du lieu de naissance (Lyon et les cinquante-quatre communes de l'agglomération) de façon à ce que ne soient envoyées des informations qu'aux personnes concernées par les activités de la communauté urbaine de Lyon.

La Commission estime qu'un tel tri informatique à partir de la liste électorale, destiné à isoler une catégorie d'électeurs en fonction de leur lieu de naissance, n'est pas justifié au regard du principe de finalité de la liste électorale qui ne comporte une telle information qu'afin de s'assurer de l'identité de l'électeur et d'éviter les fraudes au scrutin. Elle estime en conséquence qu'un tel tri n'est pas conforme à la loi.

La Commission considère, par ailleurs, que la délégation parisienne doit prendre toutes mesures de nature à s'assurer auprès des établissements d'enseignement supérieur que les informations qu'ils lui communiquent, à partir des annuaires des anciens élèves, sont bien expurgées des noms et adresses des personnes ayant refusé que leurs coordonnées soient cédées. La délégation parisienne devra, en outre, recueillir l'accord des personnes contactées, à partir des informations fournies par ces établissements, pour figurer dans son fichier, après les avoir informées de l'origine des données utilisées.

Enfin, les personnes dont les coordonnées figurent dans le fichier doivent être informées de l'origine des données nominatives utilisées les concernant ainsi que de leur droit d'accès, de rectification et de suppression, en particulier par des mentions apposées sur les courriers qui leur sont adressés.

Par ces motifs, **émet un avis favorable** au projet d'arrêté présenté par la communauté urbaine de Lyon sous réserve :
– qu'il ne soit pas procédé au tri de la liste électorale de Paris sur la base du lieu de naissance et que toute information de cette nature soit effacée ;
– que l'article 1er du projet d'acte réglementaire énumère l'origine des fichiers utilisés pour la constitution du traitement ;
– que la délégation parisienne s'assure auprès des établissements d'enseignement supérieur qu'elle contacte que les informations communiquées à partir des annuaires d'anciens élèves sont expurgées des personnes ayant refusé la cession de leurs coordonnées et qu'elle recueille l'accord des personnes contactées pour figurer dans le fichier après les avoir informées de l'origine des données utilisées ;
– que toutes les personnes dont les coordonnées figurent dans le fichier soient informées de leur droit d'accès, de rectification et de suppression.

Commerce

Délibération n° 03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance

La Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pris ensemble le décret d'application du 17 juillet 1978 ;

Vu l'article 9 du Code civil ;

Vu l'article L. 121-16 du Code de la consommation ;

Vu les articles 225-1 à 225-3 ; 226-1 et 226-16 à 226-24 du Code pénal ;

Vu la recommandation nº R (90) 19 du Conseil de l'Europe relative à la protection des données à caractère personnel à des fins de paiement et autres opérations connexes ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport et Madame Catherine Pozzo di Borgo, commissaire-adjoint du Gouvernement, en ses observations ;

La présente recommandation concerne le stockage et l'utilisation du numéro de carte bancaire collecté par un professionnel à l'occasion de la vente d'un bien ou la fourniture d'une prestation de service conclue, sans la présence physique simultanée des parties, entre lui-même et un consommateur qui, pour la conclusion de ce contrat, utilisent une ou plusieurs techniques de communication à distance.

Par numéro de carte bancaire, il faut entendre le numéro et la date de validité figurant sur le recto des cartes de paiement « CB » émises par les banques utilisables chez les commerçants et prestataires de services affiliés au réseau « CB ». La présente recommandation ne s'applique donc ni aux cartes dites privatives, c'est-à-dire aux cartes émises par les établissements financiers spécialisés dans le crédit à la consommation ou encore directement par des commerçants, ni aux cartes dites accréditives.

La présente recommandation a pour objet, en l'état du droit et des procédés actuels de paiement, notamment sur Internet, de préciser les garanties minimales à respecter lors de la mise en œuvre, par les professionnels, de traitements afférents au numéro de carte bancaire.

Sur la finalité liée à la collecte et l'utilisation du numéro de carte bancaire et sur l'information des personnes

La Commission rappelle que :

– la collecte et la conservation du numéro de carte bancaire dans un traitement automatisé d'informations nominatives doivent s'effectuer dans le respect des disposi-

tions de l'article 5 de la convention n° 108 du Conseil de l'Europe, c'est-à-dire dans le respect de finalités déterminées et légitimes ;
– le traitement automatisé du numéro de carte bancaire doit faire l'objet d'une déclaration à la CNIL décrivant avec précision la finalité poursuivie, dans les conditions prévues à l'article 16 de la loi du 6 janvier 1978. Le manquement à cette obligation est constitutif d'une infraction pénale (article 226-17 du Code pénal) ;
– la finalité première de l'utilisation d'un numéro de carte bancaire est la réalisation d'une transaction, qu'elle soit ponctuelle ou à exécutions successives, c'est-à-dire le complet paiement d'un prix en contrepartie de la délivrance d'un bien ou la prestation d'un service.

La Commission relève néanmoins que, loin de rester un simple instrument de paiement, le numéro de carte bancaire est parfois devenu un véritable identifiant, utilisé à des fins commerciales au-delà de la réalisation d'une transaction donnée (« portefeuille électronique », authentification d'un client, réservation par téléphone, etc.) ou de lutte contre la fraude au paiement.

Nonobstant la légitimité ou l'intérêt que ces pratiques nouvelles peuvent parfois revêtir, la Commission constate que les personnes ne sont pas ou peu informées sur l'existence de ces pratiques et qu'elles leur sont la plupart du temps imposées.

La Commission recommande en conséquence que l'utilisation du numéro de carte bancaire à des fins d'identification commerciale soit subordonnée, lorsque ce numéro est conservé au-delà du temps nécessaire à la réalisation de la transaction, au recueil du consentement de la personne concernée. Elle rappelle que, conformément aux termes de la directive 95/46 du 24 octobre 1995, le consentement est toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données la concernant fassent l'objet d'un traitement.

La Commission constate par ailleurs que la spécificité du paiement par carte bancaire dans la vente à distance fait peser le risque financier sur le commerçant en cas d'utilisation frauduleuse du numéro de carte.

La Commission considère en conséquence que l'utilisation du numéro de carte bancaire par un professionnel de la vente à distance dans un fichier ayant pour finalité de lutter contre la fraude au paiement en conservant la trace d'agissements lui ayant porté préjudice, est légitime, sous la réserve que ce fichier ait fait l'objet d'une déclaration spécifique à la Commission et soit conforme aux lois et règlements en vigueur, en particulier aux dispositions relatives à l'informatique et aux libertés, et que cette utilisation du numéro de carte bancaire soit subordonnée à une information claire des personnes fichées ainsi qu'à la possibilité pour ces personnes de s'opposer, pour des motifs légitimes, à un tel traitement.

La CNIL rappelle qu'en application de l'article 2 de la loi du 6 janvier 1978, aucune décision privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

De plus, l'utilisation du numéro de carte bancaire à des fins de lutte contre la fraude au paiement ne saurait aboutir à une discrimination ou un refus de vente, même si elle peut conduire légitimement le commerçant à refuser ce mode de paiement.

S'agissant de l'information des personnes, la CNIL rappelle aussi que :
– en application de l'article 27 de la loi du 6 janvier 1978 les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées du caractère obligatoire ou facultatif des réponses ; des conséquences à leur égard d'un défaut de réponse ; des personnes physiques ou morales destinataires des informa-

tions ; de l'existence d'un droit d'accès et de rectification. Lorsque de telles informations sont recueillies par voie de questionnaires, ceux-ci doivent porter mention de ces prescriptions ;
– il résulte en outre de l'article 10 de la directive 95-46 du 24 octobre 1995 que les personnes fichées doivent également être informées de l'identité du responsable du traitement ainsi que les finalités du traitement auquel les données sont destinées ;
– il résulte de l'article 26 de la loi du 6 janvier 1978 que toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement. Ce droit d'opposition, en particulier sur internet, devrait pouvoir s'exercer facilement, par exemple au moyen d'une case à cocher ;
– l'article 25 de la loi du 6 janvier 1978 dispose que la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite.

La Commission souligne en conséquence que toute utilisation du numéro de carte bancaire, quelle qu'en soit la finalité, doit faire l'objet d'une information complète et claire auprès de la personne fichée.

Sur la sécurité des traitements

La Commission observe que les pratiques liées à la collecte du numéro de carte bancaire entraînent la multiplication de bases de données pouvant faire l'objet d'une réutilisation frauduleuse, en particulier lorsque ces bases de données sont accessibles sur internet.

La Commission considère en conséquence que les commerçants devraient s'efforcer d'élaborer et d'adopter des pratiques exemplaires et de promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des individus.

À cet égard, la Commission rappelle que :
– en application de l'article 17 de la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ;
– ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. Le non-respect de l'obligation de sécurité est sanctionné par l'article 226-17 du Code pénal ;
– s'agissant de l'appel à des prestataires de services, le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et doit veiller au respect de ces mesures. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et que les obligations en matière de sécurité, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci.

La Commission considère en conséquence que les responsables de traitements devraient prendre les mesures organisationnelles et techniques appropriées

afin de préserver la sécurité, l'intégrité et la confidentialité des numéros de cartes bancaires contre tout accès, utilisation, détournement, communication ou modification non autorisés.

La Commission relève par ailleurs que le développement de solutions de paiement sécurisées par carte à puce permettrait de garantir un niveau de sécurité optimal tout en limitant la constitution de bases de données de numéros de cartes bancaires, en particulier à des fins de contrôle.

Ceci étant rappelé, elle recommande que :
– les responsables de traitements utilisent uniquement des systèmes de paiement en ligne sécurisés conformes à l'état de l'art et à la réglementation applicable ;
– les responsables de traitements ne mémorisent pas les informations relatives au cryptogramme visuel (CVV2) de la carte bancaire de leurs clients ;
– s'agissant des mesures organisationnelles propres aux responsables de traitement, ces derniers adoptent une politique de gestion stricte des habilitations de leur personnel ne donnant accès au numéro de carte bancaire des clients que lorsque cela est rigoureusement nécessaire et aux seules personnes exerçant des fonctions liées à la finalité déclarée. Les responsables devraient s'assurer que les numéros de cartes bancaires apparaissent toujours de façon tronquée sur l'écran des salariés habilités (seuls les cinq derniers chiffres restent apparents). Le personnel devrait être sensibilisé aux risques de fraudes existant en la matière ;
– dès lors que le numéro de carte bancaire est enregistré dans une base de donnée, les commerçants aient recours à des procédés techniques permettant de crypter de manière irréversible le numéro de la carte bancaire dès que la transaction a été réalisée ;
– les responsables de traitements portent une attention particulière aux risques qu'il y aurait à mémoriser le numéro de carte bancaire dans l'ordinateur personnel du client, en particulier par l'intermédiaire de « cookies » ou fichiers « log ». Dans une telle situation, et conformément aux dispositions prévues par la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, les individus doivent être informés de la mise en œuvre de dispositifs techniques sur leur ordinateur et doivent disposer de la possibilité de s'opposer à la mise en œuvre de tels dispositifs. L'exercice du droit d'opposition devrait pouvoir couvrir les utilisations futures qui pourraient être faites de ces dispositifs durant des connexions ultérieures ;
– s'agissant de la mise en place de système d'authentification en ligne, permettant d'accéder directement à un profil client et à des coordonnées bancaires (« portefeuille électronique »), les commerçants informent clairement leurs clients sur les risques induits par certains gestionnaires de mots de passe intégrés à des navigateurs internet et leur préciser la méthode permettant de désactiver ces systèmes.

Sur la durée de conservation

La Commission rappelle que :
– la conservation du numéro de carte bancaire dans un traitement automatisé d'informations nominatives doit s'effectuer dans le respect des dispositions posées par l'article 5-e de la convention nº 108 du Conseil de l'Europe, c'est-à-dire pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles l'information est exigée. Cette durée doit faire l'objet d'une déclaration à la Commission. Le fait de conserver cette information au-delà de la durée prévue dans la déclaration est constitutif d'une infraction pénale (article 226-20 du Code pénal) ;

– toute conservation du numéro de carte bancaire d'un client suppose que des mises à jour régulières soient effectuées afin de supprimer les numéros de cartes bancaires périmés.

La Commission relève qu'aucun texte de portée générale relatif à la conservation de documents comptables à des fins probatoires ne fait obligation aux responsables de traitements de conserver le numéro de carte bancaire de leurs clients.

La Commission considère en conséquence que la durée de conservation d'un numéro de carte bancaire ne saurait excéder le délai nécessaire à la réalisation de la transaction ou à la finalité de lutte contre la fraude au paiement du traitement mis en œuvre conformément aux lois et règlement en vigueur.

Sur ce point, la Commission souligne que chaque déclaration fait l'objet d'un examen spécifique et que le projet de loi modifiant la loi du 6 janvier 1978 (transposition de la directive du 24 octobre 1995) prévoit, en l'état de son examen par le Parlement, que seront soumis à l'autorisation de la CNIL *« les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure les personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire les y habilitant »*.

Sur le choix du mode de paiement électronique

La Commission relève que l'utilisation de traitements automatisés de données dans le secteur des moyens de paiement peut entraîner des risques pour la vie privée des individus, s'agissant en particulier de certains modes de paiement électronique, au regard de la quantité de données à caractère personnel qu'ils peuvent révéler du fait de leur utilisation.

La Commission estime en conséquence que les responsables de traitements devraient promouvoir, pour le commerce électronique, l'utilisation de moyens de paiement électronique sécurisés alternatifs garantissant l'anonymat des paiements réalisés par leurs clients.

Enseignement

Délibération n° 03-013 du 27 mars 2003 portant avis sur le projet d'arrêté présenté par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche concernant la modification du traitement SISE

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche, en application de l'article 15 de la loi du 6 janvier 1978, d'un projet d'arrêté concernant le système d'information sur le suivi des étudiants, dénommé SISE ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière statistique ;

Vu le décret nº 78-774 du 17 juillet 1978, modifié, pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu l'arrêté du ministre de l'Enseignement supérieur et de la Recherche en date du 12 décembre 1994 portant création du traitement SISE ;

Vu le projet d'arrêté présenté par le ministre de la Jeunesse, de l'Éducation nationale et de la Recherche portant modification du traitement SISE et abrogeant l'arrêté précité de 1994 ;

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche a saisi la CNIL d'une demande d'avis modificative du traitement automatisé de données individuelles dénommé « système d'information sur le suivi des étudiants » (SISE), géré par la direction de la programmation et du développement, service statistique ministériel.

Le traitement SISE, créé par l'arrêté du 12 décembre 1994, a pour objet de permettre au ministère de disposer de données fiables et cohérentes sur les élèves et les étudiants des établissements d'enseignement supérieur en vue de la répartition des moyens, de l'établissement de statistiques et d'études prospectives et longitudinales.

Le système SISE enregistre les données individuelles que lui transmettent les établissements d'enseignement supérieur et qui sont les suivantes : l'identifiant national étudiant (INE), le sexe, l'année de naissance, la situation de famille, la nationalité, la profession et la catégorie socioprofessionnelle des parents et de l'étudiant, le type d'hébergement de l'étudiant, le type d'aide reçue, le département de résidence

des parents, les modalités d'entrée et d'inscription dans l'enseignement supérieur (série du baccalauréat et année d'obtention, équivalence, année et établissement de première inscription, formation initiale et continue), le cursus suivi et les diplômes acquis, l'inscription et le résultat au diplôme.

L'identifiant national (INE) attribué à chaque étudiant par le ministère en 1993, conformément aux recommandations de la Commission, comporte onze caractères dont un code géographique caractérisant sur deux caractères l'académie d'immatriculation, l'année d'attribution du numéro en deux caractères, un numéro d'ordre séquentiel en six caractères, la clé de contrôle du code en un caractère.

La première modification du traitement, sollicitée par le ministère, vise à permettre aux services statistiques des rectorats de disposer de l'intégralité du fichier national de données individuelles SISE. Les données transmises seront donc celles énumérées par l'article 2 de l'arrêté de décembre 1994 susvisé.

La transmission de ces informations à des fins exclusives d'études statistiques ayant trait notamment aux migrations inter-académiques, aux parcours des élèves passés dans l'enseignement supérieur doit contribuer à une meilleure connaissance du dispositif national de l'enseignement supérieur et à la mise en œuvre de décisions appropriées. Elle s'inscrit enfin dans le cadre défini par la loi susvisée du 7 juin 1951.

Le ministère prévoit également que les établissements publics d'enseignement supérieur sous sa tutelle pourront être destinataires d'un extrait du traitement SISE avec cryptage du numéro INE et agrégation de la nationalité. Il conviendra que le procédé de cryptage soit soumis à la Commission lorsqu'il sera arrêté.

La seconde modification présentée consiste à autoriser le service statistique de l'administration centrale, la direction de la programmation et du développement ainsi que les services statistiques des rectorats à conserver les données individuelles obtenues pendant une durée n'excédant pas dix ans. Un historique des données sur une période d'au moins dix ans est en effet de nature à permettre la réalisation d'études statistiques sur la population concernée. Ce délai est pertinent compte tenu de la longueur des cursus universitaires et des réorientations possibles.

Émet un avis favorable au projet d'arrêté relatif au traitement SISE soumis à la Commission.

Délibération n° 03-037 du 16 septembre 2003 relative à la demande d'avis présentée par le ministère de l'Éducation nationale concernant le traitement « I-prof » proposant à chaque enseignant un ensemble de services internet sécurisés et personnalisés relatifs à sa carrière administrative

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche d'un projet d'arrêté portant création d'un traitement automatisé d'informations nominatives (demande d'avis nº 854083) ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu Monsieur Hubert Bouchet, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les finalités poursuivies

Dans le cadre de son programme dénommé « bureau virtuel » destiné à promouvoir l'accès aux technologies de l'information et de la communication auprès de ses personnels, le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche a saisi la Commission d'une demande d'avis concernant un traitement automatisé d'informations nominatives dénommé « I-Prof ».

Ce traitement permet à tout enseignant de bénéficier, via un point d'entrée unique, personnalisé et sécurisé, d'un bouquet de services comprenant :
– l'accès aux données professionnelles et administratives le concernant, actuellement disponibles dans les bases de données informatisées de gestion des personnels de l'éducation nationale (« AGAPE » pour le premier degré et « EPP » pour le second degré) ;
– la possibilité de signaler des erreurs dans les informations contenues dans la partie administrative du dossier ;
– la possibilité de compléter les informations le concernant dans la partie *curriculum vitae* du dossier et d'éditer le *curriculum vitae* ;
– l'accès aux procédures d'administration électronique (opérations de promotion, de mutation, de formation…), « I-Prof » constituant un portail vers les applications internet actuelles dédiées à ces opérations et qui ont succédé aux services télématiques ;
– l'accès aux résultats des actes de gestion le concernant ;
– la consultation des textes juridiques de référence et des guides concernant la carrière et le métier d'enseignant ;

– l'accès à une messagerie électronique avec un gestionnaire attitré permettant une information personnalisée en temps réel concernant tout élément de sa vie administrative et professionnelle.

L'application « I-Prof », s'appuyant sur des bases de données académiques, est constituée de deux modules, l'un dit « enseignants », l'autre dit « gestionnaires et inspecteurs ».

Le premier module est accessible par internet (site extranet) à partir de n'importe quel ordinateur. Ainsi, un enseignant peut se connecter à « I-Prof » de son domicile ou à partir des points d'accès à internet disponibles dans chaque établissement.

Le second module, non accessible via internet, est accessible soit à partir d'un poste de travail installé dans les locaux des services académiques, soit par un poste extérieur.

La Commission estime légitimes les objectifs poursuivis dans le cadre de l'outil « I-Prof ».

Sur la pertinence des données enregistrées

La Commission prend acte du fait que les données accessibles dans le cadre de « I-Prof » se limitent aux données de gestion des dossiers administratifs des enseignants extraites des applications « AGAPE » et « EPP » de gestion des personnels du premier et du second degrés, ainsi qu'aux données complémentaires librement communiquées par l'enseignant concerné.

Sur les destinataires des données enregistrées

Les destinataires des informations enregistrées dans « I-Prof » sont les enseignants concernés et les inspecteurs de l'éducation nationale (à l'exception des messages électroniques) ainsi que les inspecteurs d'académie inspecteurs pédagogiques régionaux (à l'exception des messages électroniques) qui, les uns et les autres, sont déjà destinataires des données des applications « AGAPE » et « EPP ».

Comme pour « AGAPE » et « EPP », sont également destinataires des informations enregistrées dans « I-Prof » les gestionnaires des personnels qui sont les gestionnaires administratifs des personnels enseignants du premier degré (en inspections académiques) et du second degré (rectorats) et les personnels de la direction des personnels enseignants du ministère de la Jeunesse, de l'Éducation nationale et de la Recherche gérant les personnels détachés et affectés à l'étranger. Au titre de la gestion intégrée des personnels, ils ont accès à l'ensemble des données concernant les personnels dont ils ont la charge.

La Commission estime légitimes les habilitations d'accès ainsi définies dans le cadre de « I-Prof ».

Sur les durées de conservation des données

Les informations sont accessibles sur l'extranet « I-Prof » jusqu'à la fin de l'année scolaire suivant le départ de l'enseignant.

S'agissant des éléments composant la rubrique *« curriculum vitae »*, leur conservation est laissée à la libre appréciation de l'agent.

Enfin, le contenu de la rubrique « messagerie électronique » est conservé sur deux années scolaires au plus.

La Commission considère ces durées de conservation comme non excessives.

Sur les mesures prises pour garantir la confidentialité des données

Plusieurs procédés sont mis en œuvre pour assurer l'authentification des utilisateurs et des serveurs de l'application « I-Prof », ainsi que le chiffrement et l'intégrité des données.

En particulier, l'accès à distance des gestionnaires et inspecteurs aux informations par un poste dit « nomade » est notamment sécurisé par un dispositif s'appuyant sur une « clé USB » – support physique doté d'un port de communication USB permettant la connexion de la clé sur tout ordinateur du marché – contenant un logiciel support d'un certificat associé à un code PIN que doit composer l'utilisateur pour se connecter à « I-Prof ».

En outre, les connexions à « I-Prof » sont journalisées afin de permettre un contrôle *a posteriori* des accès à l'application.

La Commission relève cependant que le procédé actuel d'authentification de « I-Prof » basé sur un « login » et un mot de passe paraît insuffisant dans la mesure où il n'est prévu aucun contrôle de la longueur minimale du mot de passe, aucune fréquence de renouvellement obligatoire, ni aucune interdiction d'utiliser les derniers mots de passe.

La Commission recommande en conséquence la définition de règles en ce domaine ou la généralisation d'un procédé assurant l'authentification des utilisateurs de « I-Prof » tel que, par exemple, le dispositif de « clé USB » déjà mis en œuvre dans le cadre du module « gestionnaires et inspecteurs ».

Sur le droit d'accès et de rectification, le droit d'opposition, et l'information des personnels enseignants

La Commission observe que, de par sa finalité et son mode de fonctionnement, le traitement « I-Prof » est de nature à faciliter l'exercice du droit d'accès et de rectification des enseignants aux données nominatives qui les concernent.

Elle relève également qu'il n'est en aucun cas fait obligation aux enseignants de se connecter à « I-Prof », de consulter ou de compléter leur dossier. En ce sens, toutes les procédures administratives et de gestion peuvent être réalisées par l'enseignant sur support papier.

De plus, les enseignants disposent de la possibilité de s'opposer, à tout moment, à la mise en ligne sur l'extranet des informations les concernant. La Commission prend acte du fait que l'exercice de ce droit ne pourra porter sur une rubrique particulière de « I-Prof », mais uniquement sur l'ensemble du dossier de l'enseignant exerçant son droit d'opposition.

Elle considère toutefois nécessaire de rappeler au ministère de la Jeunesse, de l'Éducation nationale et de la Recherche son obligation d'informer très clairement les personnels enseignants sur les objectifs poursuivis par la mise en œuvre de ce dispositif, sur les destinataires des informations enregistrées, et sur leur droit de faire compléter ou rectifier les données les concernant, mais également de s'opposer à la mise en ligne de leur dossier dans l'outil « I-Prof ».

Émet un avis favorable au projet d'arrêté présenté par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche portant création du traitement « I-Prof ».

Recommande au ministère de renforcer les mesures envisagées afin d'assurer la sécurisation des accès à l'application « I-Prof » par la définition de règles

visant à mieux encadrer l'utilisation des mots de passe ou par la généralisation d'un procédé assurant l'authentification des utilisateurs de « I-Prof » tel que, par exemple, le dispositif de « clé USB » déjà mis en œuvre dans le cadre du module « gestionnaires et inspecteurs ».

Demande à être saisie dans le délai d'un an des mesures retenues par le ministère afin de répondre à cet objectif de renforcement de l'authentification des utilisateurs de « I-Prof ».

Rappelle au ministère son obligation de procéder à une parfaite information des personnels enseignants sur les objectifs poursuivis par la mise en œuvre de ce dispositif, sur les destinataires des informations enregistrées et sur leur droit de faire compléter ou rectifier les données les concernant mais également de s'opposer à la mise en ligne de leur dossier dans l'extranet « I-Prof ».

Étrangers

Délibération n° 03-015 du 24 avril 2003 portant avis sur les articles 4 et 5 d'un projet de loi relatif à l'immigration

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis, en application de l'article 20 du décret n° du 17 juillet 1978, du projet de loi relatif à l'immigration ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention d'application de l'Accord de Schengen du 14 juin 1985, signée à Schengen le 19 juin 1990 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu l'ordonnance n° 45-2658 du 20 novembre 1945 modifiée relative aux conditions d'entrée et de séjour des étrangers en France, et notamment son article 8 -3 ;

Vu la décision du Conseil constitutionnel n° 97 -389 DC du 22 avril 1997 relative à la loi du 25 avril 1997 ;

Après avoir entendu Monsieur François Giquel, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Émet l'avis suivant :

L'article 4 du projet de loi complète le premier alinéa de l'article 8-3 de l'ordonnance du 2 novembre 1945 et a pour objet d'étendre les cas dans lesquels les empreintes digitales des ressortissants étrangers, non ressortissants d'un État membre de l'Union européenne, peuvent être relevées, mémorisées et faire l'objet d'un traitement automatisé.

Les dispositions actuelles de cet article, introduites dans l'ordonnance du 2 novembre 1945 par la loi du 24 avril 1997, prévoient que les empreintes digitales des étrangers non ressortissants d'un État membre de l'Union européenne qui sollicitent la délivrance d'un titre pour un séjour de plus de trois mois ainsi que celles des étrangers qui sont en situation irrégulière en France ou qui font l'objet d'une mesure d'éloignement du territoire français, peuvent être relevées, mémorisées et faire l'objet d'un traitement automatisé dans les conditions fixées par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elles n'ont reçu aucune application à ce jour.

Le deuxième alinéa du même article institue la possibilité pour les agents expressément habilités du ministère de l'Intérieur ou de la gendarmerie de consulter, dans les conditions fixées par la loi du 6 janvier 1978, le fichier automatisé des empreintes digitales (FAED), géré par le ministère de l'Intérieur, afin d'identifier les étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement qui n'auraient pas présenté les pièces justificatives nécessaires.

La modification envisagée par l'article 4 du projet de loi a pour objet d'étendre la possibilité de prise d'empreintes digitales et de leur traitement aux étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière en provenance d'un pays tiers, ne sont pas munis des documents et visas d'entrée exigés en application de l'article 5 de l'ordonnance du 2 novembre 1945 ou ne remplissent pas les conditions d'entrée sur le territoire des parties contractantes pour un séjour n'excédant pas trois mois, prévues à l'article 5 de la convention signée à Schengen le 19 juin 1990.

L'article 5 du projet de loi introduit un nouvel article 8-4 dans l'ordonnance du 2 novembre 1945 aux termes duquel les empreintes digitales des étrangers non ressortissants de l'Union européenne qui sollicitent la délivrance, auprès d'un consulat ou à la frontière, d'un visa afin de séjourner dans un État membre de l'Union européenne, pourront être relevées, mémorisées et faire l'objet d'un traitement automatisé dans les conditions fixées par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La Commission rappelle d'abord que, conformément aux principes généraux de la protection des données à caractère personnel et à l'article 5 de la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 susvisée, un traitement automatisé d'informations nominatives ne peut être mis en œuvre que pour *« des finalités déterminées et légitimes »*, les données enregistrées devant être adéquates, pertinentes et non excessives par rapport à ces finalités.

Elle estime dès lors que le projet de loi devrait clairement indiquer les finalités pour lesquelles il pourra être procédé à des traitements automatisés d'empreintes digitales des étrangers non ressortissants de l'Union européenne.

En tout état de cause, la Commission tient pour légitime le recours, pour s'assurer de l'identité d'une personne, à des dispositifs de reconnaissance biométrique dès lors que la donnée biométrique est conservée sur un support dont la personne a l'usage exclusif.

En revanche, elle considère que la mémorisation et le traitement de données issues des empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données qui pourraient ainsi être constituées, doivent être justifiés par des exigences impérieuses en matière de sécurité ou d'ordre public.

Il convient aussi que des garanties appropriées soient prises pour assurer le respect des droits et libertés individuelles, et ce d'autant plus que ces bases de données d'empreintes digitales seraient susceptibles de concerner à court terme plusieurs millions de personnes, puisque, par exemple, le nombre de demandes de visa reçues par le ministère des affaires étrangères atteint aujourd'hui près de trois millions par an.

Au nombre de ces garanties, figure le respect des règles de protection des données à caractère personnel telles que fixées par la convention n° 108 du Conseil de l'Europe et par la loi du 6 janvier 1978, et en particulier, l'obligation de ne conserver les données que pendant une durée n'excédant pas celle nécessaire aux finalités poursuivies, la nécessité de préserver la confidentialité de ces données et de ne les communiquer qu'aux personnes autorisées à en connaître, le respect de l'exercice du droit d'accès de chacun aux informations le concernant.

Ainsi la Commission estime que l'accès aux traitements d'empreintes digitales, eu égard à la sensibilité des données qui y seraient conservées, devrait être strictement réservé à un nombre limité de personnes expressément habilitées à cet effet et que des mesures particulières de sécurité devraient être adoptées pour éviter toute

utilisation détournée des informations, compte tenu non seulement de la dimension des fichiers mais aussi de la répartition mondiale des postes consulaires.

Se référant d'autre part aux différents avis qu'elle a rendus en particulier sur le traitement de gestion, par le ministère de l'Intérieur, des dossiers des ressortissants étrangers (AGDREF) et sur le traitement de délivrance des visas (RMV2) mis en œuvre par le ministère des Affaires étrangères, la Commission rappelle que, compte tenu des conséquences graves que pourrait entraîner à l'égard des personnes concernées la conservation dans les traitements d'empreintes digitales, d'informations incomplètes ou périmées, s'agissant par exemple de personnes ayant acquis la nationalité française ou ayant régularisé leur situation en France, les durées de conservation des informations et les procédures de mise à jour et d'apurement de celles-ci devraient être précisément définies et rigoureusement appliquées.

Enfin, la Commission considère que l'exercice du droit d'accès constitue, pour les personnes appelées à figurer dans ces fichiers, une garantie fondamentale, leur permettant ainsi de vérifier l'exactitude des informations enregistrées sur leur compte et de les faire rectifier, voire supprimer le cas échéant si celles-ci s'avèrent inexactes ou périmées.

Elle estime en conséquence que la loi devrait renvoyer explicitement à un décret en Conseil d'État pris après avis de la CNIL les modalités d'application de chacun des deux articles du projet de loi, afin de préciser notamment les modalités d'habilitation des personnes pouvant accéder aux informations, la durée de conservation et les conditions de mise à jour des informations enregistrées et l'exercice de leur droit d'accès par les personnes concernées.

La Commission prend acte qu'aux termes des dispositions dont elle est saisie, les empreintes digitales des ressortissants étrangers sollicitant un visa feraient l'objet d'un traitement automatisé distinct de celui mis en œuvre pour l'enregistrement des empreintes digitales des ressortissants étrangers qui sollicitent la délivrance d'un titre de séjour, qui sont en situation irrégulière en France, ou qui font l'objet d'une mesure d'éloignement du territoire français. De la même façon, elles ne prévoient, en l'état, aucune mise en relation, rapprochement ou interconnexion entre ces traitements ou avec d'autres fichiers hormis ceux déjà prévus par la loi.

Seul le fichier automatisé des empreintes digitales (FAED), géré par le ministère de l'Intérieur, peut, aux termes de l'article 8-3 actuel, être consulté à des fins d'identification des étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement.

Enfin, la Commission constate que ces dispositions doivent s'intégrer, comme l'indique l'exposé des motifs, dans le cadre des travaux en cours au plan communautaire visant à systématiser l'introduction de données biométriques dans les passeports, les visas et les titres de séjour.

Le Conseil européen de Laeken, en décembre 2001, a en effet demandé au Conseil et aux États membres de prendre les dispositions nécessaires pour la mise en place d'un système commun d'identification des visas, qui permettrait de recenser dans une base unique les demandes et les refus de visas, afin notamment de lutter contre la fraude, d'améliorer la coopération consulaire, de déterminer plus aisément, aux postes de contrôle aux frontières extérieures ou lors des contrôles d'immigration ou de police, les usurpations d'identité, de faciliter l'application de la convention de Dublin sur le droit d'asile, de vérifier l'identité des personnes en situation irrégulière. À cet effet, certaines lignes directrices ont déjà été définies, parmi lesquelles l'intégration dans la base des photographies numérisées et d'autres données biométriques.

Dans la mesure où, d'une part, le système d'information national qui sera appelé à se mettre en place nécessitera l'instauration de nouveaux flux transfrontières de données au sein de l'espace Schengen et où, d'autre part, les dispositions communautaires ne sont pas encore définitivement arrêtées et qu'en particulier le dispositif biométrique qui sera utilisé n'est pas encore retenu, la Commission s'interroge sur la compatibilité du dispositif prévu par le projet de loi avec le futur système européen.

La Commission s'interroge aussi sur les conditions dans lesquelles les transmissions d'informations concernant les personnes appréhendées à l'occasion du franchissement irrégulier d'une frontière extérieure de l'Union européenne ainsi que les étrangers se trouvant illégalement sur le territoire d'un État membre, prévues au titre de l'article 8 du règlement du Conseil de l'Union européenne du 11 décembre 2000 concernant « la création du système EURODAC pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin », pourraient ou non être alimentées par les données biométriques recueillies en application des articles 4 et 5 du projet de loi. La Commission observe que le système EURODAC a pour seul objet d'établir l'identité des demandeurs d'asile et de permettre à un État de vérifier si un étranger se trouvant illégalement sur le territoire ou appréhendé à l'occasion du franchissement irrégulier d'une frontière extérieure de la Communauté a présenté une demande d'asile dans un autre État membre et que l'article 5 du règlement du Conseil du 28 février 2002 fixant certaines modalités d'application du règlement précité du 11 décembre 2000 prévoit expressément que la constitution de la base de données EURODAC doit être conçue de façon à séparer les données relatives aux personnes reconnues et admises comme réfugiés et les autres données.

La Commission considère en conséquence que si le dispositif prévu par le projet de loi avait vocation à être utilisé dans le cadre du système EURODAC, il y aurait lieu d'en faire mention à l'article 4 du projet de loi.

Famille

Délibération n° 03-007 du 4 février 2003 portant avis sur le projet de décret en Conseil d'État, présenté par le ministère de la Santé, de la Famille et des Personnes handicapées, pris en application de l'article L. 147-11 du Code de l'action sociale et des familles et portant création d'un traitement automatisé d'informations nominatives pour la gestion des missions du Conseil national pour l'accès aux origines personnelles

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de la Santé, de la Famille et des Personnes handicapées d'un projet de décret en Conseil d'État pris en application de l'article L. 147-11 du Code de l'action sociale et des familles et portant création d'un traitement automatisé d'informations nominatives (demande d'avis nº 841134) ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le Code de l'action sociale et des familles ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu Monsieur Pierre Schapira, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La loi du 22 janvier 2002 relative à l'accès aux origines des personnes adoptées et pupilles de l'État a introduit dans le Code de l'action sociale et des familles plusieurs dispositions visant à favoriser le rapprochement des enfants « nés sous x » et de leurs parents de naissance.

Afin de faciliter la réalisation de cet objectif, le législateur a notamment créé un Conseil national pour l'accès aux origines personnelles (CNAOP), chargé d'assumer un rôle actif dans les recherches entamées par les personnes « nées sous x » ou par leurs parents de naissance.

Le législateur a prévu qu'un décret pris après avis de la CNIL devait fixer les conditions dans lesquelles seraient traitées et conservées les informations susceptibles de révéler l'identité des parents biologiques ou des éléments non nominatifs de leur histoire personnelle.

La Commission est donc amenée à se prononcer sur les garanties apportées par le projet de décret qui lui est soumis par le ministère de la Santé, de la Famille et des Personnes handicapées en application de l'article L. 147-11 du Code de l'action sociale et des familles.

Ce projet de décret comporte également des dispositions portant création d'un traitement automatisé d'informations nominatives nécessaire à l'accomplissement des missions légales du CNAOP.

Sur les dispositions du projet de décret prises en application de l'article L. 147-11 du Code de l'action sociale et des familles

L'objet premier du projet de décret en conseil d'État est de fixer les modalités de traitement et de conservation des données visées à l'article L. 147-5 du Code de l'action sociale et des familles.

Ces informations concernent les éléments recueillis par le CNAOP auprès des établissements de santé, des services départementaux, des organismes autorisés et habilités pour l'adoption, de l'autorité centrale pour l'adoption ou de la mission pour l'adoption internationale, pour donner suite aux demandes dont il est saisi.

D'une part, ces informations peuvent porter sur la santé des parents, les origines de l'enfant et les circonstances de la naissance, à la condition que les parents de naissance aient souhaité l'intégration de ces informations dans le dossier de leur enfant.

D'autre part, ces éléments concernent « l'identité » de la mère ou des deux parents, recueillie sous pli fermé conformément aux dispositions de la loi du 22 janvier 2002. Il s'agit des informations volontairement communiquées par la mère ou les parents ayant demandé le secret de leur identité au moment de l'accouchement ou de la remise de l'enfant aux services sociaux du département, sans qu'aucune vérification d'identité ou enquête ne soient réalisées à cette occasion.

Compte tenu de la sensibilité de ces informations au regard des situations de détresse des personnes « nées sous x » en attente de la communication de ces données, leur transmission au CNAOP doit s'entourer de garanties spécifiques.

À cet égard, l'article 1er du projet de décret prévoit la transmission de ces documents au CNAOP par porteur ou par voie postale par pli recommandé avec accusé de réception.

La Commission considère ces dispositions comme satisfaisantes.

S'agissant de la conservation de ces informations au sein du CNAOP, l'article 2 du projet de décret prévoit que le secrétaire général du Conseil national prend les dispositions nécessaires pour assurer la conservation des copies et renseignements prévus à l'article L. 147-5, et notamment du pli fermé supposé contenir l'identité parentale, dans des conditions de sécurité garantissant le respect de leur confidentialité, en particulier pour en réserver l'accès aux seules personnes qu'il habilite à en connaître.

La Commission considère néanmoins que la définition de ces dispositions relève en premier lieu du Conseil national, et estime en conséquence souhaitable que l'article 2 du projet de décret soit ainsi rédigé : *« Le Conseil national pour l'accès aux origines personnelles prend les dispositions nécessaires pour assurer la conservation des demandes et déclarations prévues à l'article L. 147-2 du Code de l'action sociale et des familles, des copies et renseignements prévus à l'article L. 147-5 du même Code, du pli prévu à l'article L. 222-6 ainsi que des demandes visées au deuxième alinéa de l'article 1 du présent décret, dans des conditions de sécurité garantissant le respect de leur confidentialité, notamment pour en réserver l'accès aux seules personnes que le secrétaire général du Conseil national habilite à en connaître. »*

Sur les dispositions portant création d'un traitement automatisé d'informations nominatives

Finalité du traitement (article 3 du projet de décret)

L'article 3 du projet de décret prévoit que le CNAOP mettra en œuvre un traitement pour assurer la conservation et la gestion des dossiers dont il est saisi, ainsi que pour établir des statistiques anonymes afin de rendre compte de son activité et de l'évolution de la question du secret des origines en france.

Pertinence des données traitées (articles 4 et 5 du projet de décret)

Seule l'identité des personnes ayant effectué une demande d'accès aux origines ou une déclaration d'identité ou de levée du secret auprès du CNAOP en application des dispositions de l'article L. 147-2 du Code de l'action sociale et des familles, des parents adoptifs du demandeur d'accès et des correspondants départementaux du CNAOP apparaît dans l'application informatique.

S'agissant des autres catégories d'informations traitées, celles-ci se limiteront aux données nécessaires au suivi administratif des dossiers et des échanges de correspondances avec les structures publiques ou privées en rapport avec le CNAOP, et à la production de statistiques d'activité non nominatives.

La Commission relève qu'aucune information sensible au sens de l'article 31 de la loi du 6 janvier 1978 – telle que l'origine raciale, les mœurs, ou la religion des parents – ne sera traitée informatiquement.

La Commission relève également que l'identité supposée des parents de naissance susceptible d'apparaître dans le pli fermé transmis au Conseil national ne sera pas enregistrée sur support informatique.

En revanche, la Commission considère que l'enregistrement informatique de l'identité des personnes déclarant leur identité auprès du CNAOP au sens de l'article L. 147-2 du Code de l'action sociale et des familles, au titre desquelles peuvent notamment figurer les parents de naissance d'un enfant « né sous x », n'appelle pas d'observation dans la mesure où cette information est nécessaire au traitement de leur dossier ainsi qu'à leur information régulière par le Conseil national sur l'état d'avancement de ce dossier.

La nationalité du demandeur d'accès ou du déclarant d'identité est enregistrée dans la mesure où le CNAOP a compétence pour connaître des demandes de personnes nées à l'étranger ou de déclarations de personnes de nationalité étrangère. Cet élément d'identité permet de recueillir des renseignements sur le demandeur auprès de l'organisme autorisé pour l'adoption ayant recueilli l'enfant dans son pays d'origine, par l'intermédiaire de la mission de l'adoption internationale ou de l'autorité centrale pour l'adoption internationale.

Sur la base de l'ensemble de ces observations, la Commission considère que les données visées à l'article 4 du projet de décret sont pertinentes, adéquates et non excessives.

S'agissant des données statistiques visées à l'article 5 du projet de décret, la Commission prend acte des engagements du CNAOP à ne traiter et diffuser que des états statistiques non nominatifs.

Destinataires des données (article 7 du projet de décret)

Les destinataires des informations enregistrées sont les structures publiques ou privées visées aux articles L. 147-4, L. 147-5, L. 147-6 et L. 147-8 du Code de l'action sociale et des familles.

Il s'agit des administrations, organismes, établissements auprès desquels le Conseil national est susceptible de recueillir des informations sur les parents de naissance pour répondre aux demandes d'accès aux origines dont il est saisi (services départementaux, organismes sociaux, organismes d'adoption, personne mandatée pour les recherches, procureur de la République, demandeurs d'accès aux origines dans le cadre de l'information régulière qui leur est donnée quant au résultat des investigations du Conseil national, etc.).

Le projet de décret précise que ces structures ne reçoivent du CNAOP que les informations nécessaires à l'accomplissement des missions du Conseil national.

La Commission estime souhaitable que le terme *« destinataires »* soit remplacé par l'expression *« personnes publiques ou privées »* au sein de l'article 7 du projet de décret.

Durée de conservation (article 9 du projet de décret)

Les données visées à l'article 4 du projet de décret sont conservées sur support informatique pendant un an à compter de la date de clôture définitive du dossier.

À l'issue de ce délai d'un an ne sont conservés dans l'application informatique que l'identité du demandeur et le numéro d'enregistrement du dossier aux seules fins d'indexation des dossiers conservés sur support papier.

La Commission considère que cette durée de conservation sur support informatique des informations nominatives visées à l'article 4 du projet de décret n'est pas excessive.

Sécurités (article 6 du projet de décret)

L'article 6 du projet de décret prévoit que sont seuls habilités à enregistrer, traiter, conserver ou modifier les données informatiques, y compris les statistiques non nominatives, le secrétaire général et les personnels du CNAOP, dans la limite de leurs missions.

En pratique, le CNAOP assurera la sécurité des informations par la mise en œuvre de différentes sécurités physiques (filtrage des accès au bâtiment) et logiques (filtrage des accès à l'information numérique).

La Commission prend acte des mesures de sécurité prises par le CNAOP.

Droit d'accès et de rectification, information des personnes concernées (article 8 du projet de décret)

Les demandeurs d'accès aux origines et les personnes déclarant leur identité seront avisés, par le courrier accusant réception de leur demande ou déclaration, du recueil sous forme de données informatiques des éléments communiqués par eux au titre de l'article 4 du projet de décret et de l'existence d'un droit d'accès et de rectification pouvant s'exercer auprès du secrétariat général du CNAOP.

La Commission relève tout particulièrement que l'article 8 du projet de décret souligne que le titulaire du droit d'accès ne peut accéder qu'aux informations relatives à sa demande ou déclaration, ainsi qu'à son suivi, sous réserve que l'exercice de ce droit ne porte pas atteinte à la vie privée d'autrui.

Les demandeurs et déclarants seront également avisés par le courrier accusant réception de leur demande ou déclaration que les informations enregistrées strictement nécessaires à l'accomplissement des missions du Conseil seront exclusivement communiquées aux destinataires définies aux articles L. 147-4, L. 147-5, L. 147-6 et L. 147-8 du Code de l'action sociale et des familles.

La Commission **émet**, au bénéfice de l'ensemble de ces observations, **un avis favorable** au projet de décret en Conseil d'État pris en application de l'article L. 147-11 du Code de l'action sociale et des familles et portant création d'un traitement automatisé d'informations nominatives pour la gestion des missions du Conseil national pour l'accès aux origines personnelles.

Fiscalité

Délibération n° 03-009 du 27 février 2003 concernant la mise en place par la direction générale des impôts d'un serveur professionnel des données cadastrales consultable par internet

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie d'un projet d'arrêté portant création, par la direction générale des impôts, du traitement automatisé d'informations nominatives dénommé « serveur professionnel de données cadastrales – SPDC » ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment les articles 29 et 31, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le Code général des impôts, notamment l'article 870 ;

Vu le Code du domaine de l'État, notamment l'article L. 76 ;

Vu le décret n° 55-22 du 4 janvier 1955 modifié portant réforme de la publicité foncière, ensemble le décret n° 55-1350 du 14 octobre 1955 modifié pris pour son application ;

Vu l'arrêté du 16 août 1984 modifié relatif à la mise à disposition des centres des impôts fonciers des moyens informatiques assurant la gestion décentralisée de la documentation cadastrale sur support magnétique (MAJIC 2), notamment l'article 4 ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle, commissaire, en son rapport et Madame Catherine Pozzo di Borgo, commissaire-adjoint du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le serveur professionnel des données cadastrales (« SPDC ») de la direction générale des impôts (DGI) vise à permettre, grâce à la technologie internet :
– la consultation par les professionnels concernés, pour l'ensemble du territoire national, notamment les départements d'outre-mer, de certaines informations foncières issues de la documentation cadastrale ;
– l'impression des extraits cadastraux modèle n° 1 dont la transmission aux services des hypothèques est nécessaire à l'accomplissement des formalités de publicité foncière, afin de certifier l'actualité de l'identification cadastrale des biens portée sur les actes notariés et ainsi, d'assurer la concordance permanente du cadastre et du fichier immobilier des conservations des hypothèques sur laquelle repose la sécurité juridique des transactions immobilières.

Le serveur « SPDC » est appelé à modifier de manière substantielle les modalités d'accès au cadastre de ses utilisateurs, en leur proposant :
– un accès immédiat et permanent à certaines informations, sans qu'ils aient besoin de présenter une demande dans un centre des impôts fonciers (CDIF) ;

– un accès au niveau national, alors que, jusqu'à présent, un CDIF n'a pas la possibilité de communiquer les informations dont il n'assure pas la mise à jour.

Le traitement ne conduit pas à la création d'une base nationale mais consiste en une procédure de consultation, au plan national, d'une partie des fichiers départementaux du cadastre. Il ne stocke par lui-même aucune information et ne modifie pas les modalités de mise à jour des données cadastrales, qui continuera de s'effectuer à partir de l'application « MAJIC 2 » des CDIF.

Les catégories d'informations accessibles via « SPDC » sont exclusivement de nature foncière, par opposition aux données du cadastre à caractère purement fiscal. Elles concernent l'adresse et la contenance cadastrale des parcelles, la nature de culture, le type de lot, la désignation des titulaires d'un droit réel sur une parcelle, la nature de leur droit, la filiation descendante entre la parcelle mère et celle qui résulte de son démembrement, le code SIREN des personnes morales, le CDIF compétent de la commune de situation du bien, ainsi que la date d'actualisation des informations.

Les personnes autorisées à interroger le serveur sont :
– les notaires et leurs collaborateurs, qui pourront y accéder directement de leur étude pour éditer les extraits cadastraux nécessaires à l'accomplissement des formalités de publicité foncière ou pour obtenir les références cadastrales d'une ou plusieurs parcelles en vue de la rédaction d'un acte notarié ;
– les agents des CDIF, qui auront ainsi la possibilité de délivrer à tout usager des extraits cadastraux, sans considération de la situation géographique de la parcelle ;
– les agents du service du domaine, afin de leur permettre de rédiger les actes soumis à publicité foncière qu'entraîne la gestion du domaine de l'État ;
– les agents des conservations des hypothèques qui seront destinataires des extraits cadastraux modèle n° 1 qui, relevant de leur compétence territoriale, ont vocation à leur être transmis sous forme papier à l'appui des demandes de publication d'actes ;
– les autres agents de la DGI qui remplissent des fonctions ayant trait à la publicité foncière, sur désignation du directeur des services fiscaux ;
– l'École nationale du cadastre, au titre de ses actions de formation.

Bien que trouvant sa source dans un décret-loi du 7 messidor an II, aujourd'hui abrogé par la loi n° 79-18 du 3 janvier 1979 susvisée, le principe, qui a été tiré de ce texte, de libre communication au public des informations nominatives du cadastre est considéré comme étant toujours en vigueur.

Pour autant, il ne saurait être contesté que celles de ces informations ayant un caractère nominatif bénéficient de la protection établie par la loi du 6 janvier 1978. En particulier, le principe de finalité trouve à s'appliquer, dans la mesure où les données sont communiquées par référence à certaines finalités.

Il en résulte que ces informations sont, en principe, communiquées de manière ponctuelle, sur demande préalable. Il est également exclu qu'elles fassent l'objet, une fois délivrées, de certaines utilisations, notamment que leurs destinataires les transmettent à des tiers, qu'ils en fassent un usage de nature à porter atteinte à l'honneur ou à la réputation des personnes ou au respect de la vie privée ou encore qu'ils les utilisent à des fins de démarchage commercial, politique ou électoral.

L'administration se réserve le droit de faire signer un engagement en ce sens aux usagers dont les motivations paraîtraient douteuses, voire de refuser de communiquer les informations.

Seules certaines catégories d'usagers du cadastre bénéficient d'un accès privilégié aux informations. La Commission constate que les professionnels et agents publics utilisateurs du serveur « SPDC » appartiennent bien à ces catégories d'usagers.

Il convient, en conséquence, de s'assurer que toutes les précautions utiles, tant juridiques que techniques, sont prises pour empêcher que les informations accessibles via « SPDC » ne soient utilisées par des tiers non autorisés à y accéder et pour des finalités autres que celles retenues pour justifier la mise en place de ce serveur.

En premier lieu, la Commission constate que les modalités d'interrogation du serveur sont de nature à limiter les risques de détournement de finalité : pour obtenir les informations relatives à une parcelle ou à plusieurs appartenant à une même personne physique ou morale, il est nécessaire de connaître le département et la commune de leur localisation, ainsi qu'au moins l'une des informations suivantes :
– la raison sociale ou l'identité du (ou de l'un des) titulaire (s) de droit sur la propriété ;
– l'identification cadastrale du bien, du groupe de biens, du lot ou de la parcelle d'assise de la copropriété ;
– le numéro d'ordre d'un document d'arpentage.

Il sera donc techniquement impossible de lancer une requête pour l'ensemble du territoire national sur la seule base du nom d'une personne ou d'interroger le serveur à partir de l'adresse d'un bien immobilier.

En deuxième lieu, les droits des personnes habilitées à utiliser le serveur sont gérés par l'intermédiaire d'un annuaire, dénommé « Annuaire DGI ». Seules les personnes reconnues par l'annuaire peuvent y accéder.

Les informations relatives aux utilisateurs externes qui figurent dans l'annuaire de la DGI proviennent, s'agissant des notaires, d'un fichier national des notaires transmis par le Conseil supérieur du notariat (CSN) et mis à jour deux fois par mois.

Par ailleurs, les notaires ont la faculté de créer, sous leur responsabilité, des habilitations individuelles pour certains de leurs collaborateurs. Tout notaire « délégant » pourra mettre à jour directement, à partir d'une application dénommée « APEX », les données relatives aux habilitations ouvertes sous sa responsabilité. Il disposera, à cette fin, d'un accès direct aux informations de l'annuaire de la DGI concernant les personnes qu'il a habilitées.

En outre, l'identifiant d'un collaborateur sera automatiquement supprimé en cas de départ du notaire « délégant » de l'office ou si aucune utilisation du service n'est constatée pendant un délai de quatre mois.

En troisième lieu, l'administration s'est engagée à mettre en place, d'ici la fin de l'année 2003, un système de traçabilité grâce à l'ajout d'un nouveau module dans l'application « Annuaire DGI ».

La Commission prend acte de cet important engagement, mais constate qu'aucune précision n'est fournie, à ce jour, sur les modalités de mise en œuvre de ce dispositif de contrôle : quelles seront les informations enregistrées ? Porteront-elles sur les consultations opérées tant par les agents de la DGI que par les utilisateurs externes ? Pendant quelle durée seront-elles conservées ? Comment seront-elles exploitées ? Par qui ? En particulier, les notaires pourront-ils consulter les journaux relatifs aux consultations effectués par leurs collaborateurs ? De ces précisions dépendra l'efficacité réelle du système de contrôle.

Une convention, en cours d'élaboration entre la DGI et le CSN, doit définir les conditions dans lesquelles les notaires pourront utiliser « SPDC ». La Commission recommande que celle-ci définisse les limitations à apporter à l'utilisation des informations consultables à partir du serveur afin d'en respecter la finalité, les engagements qui devront être pris par les notaires souhaitant bénéficier du serveur, ainsi que les conditions dans lesquelles le respect de ces engagements pourra être contrôlé. Ceux-ci devraient notamment porter sur les points suivants :

– l'interdiction de toute utilisation des informations pour des finalités étrangères à la rédaction des actes notariés, notamment pour des opérations de prospection de terrains en relation avec une activité de négociation immobilière ;
– l'obligation de doter toute personne ayant à accéder au serveur d'une habilitation personnelle, répertoriée dans l'annuaire de la DGI et assortie d'un mot de passe individuel ;
– l'annulation de toute habilitation donnée à une personne n'ayant plus vocation à utiliser le serveur, par exemple à la suite de son départ de l'étude.

Enfin, il importe d'empêcher que le serveur n'ait à faire face à une série de requêtes lancées automatiquement par un moteur d'interrogation. La Commission recommande, à ce titre, la mise en place d'un dispositif d'analyse des volumes d'interrogations, provoquant la déconnexion du serveur en cas d'augmentation inhabituelle des flux de consultation.

Au bénéfice des observations qui précèdent, la Commission **émet un avis favorable** sur le projet d'arrêté relatif au traitement « SPDC » pour une durée limitée à un an, délai qui devrait être mis à profit pour saisir la CNIL d'un dispositif complémentaire portant sur les modalités de conservation et d'exploitation des traces des consultations et lui communiquer le projet de convention en cours d'élaboration entre la direction générale des impôts et le Conseil supérieur du notariat.

Délibération n° 03-048 du 30 octobre 2003 concernant la mise en place par la direction générale des impôts d'une base nationale de recensement des liens d'intérêts existant entre personnes physiques et sociétés

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie :
– d'un projet d'arrêté portant création par la direction générale des impôts d'un traitement automatisé dénommé « Transparence des structures écrans – TSE » ;
– de trois projets d'arrêtés modificatifs, complétant les arrêtés relatifs à trois traitements automatisés de la direction générale des impôts : le traitement des actes et déclarations déposés dans les recettes des impôts (« MOOREA »), le traitement des dossiers des redevables professionnels dénommé base de données des redevables professionnels (« BDRP »), le traitement pour la simplification des procédures d'imposition (« SPI ») ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le Code général des impôts, notamment les articles 635, 638 A et 639, et son annexe III, notamment l'article 350 terdecies ;

Vu l'arrêté modifié du 7 août 1985 relatif à la création d'un traitement informatisé pour la simplification des procédures d'imposition ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

1) La base de données « TSE » de la direction générale des impôts (DGI) vise à répertorier, au niveau national, les liens connus de l'administration entre sociétés et personnes physiques (liens de dirigeant, d'associé ou d'actionnaire), entre sociétés (liens de participation) et entre les personnes physiques précitées (liens maritaux ou filiaux) et à apporter des renseignements sur leur évolution récente.

Elle est destinée à mettre à la disposition des agents habilités de la DGI et de la direction générale de la comptabilité publique (DGCP) des éléments sur la situation patrimoniale des contribuables et sur leur participation dans des groupements et sociétés – en particulier dans des sociétés de personnes, des sociétés de fait ou en participation, des groupes informels, des sociétés éphémères et des sociétés civiles immobilières – qui doivent être pris en compte pour le contrôle sur pièces des déclarations des contribuables et l'établissement de l'impôt, pour la programmation et la préparation des contrôles sur place et pour le recouvrement des impôts, droits et taxes prévus par le Code général des impôts (CGI).

Ces finalités sont légitimes et n'appellent pas d'observation de la part de la Commission.

2) La Commission observe que la création de ce traitement ne conduit à aucune collecte d'informations nominatives supplémentaire et que les données enregistrées proviennent exclusivement :
– pour les données relatives aux sociétés et aux dirigeants : des bases locales de données des redevables professionnels (« BDRP ») des centres des impôts ;
– pour les données relatives aux associés, aux actionnaires et à leurs conjoints : des traitements « MOOREA » qui enregistrent les données issues des actes ou déclarations déposés dans les recettes des impôts pour l'accomplissement des formalités de l'enregistrement et le paiement des droits correspondants ; les informations extraites de « MOOREA » et transmises à « TSE » sont celles qui concernent plus particulièrement certains événements affectant la vie des sociétés, notamment la formation, la transformation ou la dissolution d'une société, l'augmentation ou la réduction de son capital, la cession d'actions ou de parts sociales de sociétés et la cession de participations dans des personnes morales à prépondérance immobilière ;
– pour les liens filiaux, les liens d'associés déclarés avant 1999 et les liens d'intérêt avec des personnes morales de droit étranger : du dossier fiscal du contribuable.

Afin de parer aux risques d'homonymie et de permettre de compléter et de mettre à jour les informations d'état civil et d'adresse concernant les dirigeants, associés, actionnaires et leurs conjoints, l'administration prévoit un rapprochement avec le fichier national de la DGI qui recense les contribuables personnes physiques et les personnes rattachées à un foyer fiscal (« SPI »). Ce rapprochement permet en particulier l'enregistrement dans « TSE » de l'identifiant fiscal national SPI des personnes qui y sont mentionnées.

3) Les personnes morales présentes dans « TSE » sont des sociétés et groupements de formes et de régimes juridiques variés, et notamment les sociétés anonymes, les sociétés en nom collectif, les sociétés en commandite par actions, les SARL, les SICOMI, les sociétés immobilières de gestion, les sociétés créées de fait ou en participation, les EURL, les groupements d'intérêt économique, les sociétés coopératives ouvrières de production, les sociétés de caution mutuelle, les SICAV, les SCPI, les sociétés immobilières pour le commerce et l'industrie, les sociétés immobilières d'investissement, les sociétés civiles immobilières, les sociétés civiles professionnelles, les sociétés civiles coopératives, les sociétés civiles de moyens ou d'exploitation agricole, les sociétés civiles foncières, les SAFER, les groupements agricoles d'exploitation en commun, les groupements forestiers ou pastoraux, ainsi que les personnes morales de droit étranger en lien avec ces sociétés.

Pour chaque personne physique mentionnée dans la base, sont indiqués :
– ses nom, prénoms, date et lieu de naissance, éventuellement la date de décès ;
– l'identifiant fiscal national et personnel SPI,
– l'adresse du domicile fiscal ;
– les liens maritaux et filiaux avec toute autre personne physique présente dans la base ;
– les liens de dirigeant, d'associé ou d'actionnaire dans les sociétés et groupements présents dans la base ;
– pour les associés et actionnaires : le nombre de parts sociales ou d'actions détenues ;
– le nombre des parts acquises ou cédées ;
– pour chacune de ces opérations, sa nature et sa date.

La Commission observe, toutefois, que les liens d'actionnaires entre personnes physiques et sociétés de capitaux pour les actions de ses sociétés qui sont librement cessibles sur un marché ne seront pas répertoriés dans le traitement.

Elle demande, en conséquence, que le projet d'arrêté relatif au traitement « TSE » soit complété sur ce point.

Les informations sont conservées jusqu'à la fin de la troisième année suivant leur année de péremption. Cependant, en ce qui concerne les associés et actionnaires, lorsque la réalité de la péremption n'est pas certaine – c'est-à-dire lorsque le nombre d'actions ou de parts détenues par l'associé ou l'actionnaire avant un acte de cession ne figurait pas dans « TSE » –, les données sont conservées pendant cinq ans après la date de péremption présumée.

La Commission constate que ces informations nominatives sont adéquates, pertinentes et non excessives au regard des finalités poursuivies et que leur durée de conservation n'est pas excessive.

4) L'administration souhaite enrichir l'application nationale « SPI » à partir d'éléments transmis par « TSE » :
– pour les associés, actionnaires ou dirigeants qui n'étaient pas connus dans « SPI » en qualité de contribuable, l'ensemble des informations d'état civil et d'adresse les concernant, auquel sera associé un identifiant SPI spécifique ;
– systématiquement, les informations relatives aux liens d'associé, d'actionnaire et de dirigeant.

La Commission note que le traitement « SPI » ne conserve, à ce jour, que les éléments d'identification, la situation familiale et les adresses des personnes physiques ainsi que des occurrences fiscales, entendues comme toutes les situations donnant lieu pour ces personnes à l'établissement régulier d'un impôt par un service.

L'ajout d'une « occurrence » liée à « TSE » introduirait, pour les personnes concernées, une information en relation avec leur profession ou leur patrimoine mobilier qui ne correspond pas à la finalité actuelle du traitement « SPI » et qui n'a d'ailleurs fait l'objet d'aucune explication particulière.

Elle demande, en conséquence, que les projets d'arrêtés relatifs aux traitements « TSE » et « SPI » soient modifiés sur ce point.

5) Les personnes destinées à être habilitées à utiliser « TSE » sont les agents de la DGI et de la DGCP de catégorie A, B ou C qui sont chargés du contrôle sur pièces, de la programmation ou de la préparation des contrôles sur place, ou du recouvrement des impôts.

Dans l'attente de la prochaine mise en place de l'annuaire propre à la DGCP, les niveaux d'habilitation sont actuellement dans leur ensemble gérés dans le cadre de l'« Annuaire DGI », qui remplit cette fonction pour l'ensemble des applications développées dans le cadre du programme COPERNIC de refonte du système informatique fiscal. Les niveaux d'habilitation dépendent directement des fonctions remplies par l'agent.

L'administration prévoit de partager en fait, au niveau national, entre tous les utilisateurs, l'ensemble des informations traitées, que ceux-ci fassent partie d'une direction ou d'un service à compétence nationale, interrégionale ou départementale.

Pourtant, les agents des directions territoriales de la DGI et des services extérieurs du Trésor ont une compétence limitée, par principe, aux contribuables imposés dans le ressort géographique de leur direction ou trésorerie à l'égard desquels ils participent aux travaux de programmation du contrôle fiscal ou exercent une mission de contrôle ou de recouvrement d'un impôt, auxquels s'ajoutent, pour les seuls agents de contrôle, les contribuables qui sont liés aux personnes et groupements relevant de leur compétence territoriale. En conséquence, les destinataires de « TSE » ne sont pas habilités, en droit, à interroger la base à partir d'un nom de contribuable

non imposé dans le ressort territorial de leur direction, à l'égard duquel ils n'exercent pas légalement un « droit de suite ».

Si l'actuelle organisation de la base de données interdit la mise en place de profils d'habilitation tenant compte des compétences géographiques des agents de la DGI et de la DGCP, sauf à rendre impossibles certaines des utilisations envisagées de « TSE » notamment en matière d'aide au recouvrement des impôts locaux, la Commission demande que l'article 6 du projet d'arrêté « TSE » soit complété afin de rappeler dans quelles limites juridiques la qualité de destinataire des informations de « TSE » est reconnue.

La Commission rappelle, en outre, qu'il appartiendra aux chefs de service des administrations fiscales de s'assurer de la bonne application des règles d'habilitation en exploitant, de façon régulière et systématique, pendant le délai de trois mois prévu à cet effet, les journaux regroupant les traces des consultations de la base effectuées par les agents placés sous leur autorité.

Des inspecteurs principaux relevant de l'inspection générale des services pourront également être chargés de procéder à des audits ou à des vérifications et disposeront à cette fin, pendant un an, des journaux portant sur l'ensemble des consultations effectuées, notamment celles correspondant aux contrôles effectués par les chefs de service.

6) S'agissant de l'information sur les droits d'accès et de rectification, la DGI prévoit de faire figurer à brève échéance sur la totalité des formulaires de déclaration fiscale susceptibles d'être utilisés pour le recueil des données nominatives un rappel des modalités d'exercice de ces droits.

La Commission observe cependant que la plupart des actes et déclarations ne sont pas enregistrés dans les recettes des impôts par les associés, actionnaires ou dirigeants de sociétés, *a fortiori* par leurs conjoints, mais par les tiers qui les ont rédigés. En conséquence, le risque existe que les personnes intéressées ne soient pas informées de l'existence du traitement « TSE », ni des modalités d'exercice des droits d'accès et de rectification applicables aux informations les concernant.

Pour pallier cette difficulté, la Commission recommande, qu'en cas de transmission d'informations à « TSE », les documents adressés ou remis aux personnes ayant accompli les formalités d'enregistrement comportent un paragraphe leur demandant d'informer les personnes mentionnées dans l'acte ou la déclaration en qualité de dirigeant, d'associé ou d'actionnaire d'une société, des modalités d'exploitation des données les concernant et des conditions dans lesquelles elles peuvent exercer leurs droits d'accès et de rectification.

Plus généralement, la Commission rappelle qu'il incombe à l'administration de prendre les mesures nécessaires pour que les personnes figurant dans « TSE » soient effectivement informées de l'existence du traitement « TSE » ainsi que des modalités d'exercice de leurs droits d'accès et de rectification, et de faire des propositions en ce sens. Elle demande une modification de l'article 7 du projet d'arrêté « TSE » sur ce point.

Émet un avis favorable sur le projet d'arrêté relatif à l'application « TSE » et sur les projets d'arrêtés modificatifs concernant les traitements « MOOREA », « BDRP » et « SPI » qui lui sont soumis par le ministère de l'Économie, des Finances et de l'Industrie, sous réserve que :

1) S'agissant du projet d'arrêté concernant le traitement « TSE » :
— soit ajouté à l'article 3, après le 1er alinéa, un nouvel alinéa ainsi rédigé : *« Ne sont pas répertoriés dans le traitement les liens d'actionnaires entre personnes physi-*

ques et sociétés de capitaux pour les actions de ces sociétés qui sont librement cessibles sur un marché » ;
— les mots *« et à la création, dans cette application, d'une occurrence »* soient supprimés au II de l'article 5 ;
— l'article 6 soit modifié comme suit : *« Sont destinataires des informations :*
. les agents habilités de la direction générale des impôts chargés du contrôle et du recouvrement des impôts, droits et taxes prévus par le Code général des impôts, pour les informations relatives aux contribuables à l'égard desquels ils participent aux travaux de programmation du contrôle fiscal ou exercent les missions de contrôle ou de recouvrement précitées ;
. les agents habilités de la direction générale de la comptabilité publique chargés du recouvrement en matière fiscale, pour les informations relatives aux contribuables à l'égard desquels ils exercent cette mission » ;
— soit ajouté après le premier alinéa de l'article 7, un nouvel alinéa ainsi rédigé : *« La direction générale des impôts prend les mesures nécessaires pour que les personnes soient effectivement informées de l'existence du traitement "TSE" et des modalités d'exercice de leurs droits d'accès et de rectification » ;*

2) S'agissant du projet d'arrêté modificatif concernant le traitement « SPI » :
— l'article 1er soit modifié comme suit : *« Au deuxième alinéa de l'article 7 de l'arrêté du 7 août 1985 modifié susvisé, après les mots "*SPI *délivre à chacun d'eux", sont ajoutés les mots : "et au traitement TSE (transparence des structures écrans)" ».*

Immobilier

Délibération n° 03-067 du 18 décembre 2003 relative à la gestion et aux négociations des biens immobiliers

Norme simplifiée nº 21

La Commission nationale de l'informatique et des libertés ;

Vu les articles 6, 17 et 21 (1°) de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés habilitant la Commission nationale de l'informatique et des libertés à édicter, en vertu de son pouvoir réglementaire, des normes simplifiées concernant certains traitements automatisés d'informations nominatives ;

Considérant que pour l'application de l'article 17 susvisé, il faut entendre par norme simplifiée l'ensemble des conditions que doivent remplir certaines catégories les plus courantes de traitements pour être regardées comme ne comportant pas de risques d'atteinte à la vie privée et aux libertés et comme pouvant dès lors faire l'objet d'une déclaration simplifiée ;

Considérant que certains traitements automatisés, portant sur la gestion et les négociations des biens immobiliers sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 susmentionné ;

Décide :

Norme simplifiée relative à la gestion et aux négociations des biens immobiliers

Article 1er

Les dispositions de la présente décision concernent les traitements automatisés d'informations nominatives relatifs à la gestion et aux négociations des biens immobiliers mis en œuvre par toute personne publique ou privée.

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée, ces traitements doivent :

– ne porter que sur des données objectives aisément contrôlables par les intéressés grâce à l'exercice du droit individuel d'accès ;

– n'appliquer à ces données que des logiciels dont les résultats puissent être facilement contrôlés ;

– ne pas procéder à des cessions ou locations des contenus des fichiers de l'organisme ;

– ne pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des fonctions énoncées à l'article 2 ci-dessous ;

– comporter des dispositions propres à assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi ;

– satisfaire en outre aux conditions énoncées aux articles 2 à 5 ci-dessous.

Article 2

Finalité du traitement

Le traitement ne doit pas avoir d'autres fonctions que :

a) d'établir le quittancement des loyers : l'émission de titres de recettes des locations et la gestion des relances, le décompte des taxes et charges y afférentes, la régulari-

sation des charges, les pièces comptables nécessaires au recouvrement et à la gestion des comptes des locataires concernés ;
b) d'assurer la gestion des sociétés civiles immobilières, des sociétés ayant pour objet la construction, des coopératives et des syndicats de copropriété, des associations syndicales libres et des immeubles en jouissance à temps partagé : la comptabilité de ces organismes, la tenue des comptes des intéressés, la convocation aux assemblées générales, les lettres de relance, les appels de fonds ;
c) d'établir la gestion des mandats de gérance : la comptabilité du mandat de gérance, la tenue des comptes des propriétaires, la tenue des comptes des locataires, la déclaration des revenus fonciers ;
d) d'enregistrer les éléments permettant d'apprécier la solvabilité des candidats à la location d'un bien immobilier à l'exclusion du calcul automatisé de l'appréciation du risque et de procéder aux opérations de recouvrement de créance ;
e) d'assurer la gestion et la transaction par voies télématique et électronique ;
f) d'assurer les opérations de négociation immobilière ;
g) d'assurer l'attribution des dispositifs individuels d'accès aux immeubles sous réserve d'une information préalable des intéressés portant description de ces dispositifs.

Article 3

Catégories d'informations traitées

Dès lors que les dispositions de l'article 27 de la loi n° 78-17 du 6 janvier 1978 ont été respectées lors du recueil des informations traitées, celles-ci doivent relever seulement des catégories suivantes :

1) Informations générales :
a) identité :
– pour le locataire, le candidat à la location et, le cas échéant, sa caution : nom, nom marital, prénoms, date et lieu de naissance, nationalité, adresse, adresse de courrier électronique, numéro de téléphone, code interne de traitement permettant l'identification (à l'exclusion du numéro d'inscription au répertoire national d'identification) ;
– pour l'acquéreur, le candidat acquéreur, le copropriétaire ou le propriétaire, l'associé, le conjoint du copropriétaire ou du propriétaire, leur partenaire signataire d'un pacte civil de solidarité (sous réserve de l'accord exprès des intéressés) à condition qu'il ait des droits dans la copropriété, chacun des co-indivisaires en cas d'indivision, le ou les titulaires des droits visés à l'article 6 du décret du 17 mars 1967 : nom, nom marital, prénoms, date et lieu de naissance, nationalité, situation familiale, régime matrimonial, adresse, adresse de courrier électronique, numéro de téléphone, code interne de traitement permettant l'identification (à l'exclusion du numéro d'inscription au répertoire national d'identification) ;
– coordonnées du mandataire commun en cas d'indivision ou du gérant qui gère les lots ;
b) identité bancaire ou postale ;
c) logement :
– caractéristiques du logement ou des biens immobiliers, conditions de location ou d'accession à la propriété, date d'entrée et de départ, montant du dépôt de garantie, montant du loyer, nature et montant des charges, des travaux d'entretien et d'amélioration et nature des prêts consentis et des modalités de remboursement, compagnie d'assurance, numéro de police du locataire ;
d) numéro d'identification, identité et coordonnées du porteur du support électronique d'identification pour l'accès aux immeubles.

2) Informations spécifiques aux locataires et candidats locataires :
a) situation familiale, composition du foyer, conclusion d'un pacte civil de solidarité (sous réserve de l'accord exprès des intéressés) ;
b) numéro d'inscription à la caisse d'allocations familiales du bénéficiaire exclusivement pour permettre le versement des aides au logement ;
c) situation professionnelle, coordonnées de l'employeur ;
d) ressources.

3) Informations spécifiques aux cautions :
– ressources.

4) Informations spécifiques aux candidats acquéreurs et acquéreurs d'un bien immobilier :
– disponibilités financières.

Article 4
Durée de conservation

Les informations nécessaires aux traitements automatisés d'informatisations nominatives définies aux articles 1, 2 et 3 ne doivent pas être conservées après le règlement du solde des comptes ou la rupture de la relation contractuelle à l'exception des informations nécessaires à l'accomplissement des obligations légales.

Les informations relatives au candidat à la location ou au candidat acquéreur ne peuvent être conservées que si la location ou l'acquisition est effectivement réalisée. À défaut de location ou d'acquisition, ces informations doivent être supprimées en cas de non-renouvellement de la demande dans un délai de trois mois.

Article 5
Destinataires des informations

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des informations les concernant :
– les services chargés de la gestion et de la comptabilité des immeubles ;
– l'organisme financier teneur du compte du locataire, de l'accédant ou du propriétaire ;
– les auxiliaires de justice et les officiers ministériels dans le cadre de leur mission de recouvrement de créances ;
– les services publics, exclusivement pour répondre aux obligations légales.

Article 6

La norme simplifiée instituée par la délibération n° 99-055 du 18 novembre 1999 est abrogée.

Police et douanes

Délibération n° 03-001 du 9 janvier 2003 portant avis conforme sur le projet de décret en Conseil d'État portant création du système d'information judiciaire « JUDEX » et faisant application à ce traitement des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministre de la Défense d'un projet de décret en Conseil d'État portant création du « système d'information judiciaire JUDEX » et faisant application à ce traitement du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le Code pénal ;

Vu le Code de procédure pénale ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi du n° 95-73 21 janvier 1995 modifiée, et notamment son article 17-1 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le décret n° 79-1160 du 28 décembre 1979 fixant les conditions d'applications aux traitements automatisés d'informations nominatives intéressant la sûreté de l'État, la défense et la sécurité publique de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées ;

Vu la délibération n° 00-064 du 19 décembre 2000 relatif à un projet de décret en Conseil d'État portant création du « système de traitement des infractions constatées » (STIC) et application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 ;

Après avoir entendu Monsieur François Giquel, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

La Commission est saisie pour avis par le ministère de la Défense d'un projet de décret en Conseil d'État portant création du « système d'information judiciaire JUDEX » et faisant application à ce traitement du troisième alinéa de l'article 31 de la loi du 6 janvier 1978, alors qu'un projet de loi comportant plusieurs dispositions visant à définir les modalités de fonctionnement de tels fichiers de police judiciaire est actuellement examiné au Parlement.

En application des dispositions des articles 15 et 31 de la loi du 6 janvier 1978, la Commission estime cependant devoir rendre son avis, en l'état du droit positif, sur les dispositions régularisant le fichier JUDEX dans la mesure où, conformé-

ment aux demandes réitérées de la Commission, la mise en œuvre de ce fichier doit être assurée dans le respect des règles de protection des données.

La Commission rappelle à cet égard que l'ensemble des fichiers de données personnelles actuellement mis en œuvre par les services de la gendarmerie nationale doivent de la même façon être rendus conformes aux dispositions de la loi du 6 janvier 1978. Il en est ainsi en particulier du fichier alphabétique des renseignements.

Le système d'information judiciaire JUDEX est un fichier national de même nature que le « système de traitement des infractions constatées » (STIC) mis en œuvre par la police nationale dans le cadre de ses missions de police judiciaire. Dès lors, la Commission considère que cette nouvelle centralisation d'informations de police judiciaire impose que le ministère de la Défense prévoit des garanties aussi protectrices que celles demandées par la Commission dans sa délibération du 19 décembre 2000 pour la mise en œuvre, par le ministère de l'Intérieur, du système STIC.

Sur la finalité du système d'information judiciaire JUDEX

Aux termes de l'article 1er du projet de décret, le système d'information judiciaire JUDEX a pour seule finalité l'exploitation des informations contenues dans les procédures établies par les unités de gendarmerie aux fins de recherches criminelles.

La Commission prend note que le système JUDEX est appelé à enregistrer des informations relatives aux crimes, aux délits et à six catégories de contraventions de cinquième classe limitativement énumérées (les violences volontaires avec incapacité totale de travail inférieure ou égale à huit jours, le racolage, la destruction ou la dégradation volontaire d'un bien appartenant à autrui avec dommage léger, le port ou l'exhibition d'uniformes, d'insignes ou d'emblèmes rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité, l'intrusion dans les établissements scolaires, la provocation non publique à la discrimination, à la haine ou à la violence raciale).

La Commission relève également que seules les personnes mises en cause dans une procédure judiciaire, au sens de l'article 105 du Code de procédure pénale, et les victimes d'infractions donnant lieu à l'ouverture d'une enquête judiciaire sont susceptibles d'être inscrites dans le système JUDEX, à l'exclusion de toute autre personne, et en particulier des témoins.

La Commission rappelle cependant que les personnes mineures mises en cause ne peuvent être inscrites dans ce fichier que dans les cas où, conformément aux dispositions du Code de procédure pénale et à celles de l'ordonnance du 2 février 1945 relative à l'enfance délinquante, leur responsabilité est susceptible d'être engagée devant les juridictions répressives.

Il conviendrait donc, dans un souci de clarté, d'insérer, au premier alinéa de l'article 2, après les mots : « […] *lorsqu'elles concernent des personnes* […] » les mots : « […] *majeures ou mineures âgées de plus de dix ans* […] ».

Sur le contrôle de l'alimentation du fichier

La Commission prend acte que si le fichier JUDEX est mis en œuvre par le ministère de la Défense (direction générale de la gendarmerie nationale), le projet de décret précise que le traitement des informations nominatives est effectué sous le contrôle du procureur de la République territorialement compétent. Cette garantie est

conforme aux dispositions de l'article 12 du Code de procédure pénale qui précise que la police judiciaire s'exerce sous la direction du procureur de la République.

La Commission prend note qu'afin d'assurer un contrôle de la qualification des faits, les informations nominatives concernant les personnes mises en cause et les victimes sont transmises avec la procédure au procureur de la République territorialement compétent afin qu'il puisse user, le cas échéant, du pouvoir qui lui est reconnu par l'article 3 du projet de décret de demander la rectification ou l'effacement des informations enregistrées.

Sur les conditions de consultation du système JUDEX à des fins administratives

L'article 6 du projet de décret prévoit que, par dérogation aux dispositions de l'article R. 156 du Code de procédure pénale et sous réserve des dispositions de l'article 17-1 de la loi du 21 janvier 1995, les informations figurant dans le traitement peuvent être consultées *« dans le cadre de missions de police administrative ou de sécurité »*, à la condition que *« la nature de ces missions ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes »*.

Comme dans le décret du 5 juillet 2001 portant création du STIC, cette consultation est entourée de plusieurs conditions énumérées à l'article 6 :
– elle ne peut concerner des procédures en cours ;
– elle ne peut porter ni sur des informations relatives à des victimes, ni sur des données ayant fait l'objet d'une mise à jour par le procureur de la République ;
– elle est réservée aux personnels de la gendarmerie nationale ;
– ceux-ci doivent être individuellement désignés et spécialement habilités à cette fin par le directeur général de la gendarmerie ou l'autorité déléguée par lui ;
– cette habilitation comporte deux niveaux d'accès et précise le niveau qui est conféré à son titulaire par l'autorité compétente.

Dès lors que l'article 17-1 de la loi du 21 janvier 1995 prévoit expressément la possibilité de consulter à des fins administratives les informations figurant dans les fichiers de police judiciaire, y compris pour les procédures en cours, la Commission prend acte que cette garantie n'a plus à recevoir application, mais estime cependant que les autres conditions énoncées à l'article 6 ont lieu de s'appliquer, y compris lorsque les informations sont consultées dans le cadre des enquêtes administratives prévues par l'article 17-1 de la loi du 21 janvier 1995.

Sur les catégories d'informations traitées et sur les données sensibles

Les informations nominatives enregistrées dans JUDEX sont, s'agissant des personnes mises en cause, l'identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), les surnoms et les alias s'il y a lieu, les date et lieu de naissance, la situation familiale, la filiation, la nationalité, l'adresse, l'état de la personne (modes opératoires et informations relevant de l'article 31 de la loi lorsque ces renseignements sont susceptibles d'éclairer le mode opératoire ou les mobiles de l'infraction, références des affaires judiciaires pour lesquelles la personne est mise en cause, suites judiciaires transmises par le procureur de la République territorialement compétent dans les conditions du projet de décret), la profession, le signalement et la photographie.

S'agissant des victimes, sont enregistrés : identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), date et lieu de naissance, situation familiale, nationalité, adresse, profession, état de la personne (références des affaires judiciaires dans lesquelles la personne est victime, suites judiciaires transmises par le procureur de la République territorialement compétent dans les conditions du projet de décret), signalement et photographie pour les personnes disparues et les corps non identifiés uniquement.

Sont également enregistrées des informations non nominatives ou indirectement nominatives concernant les faits objets de l'enquête, les lieux, dates et modes opératoires, ainsi que des informations et images relatives aux objets.

Certaines informations nominatives pouvant faire apparaître, directement ou indirectement, des données relevant de l'article 31 de la loi de la loi du 6 janvier 1978, le projet de décret fait également application des dispositions du troisième alinéa de cet article.

La Commission considère que la finalité du fichier justifie la collecte et l'enregistrement pour des motifs d'intérêt public d'informations nominatives relevant de l'article 31 de la loi, à la condition toutefois que cette collecte et cet enregistrement, ainsi que le prévoit l'article 1er du projet de décret, ne soient effectués que dans les seuls cas où ces informations résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes et dès lors que ces éléments sont nécessaires à la recherche et à l'identification des auteurs des infractions répertoriées dans le système JUDEX.

Sur les destinataires

Seuls peuvent être destinataires des informations enregistrées dans le système JUDEX les personnels des unités de la gendarmerie nationale et des services de la police nationale exerçant des missions de police judiciaire et ayant fait l'objet d'une désignation par l'autorité hiérarchique, ainsi que les magistrats du parquet, pour les seules informations relatives à la procédure en cours.

Sur la communication de données à des États ou à des organismes intergouvernementaux et communautaires

Le projet de décret prévoit que les informations traitées au niveau central (bases « JUDEX-affaires » et « JUDEX-personnes mises en cause ») peuvent être communiquées aux *« autorités d'États ou organismes intergouvernementaux ou communautaires liés à la France par un accord international ou un acte de l'Union européenne* [...] *lorsque cette transmission est prévue par cet accord ou cet acte »*.

La Commission estime que les transferts de données envisagés doivent faire l'objet d'une disposition spécifique, distincte de celle relative aux destinataires, dans la mesure où ils ne concernent que des communications ponctuelles et ne visent pas à permettre un accès en temps réel aux bases du système JUDEX.

La Commission considère en outre qu'il serait souhaitable de préciser que ces communications d'informations ne peuvent s'effectuer qu'à la condition de présenter, pour la protection des données personnelles, des garanties équivalentes à celles du droit français.

Sur la mise à jour

Le projet de décret prévoit la mise à jour des informations nominatives enregistrées dans les hypothèses suivantes :
– décisions de relaxe et d'acquittement devenues définitives : effacement par le gestionnaire du fichier des informations concernant les personnes mises en cause ;
– décisions de non-lieu : mise à jour par le gestionnaire du fichier pouvant aller jusqu'à la suppression des informations concernant les personnes mises en cause ;
– décisions de classement sans suite motivées par une insuffisance de charges : mise à jour par le gestionnaire du fichier des informations concernant les personnes mises en cause ;
– possibilité, à l'initiative de la personne mise en cause, de substitution de la qualification initialement choisie par celle finalement retenue par l'autorité judiciaire ;
– mise à jour, à l'initiative de la personne mise en cause et dans les conditions décrites ci-dessus, en cas d'intervention d'une mesure de classement sans suite pour insuffisance de charges, de non-lieu, de relaxe ou d'acquittement.

La Commission prend note de ce que le ministère de la Défense s'engage à lui rendre compte chaque année de ses activités de vérification, de mise à jour et d'effacement des informations enregistrées dans le traitement.

Sur la durée de conservation

Le projet de décret précise que les données concernant les personnes majeures mises en cause seront, en principe, conservées vingt ans à compter de la date d'établissement de la procédure. Toutefois, les informations concernant certains crimes et délits figurant sur une liste annexée au décret seront conservées pendant quarante ans. En tout état de cause, les données relatives aux personnes âgées de plus de 75 ans seront systématiquement supprimées du fichier.

Par dérogation à ces règles, les informations relatives aux six catégories de contraventions de cinquième classe, aux délits routiers, aux délits d'abandon de famille et de non-représentation d'enfant et aux délits d'usage de stupéfiant seront conservées pendant cinq ans.

S'agissant des mineurs, le projet de décret prévoit que la durée de conservation de principe est de cinq ans, exception faite de certains crimes et délits graves énumérés dans deux listes annexées au décret, qui déterminent des durées de conservation, respectivement, de dix et vingt ans.

Le projet de décret prévoit, enfin, s'agissant des personnes mises en cause, que, dans l'hypothèse où une nouvelle infraction serait commise avant l'expiration de ces durées, l'ensemble des informations enregistrées serait alors conservé pendant le délai le plus long.

La durée de conservation des informations concernant les victimes est au maximum de quinze ans, sous réserve de la faculté qui leur est ouverte de demander la suppression des informations qui les concernent dès lors que l'auteur de l'infraction aura été définitivement condamné. Cette durée est prolongée jusqu'à la découverte des objets lorsque l'infraction porte sur des œuvres d'art, des bijoux ou des armes.

Dans leur principe, de telles durées paraissent justifiées par la finalité de recherche et d'identification des auteurs d'infractions, dès lors que les informations enregistrées sont mises à jour ou effacées selon les règles précédemment définies.

Sur l'information des personnes et l'exercice de leur droit d'accès

Les personnes concernées sont informées de la collecte des informations nominatives les concernant par une mention sur le service télématique et sur le site web de la gendarmerie nationale, par un affichage dans le local d'accueil du public de chaque unité élémentaire et par une mention sur l'attestation de dépôt de plainte remise aux victimes.

La Commission estime que ces mesures sont satisfaisantes au regard de la finalité du fichier et de l'importance de la population concernée et mettent les victimes en mesure d'exercer leur droit d'opposition à figurer dans le fichier après la condamnation définitive de l'auteur de l'infraction.

Dans la mesure où le traitement intéresse la sûreté de l'État, la défense et la sécurité publique, le droit d'accès s'exercera de manière indirecte, par l'intermédiaire des membres de la Commission appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes, conformément aux dispositions de l'article 39 de la loi du 6 janvier 1978. Toutefois, si le commissaire constate, en accord avec le ministère de la Défense et le procureur de la République compétent, et à la condition que la procédure concernée soit judiciairement close, que les informations ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique, celles-ci pourront être communiquées à l'intéressé.

Afin d'améliorer les modalités pratiques d'exercice du droit d'accès indirect, la Commission estime qu'il y a lieu d'envisager la possibilité pour les personnes ne faisant pas ou plus l'objet d'un signalement dans JUDEX d'en être informées à l'occasion de l'exercice de leur droit d'accès indirect et de prévoir, pour les personnes signalées dans le système JUDEX en tant que victimes, la communication du contenu de leur fiche JUDEX, après accord du ministère de la Défense.

Sur les mesures de sécurité adoptées

Afin de prévenir toute utilisation du système JUDEX à des fins étrangères à ses finalités, une procédure d'habilitation individuelle est mise en place. Cette habilitation comporte deux niveaux en matière de consultation à des fins administratives lorsque celles-ci sont autorisées.

Un système de journalisation des interrogations permet de conserver trace des connexions pendant trois ans et un historique des requêtes effectuées est mis en œuvre au niveau central.

De même, toute mise à jour (création, modification, suppression) provoquera l'enregistrement pendant trois ans des informations relatives au personnel qui y aura procédé.

Émet un avis conforme au projet de décret sous les réserves suivantes :
– à l'article 2, premier alinéa, après les mots : « *Lorsqu'elles concernent des personnes* » insérer les mots : « *Majeures ou mineures âgées de plus de dix ans* » ;
– à l'article 5, disjoindre le 2° relatif à la communication de données à des États ou à des organismes intergouvernementaux et communautaires et le faire figurer dans un nouvel article.

Demande au ministère de la Défense :
– d'envisager la possibilité pour les personnes ne faisant pas ou plus l'objet d'un signalement dans JUDEX d'en être informées à l'occasion de l'exercice de leur droit d'accès indirect et de prévoir, pour les personnes signalées dans le système JUDEX

en tant que victimes, la communication du contenu de leur fiche JUDEX, après accord du ministère de la Défense ;
– de confirmer que les communications de données prévues vers les autorités d'États ou organismes intergouvernementaux ou communautaires liés à la France par un accord international ou un acte de l'Union européenne ne sont réalisées qu'à la condition de présenter, pour la protection des données personnelles, des garanties équivalentes à celles du droit français.

Délibération n° 03-006 du 28 janvier 2003 portant avis sur le projet d'arrêté du maire de Roubaix portant création d'un traitement d'informations nominatives ayant pour objet de permettre la localisation et la cartographie des phénomènes de délinquance sur le territoire de la commune

Saisie par le maire de Roubaix d'un projet d'arrêté portant création d'un traitement d'informations nominatives ayant pour objet la localisation et la cartographie des phénomènes de délinquance sur le territoire de la commune ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu les articles 21 à 21-2 du Code de procédure pénale ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié ;

Vu le décret nº 2001-583 du 5 juillet 2001 pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées ;

Vu la délibération nº 00-064 du 19 décembre 2000 relatif à un projet de décret en Conseil d'État portant création du système de traitement des infractions constatées (STIC) et application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 ;

Vu le contrat local de sécurité signé le 4 mai 1999 entre les représentants de l'État, du parquet, de l'éducation nationale, du centre hospitalier et le maire de Roubaix ;

Vu la convention de coordination et de partenariat signé le 14 mars 2002 entre le préfet du Nord et le maire de Roubaix ;

Après avoir entendu Monsieur François Giquel, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

La mairie de Roubaix a saisi la Commission d'un projet d'arrêté portant création, au sein du service de police municipale, d'un traitement automatisé d'informations indirectement nominatives ayant pour objet la localisation et la cartographie des phénomènes de délinquance sur le territoire de la commune.

Cette application, prévue par l'article 6 de la convention de coordination et de partenariat passée entre la ville de Roubaix et l'État le 14 mars 2002, elle-même prévue par le contrat local de sécurité signé le 4 mai 1999, vise ainsi à disposer d'informations statistiques plus détaillées concernant la délinquance locale et est susceptible de servir d'outil d'aide à la décision en matière d'installation de systèmes de vidéosurveillance et de positionnement des caméras sur la voie publique.

Les informations utilisées pour constituer la base sont issues de deux traitements : le système de traitement d'infractions constatées (STIC) pour la police nationale, institué par un décret du 5 juillet 2001, et la base « service d'information centralisé » (SIC) pour la ville de Roubaix, traitement non nominatif recensant unique-

ment des faits de petite délinquance ainsi que leur localisation et alimenté par la police municipale et le service de médiation de la ville de Roubaix, à partir notamment d'informations non nominatives relatives à des événements et incidents fournies par une société de transport, deux bailleurs sociaux, un foyer de personnes âgées et une société commerciale s'agissant de son parc de véhicules.

La Commission relève que, s'agissant des informations issues du STIC et conformément aux dispositions de l'article 5 du décret du 5 juillet 2001, aucune information permettant l'identification directe des victimes ou des personnes mises en cause n'est transmise à la police municipale. Les services de police nationale utilisent à cette fin un logiciel statistique, « Geoprevention 4001 », sur les caractéristiques duquel la Commission a souhaité recueillir les observations du ministère de l'Intérieur, observations qui ne lui sont pas encore parvenues.

Les catégories d'informations collectées sont aux termes du dossier de demande d'avis : l'origine du fichier utilisé, les faits concernés (le type d'infraction, l'information selon laquelle elle a été commise ou seulement tentée, un commentaire non nominatif), la localisation géographique de la commission des faits (numéro, voie, secteur, quartier, commune, département, qualification du lieu, type précis de lieu), la date et l'heure des faits, le sexe, la tranche d'âge et la catégorie socioprofessionnelle de la victime, le nombre d'auteurs et leur tranche d'âge, la présence d'armes, l'indication « usage » ou « trafic » en cas d'infraction à la réglementation sur les stupéfiants.

La Commission observe toutefois que certaines de ces catégories d'informations ne figurent pas expressément dans le projet d'acte réglementaire (définition objective des faits ou événements concernés, présence ou non d'une arme pour le mis en cause et les précisions « usage » ou « trafic » en cas d'infraction à la réglementation sur les stupéfiants) : il devra être complété en conséquence avant publication.

La Commission estime en outre que seules des informations objectives et pertinentes doivent être utilisées pour dresser la cartographie de la délinquance sur le territoire de la commune de Roubaix et qu'en conséquence, seules peuvent être enregistrées dans le traitement projeté des informations relatives à des faits ou des événements relevant de catégories précises et définies préalablement à toute collecte.

Le seul traitement appliqué aux informations ainsi transmises consiste en leur représentation, sous la forme de points géocodés sur un plan de la ville, à l'adresse de commission des faits, ainsi que, pour chaque point, la liste des informations qui lui sont associées, c'est-à-dire celles relatives à l'infraction ainsi matérialisée.

La mairie de Roubaix prévoit, pour la base de données ainsi constituée et les informations utilisées à cette fin, des durées de conservation identiques à celles prévues par le décret du 5 juillet 2001 portant création du STIC. La Commission estime qu'eu égard à la finalité du traitement, qui vise à disposer d'une représentation cartographique mise à jour hebdomadairement des infractions constatées sur le territoire de la commune de Roubaix, cette durée de conservation est excessive.

La Commission relève qu'aux termes du projet d'arrêté seuls le directeur du service prévention et relations police justice, l'opérateur de saisie, le chef de la police municipale et le chef du service prévention auront accès aux informations permettant d'établir leur représentation cartographique et qu'en outre, la carte résultant de ce traitement ne sera pas rendue publique mais est réservée à la seule connaissance de ces mêmes personnes, du maire, des adjoints au maire et des maires de quartier, du personnel de la ville chargé de la police municipale et de la prévention et des partenaires de la ville au contrat local de sécurité. Elle considère que la limitation

des possibilités de consultation et de diffusion des cartes constitue une garantie en matière de protection des libertés.

La Commission considère que, eu égard aux caractéristiques spécifiques de cet outil de cartographie et, en particulier, à l'application nouvelle qui est en faite pour parvenir à une meilleure connaissance de la délinquance locale, à la multiplicité des sources potentielles d'alimentation de ce traitement, au manque de pertinence que peut revêtir l'enregistrement de faits ou d'événements qui ne sont pas tous constitutifs d'infractions pénales et à l'incertitude relative à la précision de la collecte de l'adresse de commission des infractions ou de survenance des faits recensés, il y a lieu de limiter l'autorisation de mise en œuvre de ce traitement à une durée expérimentale d'une année à compter de la publication de l'arrêté municipal en portant création.

La Commission procédera dans ce délai à une mission de contrôle sur place au cours de laquelle elle vérifiera la conformité du traitement projeté aux dispositions de la loi du 6 janvier 1978 et en particulier la pertinence des informations enregistrées.

Émet en conséquence **un avis favorable** au projet d'arrêté portant création, au sein du service de police municipale, d'un traitement automatisé de données indirectement nominatives ayant pour objet la localisation et la cartographie des phénomènes de délinquance sur le territoire de la commune de Roubaix, sous réserve, pour cette commune :

– de limiter en l'état la mise en œuvre de ce traitement et donc la durée de conservation des données à une durée expérimentale d'un an à compter de la publication de l'arrêté municipal en portant création ;

– de compléter l'article 2 de ce projet d'arrêté afin qu'il mentionne l'ensemble des informations collectées et traitées et tout particulièrement en l'espèce la définition objective des faits ou événements concernés.

Délibération n° 03-016 du 24 avril 2003 portant avis sur un projet d'arrêté du préfet de Haute-Savoie relatif à un traitement automatisé ayant pour finalité la constitution d'un fichier des personnes titulaires d'un badge permanent d'entrée dans le périmètre de protection du sommet des chefs d'État (G8)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le préfet de Haute-Savoie d'un projet d'arrêté relatif à la constitution d'un fichier des personnes titulaires d'un badge permanent d'entrée dans le périmètre de protection (zone 1) du sommet des chefs d'État (G8) qui se tient à Évian du 1er au 3 juin 2003 ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, ensemble le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Après avoir entendu Monsieur François Giquel, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Dans le cadre des mesures de sécurité mises en place à l'occasion de l'organisation du sommet des chefs d'État (G8) qui se tient à Évian du 1er au 3 juin 2003, le préfet de Haute-Savoie a décidé de limiter, pendant cette période, l'accès au périmètre de protection du lieu de tenue du sommet. Il est ainsi prévu que seules pourront accéder à cette zone les personnes titulaires d'un badge attestant qu'elles y résident ou qu'elles y exercent une activité professionnelle.

Pour faciliter la délivrance des badges, un traitement automatisé d'informations nominatives sera mis en œuvre par la direction départementale des renseignements généraux de Haute-Savoie sur des moyens informatiques réservés à ce seul usage.

Le traitement n'enregistrera que les informations communiquées par les personnes s'étant présentées volontairement aux permanences d'accueil des trois communes situées dans le périmètre de protection, à savoir Évian-les-Bains, Neuvecelle et publier et ayant justifié de leur identité et le cas échéant de l'exercice d'une activité professionnelle dans la zone de protection. Ces informations concernent les noms et prénoms de la personne, sa date de naissance, l'adresse du domicile et le numéro d'immatriculation du véhicule que la personne est susceptible d'utiliser dans la zone de protection (un macaron étant alors apposé sur le véhicule).

La Commission prend acte :
– qu'aucun autre fichier ne sera consulté pour assurer la délivrance des badges ;
– que la finalité du traitement est strictement limitée à la gestion des badges permanents et qu'aucune consultation, qu'elle soit ponctuelle ou systématique, de fichiers de police tels que le fichier des personnes recherchées ou le fichier des véhicules volés ne sera réalisée ;

– que seuls les personnels des services de la police nationale habilités à effectuer des opérations de vérifications aux abords et à l'intérieur du périmètre de protection, pourront être destinataires des informations contenues dans le fichier ;
– que le traitement automatisé et les données nominatives qu'il contient seront détruits le 6 juin 2003.

La Commission demande à cet égard qu'un procès verbal de destruction du fichier soit établi et lui soit adressé.

La Commission estime que compte tenu des garanties ainsi prises et eu égard aux impératifs particuliers de sécurité auxquels doit répondre l'organisation du sommet du G8, la mise en œuvre de ce traitement n'est pas disproportionnée aux objectifs poursuivis.

Émet, au bénéfice des observations qui précèdent, **un avis favorable** sur le projet d'arrêté présenté par le préfet de Haute-Savoie.

Délibération n° 03-029 du 22 mai 2003 concernant la création par la direction générale des douanes et droits indirects d'un système d'information de lutte contre la fraude

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie d'un projet d'arrêté « portant création à la direction générale des douanes et droits indirects d'un système informatisé concourant au dispositif de lutte contre les fraudes » (SI LCF), que complètent les autres documents inclus dans la demande d'avis du ministère ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment les articles 34 et 39, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le Code des douanes communautaire ;

Vu le Code des douanes, notamment les articles 65 A*bis*, 350, 392 et suivants et 464 ;

Vu le Code général des impôts, notamment l'article 1649*quater* A ;

Vu le livre des procédures fiscales, notamment les articles L. 80 J et L. 83 A ;

Vu l'arrêté du 23 avril 1993 relatif au fichier national informatisé de documentation de la direction générale des douanes et droits indirects ;

Après avoir entendu Monsieur Jean-Pierre de Longevialle, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le système d'information SI LCF développé par la direction générale des douanes et droits indirects (DGDDI) est appelé à remplacer, au terme d'une période d'expérimentation, l'actuel fichier national informatisé de documentation (FNID) qui a donné lieu à deux avis de la CNIL en date des 5 février 1980 et 17 mars 1992. Il a la même finalité générale – apporter une aide à la bonne exécution des missions de recherche, de constatation, de poursuite et de répression des fraudes qui sont confiées à la douane, notamment dans le cadre de ses compétences en matière économique, fiscale et de protection de l'espace national et communautaire – et sensiblement le même périmètre.

Par rapport au FNID, le nouveau système d'information national vise à améliorer, d'une part, la saisie des données relatives aux fraudes constatées – qui sera directement effectuée par les services de contrôle dans les cinq jours suivant la constatation – et des éléments susceptibles de permettre la détection des risques de fraude – dont certains n'étaient pas jusqu'à présent traités sur support informatique –, d'autre part, leur exploitation par un plus grand nombre d'agents des douanes, notamment ceux des services spécialisés dans l'analyse des risques de fraude et le traitement du renseignement qui contribuent à l'orientation des contrôles douaniers. Une plus grande efficacité dans la recherche des infractions que la douane est habilitée à constater en est attendue.

La CNIL considère qu'une telle centralisation d'informations nominatives et leur mise à la disposition d'un grand nombre de destinataires potentiels appellent nécessairement à la vigilance et à la reconnaissance de garanties sérieuses destinées à prévenir :
– tout fichage de personnes non contrôlé, erroné ou abusif ;
– toute utilisation d'un tel traitement à des fins étrangères à celles qui ont légalement été prévues ;
– toute mise à la disposition d'un agent des douanes d'informations dont il n'a pas à connaître pour l'accomplissement des missions qui lui sont dévolues ;
– toute transmission d'informations à des tiers qui serait dépourvue d'un fondement juridique ou qui serait excessive au regard des dispositions légales.

Sur l'alimentation du système d'information

Les personnes concernées

Le projet d'arrêté transmis à la CNIL énumère à l'article 2 les différentes catégories de personnes pour lesquelles des informations directement ou indirectement nominatives peuvent être enregistrées.

. La catégorie la plus importante en nombre est celle des personnes impliquées dans une ou plusieurs fraudes constatées par la douane

Pour lesquelles des « fiches de constatations réalisées » sont directement saisies dans le SI LCF, que les actes de poursuite ultérieurs incombent ou non à la douane. Parmi celles-ci, il y a lieu de distinguer :

1) Les personnes dont la participation dans la fraude a été directement constatée lors des contrôles physiques de la douane ou à partir des déclarations en douane effectuées, y compris sur le fondement de présomptions légales, telles que les détenteurs des marchandises de fraude, les capitaines de navires, les commandants d'aéronefs, les signataires des déclarations, les commissionnaires en douane agréés et les soumissionnaires.

La CNIL fait observer que ne peuvent être inscrits à ce titre dans le SI LCF que des noms tirés des déclarations en douane ou figurant dans un acte de procédure se présentant sous la forme d'un procès verbal de constatation ou de saisie régulièrement établi ou de tout autre acte de constatation ou de règlement transactionnel pouvant être assimilé à des procès verbaux.

Il est précisé par la direction générale des douanes qu'aucune information ne doit être saisie dans le SI LCF lorsque les agents des douanes se contentent de procéder à la retenue provisoire des personnes aux fins de mise à disposition d'un officier de police judiciaire sur le fondement du signalement dont elles font l'objet dans le système d'information Schengen ou dans un fichier du ministère de l'Intérieur ou du signalement d'une marchandise dont elles sont détentrices.

2) Les personnes autres que celles déjà mentionnées qui sont réputées par la loi pénalement responsables d'une fraude constatée, telles que, pour ce qui concerne les seuls délits douaniers, les personnes *« intéressées à la fraude »* au sens de l'article 399 du Code des douanes, notamment celles ayant un intérêt direct à la fraude.

La CNIL fait observer que ne peuvent être inscrites à ce dernier titre que des personnes ayant eu conscience de coopérer à une opération irrégulière pouvant aboutir à une fraude dont les noms figurent dans les pièces de procédure rédigées par la douane.

. Le SI LCF permet la collecte d'informations sur des personnes qui sont seulement soupçonnées de fraude

La CNIL considère qu'aucune personne ne doit faire l'objet d'un avis de fraude ou d'une enquête sur la base d'un simple soupçon ou d'une dénonciation malveillante ou non étayée. Le dispositif conçu par la douane est de nature à garantir le respect de ces conditions, dès lors que le projet d'arrêté qui lui est soumis précise que :
– seules les personnes à l'encontre desquelles existent une ou plusieurs raisons plausibles de leur implication dans une fraude peuvent faire l'objet d'une fiche de risque de fraude ou d'une demande d'enquête ;
– seules des informations enrichies puis validées par un service national ou régional, spécialisé dans l'analyse du risque et le traitement du renseignement peuvent faire l'objet d'une enquête ou d'un avis de fraude consultable par les services investis d'une mission de contrôle, notamment les services de surveillance et les services de contrôle des opérations commerciales et des contributions indirectes.

La catégorie des personnes détentrices d'une marchandise qui a fait l'objet, au cours d'un contrôle, d'un prélèvement d'échantillons aux fins d'analyse et d'expertise par un laboratoire des douanes peut être rapprochée de celle des personnes à l'égard desquelles existent des risques de fraude.

. Les autres informations nominatives ne sont liées à aucune fraude constatée ou soupçonnée

Elles concernent, outre les différentes catégories d'agents des douanes mentionnées à l'article 2 :
– les personnes qui ont déclaré à la douane, en application de l'article 464 du Code des douanes, un transfert de sommes, titres ou valeurs à destination ou en provenance de l'étranger, effectué sans l'intermédiaire d'un établissement de crédit ou assimilé ;
– les personnes autres que celles déjà mentionnées, qui sont tenues solidairement pour le paiement des droits et taxes éludés, pénalités et autres sommes dues par les personnes responsables d'une fraude.

La CNIL estime que le regroupement dans un même système d'information de données se rapportant à des catégories de personnes aussi diverses n'est pas, par elle-même, contraire à la loi du 6 janvier 1978, si l'enregistrement des informations les concernant est adéquat, pertinent et non excessif au regard de l'une ou l'autre des finalités précises du traitement, si la durée de leur conservation sous forme nominative est elle-même chaque fois pertinente au regard des finalités qui en ont justifié la saisie, si la consultation de chaque catégorie de signalements n'est ouverte qu'aux seules personnes dûment habilitées pour en connaître, et si tout risque de confusion sur le motif de l'enregistrement est écarté chez les utilisateurs des informations. C'est notamment au regard de ces règles que la CNIL a examiné la conformité du projet de la DGDDI à la loi du 6 janvier 1978.

Les catégories d'informations traitées

Les informations relatives aux fraudes constatées se rapportent aux éléments matériels de la fraude, aux personnes impliquées, à la nature de la fraude et à la qualification de l'infraction. Elles sont enregistrées par le service ayant effectué les constatations, puis complétées par des données relatives au suivi du dossier contentieux, notamment en cas de procédures juridictionnelles, et aux opérations de recouvre-

ment, saisies ultérieurement par les services contentieux des directions régionales des douanes et par les recettes des douanes.

Par dérogation, les constatations d'infraction auxquelles l'administration décide de ne pas donner de suites contentieuses ne se traduiront que par la conservation d'informations non nominatives, à moins que les nécessités du recouvrement ultérieur des droits et taxes dus n'imposent de disposer de l'identité des redevables.

La CNIL prend acte que le SI LCF ne doit comporter aucune indication sur les condamnations pénales prononcées à l'encontre des auteurs d'infraction, à l'exception des condamnations pécuniaires dont le produit est recouvré par la douane, ni aucune donnée sensible au sens de l'article 31 de la loi du 6 janvier 1978.

La CNIL recommande à la douane d'être tout spécialement vigilante à l'égard du contenu des zones de commentaires qui sont surtout développées pour les risques de fraude. L'avant-dernier alinéa de l'article 3 du projet d'arrêté dispose que ces zones de texte libre ne comportent pas d'autres catégories d'information que celles énumérées au même article.

La CNIL prend acte que la DGDDI diffusera une instruction rappelant notamment que ces zones ne doivent, en aucun cas, intégrer de données mentionnées aux articles 18 et 31 de la loi du 6 janvier 1978. Le dispositif de validation systématique par un service spécialisé de la plupart des informations enregistrées, notamment des données sur les constatations réalisées et les signalements de fraude, permet d'assurer le respect de ces dispositions.

Sur la mise à jour des informations enregistrées

Aux termes de l'article 37 de la loi du 6 janvier 1978, un fichier nominatif doit être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert la connaissance de l'inexactitude ou du caractère incomplet d'une information qui y figure. Il appartient au responsable du traitement d'organiser les circuits d'informations et les mécanismes de surveillance qui lui permettront de donner toute sa portée à cette disposition.

Il convient d'abord que la douane rappelle aux administrations et organismes qui lui transmettent des informations qu'ils doivent porter à sa connaissance toute mise à jour ou actualisation des informations communiquées dont ils seraient informés.

Par ailleurs, le projet d'arrêté prévoit l'effacement pur et simple de l'ensemble des informations relatives aux personnes bénéficiant d'une mesure d'amnistie ou d'une décision de justice définitive ne retenant pas leur responsabilité dans la commission des infractions initialement relevées à leur encontre.

Cependant, les conditions de mise à jour des informations pour tenir compte des décisions de justice se présentent différemment selon que les informations conservées dans le SI LCF se rapportent à des fraudes poursuivies et réprimées par la douane ou à des fraudes dont la poursuite ne relève pas de ses missions.

Lorsque les services du contentieux des directions régionales de la douane sont en charge des poursuites – en présence de contraventions ou délits douaniers ou de délits concernant les contributions indirectes ou les réglementations assimilées –, il leur appartiendra de mettre à jour ou de supprimer sans délai les informations enregistrées sur la base des décisions de justice devenues définitives, tout particulièrement des décisions de relaxe ou d'acquittement et des décisions de non-lieu, ainsi que de s'assurer de la concordance entre la qualification juridique des faits qui figure dans le SI LCF et celle retenue par la juridiction.

Lorsque le rôle de la DGDDI se limite normalement à transmettre la procédure au parquet territorialement compétent et, s'il y a lieu, à d'autres autorités administratives désignées par la loi, les services de la douane risquent de ne pas être informés des suites judiciaires réservées aux fraudes constatées qui sont enregistrées dans le SI LCF.

C'est pourquoi il a paru nécessaire de prévoir, pour les fraudes dont la poursuite n'incombe pas à la douane, la mise en place d'une procédure spéciale, annuelle, d'actualisation des informations nominatives à partir de données obtenues des autorités judiciaires, dont l'organisation suppose en conséquence la coopération des parquets. En l'absence de réponse de ces derniers, le projet d'arrêté dispose, à la demande de la CNIL, que les informations directement ou indirectement nominatives sont effacées au terme d'un délai de dix-huit mois à compter de leur dernière actualisation. La CNIL considère que la mise en œuvre effective de ce dispositif est seule de nature à assurer le respect des prescriptions de l'article 37 de la loi du 6 janvier 1978. Elle demande donc à être informée annuellement des diligences accomplies par la DGDDI pour assurer la mise à jour et l'apurement des informations nominatives conservées dans le SI LCF. Le projet d'arrêté devra être complété sur ce point.

Sur la durée de conservation des informations

Le projet d'arrêté prévoit que les informations nominatives relatives aux fraudes constatées ne peuvent pas être conservées au-delà d'un délai de dix ans à compter de l'année de la constatation. Cette durée est réduite à cinq ans pour les informations relatives à des contraventions ayant donné lieu à une amende, recouvrée par la douane, inférieure à 1 000 euros.

Cependant, pour les personnes récidivistes, la durée de conservation la plus longue calculée sur la base des règles précitées est appliquée à l'ensemble des informations relatives aux fraudes dont elles sont responsables. Il convient cependant que cet allongement de la durée de conservation soit sans incidence sur les délais appliqués aux signalements dont font l'objet les co-responsables des mêmes fraudes lorsqu'aucune nouvelle infraction ne leur est imputée.

Par ailleurs, si dans les délais précités, le paiement de la totalité des sommes dues au titre des droits, taxes, amendes et pénalités n'a pas pu être obtenu, les informations nécessaires au recouvrement des sommes restant dues sont conservées jusqu'à leur complet paiement.

Les informations nominatives relatives à l'existence d'un risque de fraude, à une demande d'enquête, à une demande d'analyse ou d'expertise d'une marchandise, ainsi qu'au respect de l'obligation déclarative des mouvements de sommes, titres ou valeurs ne sont pas normalement conservées au-delà de trois ans. Par exception, ce délai peut être renouvelé une fois pour autant que, s'agissant d'une demande d'enquête, les premières diligences aient été accomplies, ou que, pour les données relatives à un risque de fraude, des éléments objectifs nouveaux concernant la même personne aient été enregistrés.

Il ressort également du projet d'arrêté que les informations nominatives traitées par les services spécialisés d'enquête ne sont pas conservées après la conclusion de l'enquête qui a justifié leur recueil, à l'exception de celles qui sont reprises dans des fiches de constatations réalisées, qui en suivent le régime.

La CNIL considère que les durées de conservation appliquées à chacune des catégories d'informations précitées ne sont pas excessives, dès lors que les règles

retenues tiennent compte de leur nature, des finalités qui en justifient l'enregistrement, de la qualification juridique des faits auxquels elles se rapportent, des conséquences qui leur sont attachées, ainsi que des antécédents de la personne concernée.

Sur l'utilisation du SI LCF et les destinataires des informations

L'utilisation du traitement par les agents des douanes

Le SI LCF est d'abord destiné à être utilisé au sein de la DGDDI au titre de la constatation des fraudes. Il doit permettre aux agents dûment habilités qui sont investis d'une mission de lutte contre la fraude, notamment à ceux des services de surveillance et des services de contrôle des opérations commerciales et des contributions indirectes, d'enregistrer les éléments matériels des constatations auxquelles ils ont procédé.

La CNIL rappelle que ces données devront exclusivement provenir de procès-verbaux de constatation ou de saisie, de documents établis à l'occasion d'un règlement transactionnel ou de tout autre acte de constatation également formalisé.

Les mêmes informations sont également destinées à être exploitées et complétées par les agents habilités des services du contentieux des directions régionales des douanes pour la gestion des transactions et des procédures juridictionnelles et le contrôle de l'exécution des décisions de justice. De même, les agents habilités des recettes des douanes compétentes pour procéder au recouvrement des droits et taxes éludés, des pénalités et autres sommes dues sont destinataires des informations y afférant et les complètent à ce titre.

Cependant, la finalité principale du SI LCF consiste, pour la DGDDI, dans la recherche des fraudes, qui constitue l'unique justification de la saisie d'un grand nombre d'informations.

Certaines de ces informations ne peuvent être consultées que par les agents habilités des services régionaux ou nationaux spécialisés dans l'analyse du risque et le traitement du renseignement, qui sont chargés de leur analyse et de leur enrichissement. Elles sont relatives non seulement aux signalements de risque de fraude, mais aussi aux déclarations de transfert de sommes, titres ou valeurs à destination ou en provenance de l'étranger, déposées en application de l'article 464 du Code des douanes, qui sont susceptibles de fournir des indices de réseaux de blanchiment.

Ces informations restent réservées à ces services aussi longtemps qu'ils ne les ont pas reprises sous la forme de fiches d'enquête ou d'avis de fraude comportant éventuellement l'identité de personnes à contrôler. Par exception, les agents des services ayant signalé un risque de fraude ont toujours la possibilité d'accéder aux informations s'y rapportant.

D'autres informations peuvent être consultées, pour favoriser le ciblage des contrôles douaniers, par l'ensemble des agents investis d'une mission de lutte contre la fraude : il s'agit des avis de fraude validés par les services d'analyse des risques de fraude et des informations relatives aux éléments matériels et aux auteurs des fraudes antérieurement constatées.

Le traitement permet le suivi du déroulement des enquêtes, les agents dûment habilités des services d'enquête y enregistrant et y consultant les informations correspondant aux investigations qui leur ont été confiées. Les agents des autres services sont seulement informés qu'une personne fait l'objet d'une demande d'enquête.

Les agents habilités des laboratoires des douanes peuvent, en outre, consulter et compléter les informations relatives aux demandes d'analyse et d'expertise d'une marchandise.

Le SI LCF doit enfin faciliter le pilotage des actions de la douane en matière de lutte contre la fraude. C'est à ce titre que les agents dûment habilités de l'administration centrale chargés de cette mission ont accès à l'ensemble des informations du SI LCF et que les autorités hiérarchiques des services peuvent accéder à l'ensemble des informations relatives à l'activité des services qui relèvent de leur compétence.

Par ailleurs, la CNIL prend acte des précisions apportées par l'administration selon lesquelles les agents des douanes habilités à effectuer des enquêtes judiciaires, dont les compétences sont fixées par l'article 28-1 du Code de procédure pénale, n'ont pas directement accès au SI LCF.

Les utilisations externes des informations contenues dans le SI LCF

Une proportion non négligeable des informations nominatives enregistrées est susceptible d'être communiquée à des partenaires extérieurs, français, communautaires ou étrangers.

Cette perspective appelle à une vigilance particulière. En effet, toute cession d'informations, en particulier vers l'étranger, peut entraîner un risque de détournement de finalité ou de mise en péril des informations dont il s'agit.

Par ailleurs, le SI LCF constitue un fichier d'infractions. Or, la CNIL veille à ce que de tels fichiers, qui peuvent permettre de répertorier l'ensemble des procédures dans lesquelles une même personne a pu être mise en cause, ne soient pas utilisés comme des casiers judiciaires parallèles, alors même qu'ils n'offrent pas les mêmes garanties que le casier judiciaire en termes de certitude de la culpabilité et d'effacement des informations lorsque la loi le prévoit.

La CNIL prend acte de ce que les cessions d'informations aux partenaires de la douane dans le cadre de coopérations instituées sont, à la date de la présente délibération, celles prévues par le projet d'arrêté. Elles bénéficient :
– à la direction générale des impôts, pour les déclarations de transfert de sommes, titres ou valeurs à destination ou en provenance de l'étranger, les informations relatives aux sommes qui n'ont pas donné lieu au dépôt de la déclaration requise, ainsi que les informations destinées à prévenir les manquements aux règles de facturation dans les échanges intracommunautaires ;
– aux agents de la cellule Tracfin, pour les informations susceptibles d'être utilisées dans la lutte contre le blanchiment de capitaux ;
– aux services habilités de la Commission européenne, pour les informations relatives aux constatations de fraude portant sur un montant de droits de douane supérieur à 10 000 euros et aux cas de fraude ou d'irrégularité concernant le FEOGA-garantie lorsque les montants en jeu sont égaux ou supérieurs à 4 000 euros.

Il ressort cependant du dossier que d'autres cessions d'informations sont envisagées à brève échéance, par exemple avec Europol. La CNIL rappelle que toute modification de l'actuel dispositif de transfert d'informations au bénéfice d'une administration, nationale ou communautaire, quel que soit le support utilisé, ne peut intervenir qu'après avoir fait l'objet d'une déclaration de modification.

Le projet d'arrêté prévoit, de manière générale, que des informations peuvent être cédées aux autorités étrangères des États et organismes intergouvernementaux liés à la France, par un accord international ou un instrument communautaire

leur permettant de connaître, dans la limite des dispositions prévues par ces textes, des informations recueillies par la DGDDI.

La CNIL prend acte, s'agissant des transferts d'informations à destination de services étrangers, que la DGDDI s'assurera de la pertinence des données demandées au regard des accords conclus et de l'existence, à destination, de garanties équivalentes à celles du droit interne en matière de protection des données à caractère personnel. Elle note également qu'aucune transmission d'informations nominatives vers l'étranger ne sera réalisée sur le seul fondement du paragraphe 6 de l'article 65 du Code des douanes.

La CNIL considère que les extractions de fichiers d'informations directement ou indirectement nominatives effectuées en vue de leur transmission à toute administration nationale, communautaire, étrangère ou internationale doivent être réalisées par l'intermédiaire et sous le contrôle du bureau de l'administration centrale chargé du pilotage de la lutte contre la fraude. Compte tenu du caractère évolutif et de la relative imprécision du dossier sur ce point, la CNIL ne peut émettre un avis favorable qu'à la condition de recevoir chaque année de la DGDDI la liste exhaustive des extractions effectuées et de leurs bénéficiaires. Le projet d'arrêté devra être modifié sur ce point.

Par ailleurs, les informations sont communicables aux parquets ainsi que, sous réserve qu'une enquête judiciaire soit diligentée, aux agents des douanes habilités pour mener des enquêtes judiciaires ou aux officiers de police judiciaire compétents, notamment à ceux des offices centraux de police judiciaire lorsque les textes qui les régissent le prévoient.

La CNIL fait observer que les seules informations qui peuvent être jointes aux dossiers de procédure transmis aux parquets sont celles relatives aux procédures en cours, à l'exclusion de celles concernant les affaires pour lesquelles la procédure judiciaire est close.

De même, lorsque la douane n'est pas compétente pour la poursuite des infractions qu'elle a constatées, elle communique aux administrations ou services intéressés les informations correspondantes lorsque les dispositions légales le permettent.

S'agissant de la communication ponctuelle d'informations à des administrations ou organismes tiers autorisés, par exemple en application d'un droit de communication ou de pouvoirs d'enquête, la CNIL rappelle que les tiers autorisés ne peuvent bénéficier de transferts d'informations qu'en réponse à des demandes ponctuelles, portant sur une affaire ou une personne déterminée, et trouvant leur fondement légal dans un texte attribuant au bénéficiaire, par exemple, un droit général de communication ou d'investigation.

Il en résulte que des informations ne doivent être transmises à un tiers autorisé que sur présentation d'une demande formalisée qui devra être conservée. Le motif de la recherche d'informations saisi à cette occasion devra préciser l'organisme à l'origine de la requête, son étendue et son fondement juridique.

La CNIL souhaite qu'une instruction, régulièrement tenue à jour, soit consacrée au recensement de l'ensemble des circonstances dans lesquelles les services douaniers ont l'obligation ou la faculté de transmettre à d'autres administrations des informations nominatives portant sur les constatations effectuées par la douane ou sur les risques de fraude. Elle souhaite également avoir connaissance de ce document, dont l'élaboration lui semble une priorité, qui devrait apporter une aide aux agents des douanes saisis de demandes de communication et prévenir toute transmission à des tiers non autorisés des informations nominatives détenues par la DGDDI.

Sur le contrôle de l'utilisation et de la transmission des informations

Les seules personnes à pouvoir bénéficier d'un accès direct au SI LCF sont les agents de la DGDDI dûment habilités, sous réserve qu'ils puissent se connecter au système informatique suivant une procédure d'identification individuelle. Les autres destinataires ne peuvent avoir communication d'informations que sur la base d'extractions, à l'exclusion de toute connexion directe au SI LCF.

Le SI LCF comportant des données confidentielles, la douane met en place un dispositif spécifique de sécurité et de surveillance, afin de garantir le respect des règles relatives à la consultation et à l'exploitation des informations enregistrées dans la base et, par voie de conséquence, la protection des données qui y sont conservées.

Ce dispositif de journalisation des interrogations comporte l'enregistrement, sur un support inaltérable, pour chaque intervention d'un agent dans le SI LCF – notamment les intégrations, consultations, modifications et annulations d'informations – de l'identité de l'auteur de la requête, du motif précis et concret invoqué à l'appui de la recherche – qui sera obligatoirement saisi avant son lancement – et, lorsque celle-ci est effectuée pour le compte d'une personne n'appartenant pas à la DGDDI, de son fondement juridique.

Ces informations sont conservées pendant cinq ans et pourront être utilisées pour des besoins d'audit hiérarchique, à des fins statistiques ou de contrôle par les autorités judiciaires. Elles pourront également être consultées et exploitées par la CNIL dans l'exercice de ses missions de contrôle.

La CNIL prend acte de ce dispositif mais estime qu'il doit être complété par des procédures de contrôle *a posteriori*. Elle recommande, à cet égard, le développement de logiciels d'analyse des fichiers de traces permettant notamment d'identifier les accès à un dossier particulier ainsi que les actions – mise à jour, consultation, recherche… – réalisées par un utilisateur, et que la mise en œuvre, à une fréquence à déterminer, de ces logiciels d'analyse soit confiée à une structure indépendante, telle que l'inspection générale des services, et porte au moins sur 1 % des interrogations de la base.

La CNIL suggère également que toute première connexion au traitement provoque l'affichage d'une page écran informant les utilisateurs que les données de connexion permettant d'identifier les interrogations et leur auteur sont conservées pendant cinq ans et que l'ensemble des agents des douanes en soit par ailleurs informé par une circulaire rappelant que toute consultation du fichier à des fins étrangères aux finalités mentionnées dans l'arrêté portant création du SI LCF constitue le délit de détournement de finalité réprimé par l'article 226-21 du Code pénal.

La CNIL demande également que le responsable du traitement, représenté par le service en charge du pilotage de la lutte contre la fraude, l'informe chaque année des diligences accomplies pour vérifier la correcte utilisation du traitement et le contrôle des interrogations. Le projet d'arrêté devra être modifié sur ce point.

Sur les autres mesures de sécurité

La Commission recommande un renforcement du dispositif assurant la sécurité et la confidentialité d'ensemble du réseau Intranet du SI LCF par le chiffrement du transport des données, par exemple au moyen du protocole SSL associé à une clé d'une longueur de 128 bits.

Pour les postes de travail fixes, la fiabilité du procédé d'authentification du couple nom/mot de passe devrait être renforcée par :
– l'obligation d'utiliser des mots de passe d'une longueur d'au moins huit caractères ;
– l'interdiction d'utiliser des mots de passe trop faciles à deviner, tels que les : nom, prénom et date de naissance ;
– l'obligation de renouveler le mot de passe une fois tous les deux mois ;
– l'impossibilité de réutiliser les trois mots de passe précédemment utilisés lors du renouvellement d'un mot de passe ;
– l'invalidation du code d'accès au SI LCF de l'utilisateur après plus de trois essais de connexion successifs infructueux ;
– la déconnexion automatique après une durée d'inactivité à déterminer ;
– l'affichage, lors de la connexion, de la date et l'heure de la précédente connexion effectuée à partir du même compte.

La Commission recommande enfin le renforcement par un procédé d'authentification fort, par exemple à base de carte à puce associée ou non à un identifiant biométrique, des contrôles d'accès au SI LCF dans les situations les plus exposées, notamment :
– en cas d'utilisation de micro-ordinateurs portatifs ou d'autres dispositifs mobiles pour l'accès au traitement ;
– pour les personnels disposant de droits privilégiés d'accès aux données du SI LCF, tels que les super-utilisateurs, administrateurs système et gestionnaires de la base de données.

Sur la mise en œuvre des droits d'accès et de rectification et l'information des personnes

Le projet d'arrêté prévoit que les droits d'accès et de rectification s'exercent auprès des directions régionales des douanes, même si la DGDDI souhaite assurer la cohérence des décisions relatives au droit d'accès, en confiant à un seul service de l'administration centrale le soin de leur répondre.

Lorsque la douane estime que tout ou partie des informations demandées intéresse la sûreté de l'État, la défense ou la sécurité publique au sens de l'article 39 de la loi du 6 janvier 1978 ou sont couvertes par une règle de secret résultant d'une convention internationale, elle transmet la demande à la CNIL. Celle-ci délimite, le cas échéant, les informations qui sont communicables de plein droit par application de l'article 34 et celles qui relèvent de la procédure de l'article 39 modifié.

La CNIL **recommande**, par ailleurs, que les personnes concernées soient informées de l'existence du traitement SI LCF et des modalités d'exercice des droits qui leur sont reconnus par les articles 34 et suivants de la loi du 6 janvier 1978, d'une part, par une mention sur les documents qui leur sont adressés par la douane lors de la constatation d'une fraude et sur les formulaires de déclaration des transferts de capitaux et, d'autre part, par l'affichage de l'arrêté portant création du traitement dans les locaux de la douane ouverts au public et via le site internet de la douane.

Au bénéfice des observations et recommandations qui précèdent, la commission **émet un avis favorable** sur le projet d'arrêté du ministère de l'Économie, des Finances et de l'Industrie relatif au traitement SI LCF de la direction générale des douanes et droits indirects sous réserve de l'adjonction, avant le dernier article, d'un nouvel article ainsi rédigé : *« La Commission nationale de l'informatique et des libertés recevra chaque année un rapport décrivant la liste des extractions de données effectuées en vue de leur transmission à toute administration nationale, communautaire, étrangère ou internationale, ainsi que les diligences faites pour assurer la vérification, la mise à jour et l'apurement du traitement et le contrôle des interrogations. »*

Délibération n° 03-041 du 23 septembre 2003 portant avis sur un projet d'arrêté interministériel portant création d'un dispositif expérimental visant à automatiser la constatation de certaines infractions routières et l'envoi de l'avis de contravention correspondant et sur un projet d'arrêté modifiant l'arrêté du 29 juin 1992 portant création du système national des permis de conduire

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère de l'Intérieur d'un projet d'arrêté interministériel élaboré conjointement par les ministères de la Justice, de l'Intérieur et de l'Équipement, portant création d'un traitement expérimental, dénommé « système de contrôle sanction automatique » et d'un projet d'arrêté modifiant l'arrêté du 29 juin 1992 portant création du système national des permis de conduire ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 2003-495 du 12 juin 2003 renforçant la lutte contre la violence routière ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu ensemble l'arrêté du 29 juin 1992 portant création du système national des permis de conduire et le projet d'arrêté modificatif de cet arrêté ;

Vu l'arrêté du 20 janvier 1994 portant création du fichier national des immatriculations ;

Vu l'arrêté du 18 juillet 1994 portant création du traitement automatisé de suivi du recouvrement des amendes et des condamnations pécuniaires ;

Vu le projet d'arrêté interministériel présenté par le ministre de l'Intérieur et le projet d'arrêté modificatif de l'arrêté du 29 juin 1992 ;

Après avoir entendu Monsieur Michel Gentot, président, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère de l'Intérieur a saisi la CNIL d'une demande d'avis accompagnée d'un projet d'arrêté interministériel portant création du « système de contrôle sanction automatique » et d'un projet d'arrêté modifiant l'arrêté du 29 juin 1992 portant création du système national des permis de conduire.

Ce dispositif expérimental, dont la mise en place est prévue pour une durée d'un an, permet l'automatisation de la constatation de certaines infractions routières, l'identification du titulaire du certificat d'immatriculation du véhicule concerné et l'envoi de l'avis de contravention correspondant.

Le fondement juridique de ce dispositif résulte de la combinaison des articles 529-11 du Code de procédure pénale, qui dispose notamment que *« l'avis de contravention prévu par les articles 529-1 et 529-8 peut être envoyé à la suite de la cons-*

tatation d'une contravention au Code de la route réalisée grâce à un appareil homologué de contrôle automatique », et L. 130-9 du Code de la route, qui pose le principe de la force probante des constatations automatisées ainsi effectuées et fixe la liste des infractions qui, à terme, seront concernées par ce dispositif.

Ne sont en effet concernées, dans le cadre de cette expérimentation, que les infractions aux limitations de vitesse, celles relatives au respect des signalisations imposant l'arrêt des véhicules à un ou deux carrefours toulousains et les infractions au respect des distances de sécurité dans les tunnels du Mont-Blanc, du Fréjus et du Somport.

Ce dispositif expérimental repose sur le déploiement, d'ici la fin de l'année 2003, de cent cinémomètres, fixes ou mobiles, couplés à des appareils photographiques numériques. Ces appareils devront être homologués conformément à la réglementation sur les poids et les mesures préalablement à leur mise en place.

Les informations collectées, sous la forme d'un cliché numérique, par ces appareils seront transmises à vingt centres de supervision répartis sur l'ensemble du territoire et situés dans les locaux des forces de l'ordre responsables des axes routiers surveillés, avant d'être acheminés vers un centre de traitement national.

Ce centre, où seront effectués l'ensemble des opérations nécessaires à l'identification des titulaires du certificat d'immatriculation du véhicule en infraction et l'envoi de l'avis de contravention, gère et exploite le système d'informations automatisé. Il est placé sous la supervision de six officiers de police judiciaire, chargés notamment de valider les constats d'infractions effectués par les dispositifs de contrôle automatisé.

Afin d'identifier le titulaire du certificat d'immatriculation du véhicule en infraction, redevable pécuniairement de certaines infractions commises avec son véhicule aux termes des articles L. 121-2 et L. 121-3 du Code de la route, le centre national de traitement procédera, par l'intermédiaire d'un logiciel de reconnaissance de caractères, à la reconnaissance automatique des numéros d'immatriculation à partir des prises de vue d'infractions transmises par les équipements de terrain et ensuite interrogera automatiquement le fichier des véhicules loués puis le fichier national des immatriculations.

Sur la consultation du fichier des véhicules loués

Le fichier des véhicules loués, créé par le centre national de traitement, recensera uniquement la raison sociale et l'adresse d'une vingtaine de sociétés de location, ainsi que les numéros de plaques minéralogiques des véhicules de leur parc, sans référence à l'identité des clients de ces sociétés.

Si le numéro de plaque minéralogique du véhicule concerné s'y trouve, une requête sera adressée de façon automatisée à la société ayant loué le véhicule afin d'obtenir les nom, prénom, date de naissance, adresse et numéro de permis de conduire du locataire du véhicule en infraction, conformément aux dispositions de l'article L. 121-3 du Code de la route.

Ce fichier ne concerne que des personnes morales et le ministère de l'Intérieur a prévu, avant tout échange de données, de faire signer une convention entre le centre national de traitement et chaque société de location de véhicules souhaitant mettre en place cet échange.

La Commission prend acte de ce que cette convention impose notamment aux sociétés de location que leur fichier de gestion des contrats de location soit tenu conformément aux dispositions de la loi du 6 janvier 1978, qu'elles procèdent à une

déclaration modificative de ce fichier prenant en compte les échanges nouveaux d'informations avec le centre national de traitement et qu'elles ne gardent pas trace des requêtes effectuées par le centre national de traitement. Cette convention leur impose en outre la mise en place de contraintes techniques d'échange informatique ainsi que des mesures destinées à assurer la sécurité des systèmes d'information des données et des mécanismes d'échange.

Sur la consultation du fichier national des immatriculations

Le fondement juridique de cette interrogation résulte de la combinaison des articles L. 330-1 et L. 330-2 du Code de la route qui prévoient que toutes les informations concernant les pièces administratives exigées pour la circulation des véhicules ou affectant la disponibilité de ceux-ci et faisant l'objet de traitements automatisés dans les services de l'État et sous l'autorité et le contrôle du ministre de l'Intérieur sont communiquées, sur leur demande, notamment, aux autorités judiciaires, aux officiers ou agents de police judiciaire, dans l'exercice des missions définies à l'article 14 du Code de procédure pénale, aux militaires de la gendarmerie ou aux fonctionnaires de la police nationale habilités à effectuer des contrôles routiers en application des dispositions du Code de la route, ainsi qu'aux fonctionnaires habilités à constater des infractions au Code de la route, aux seules fins d'identifier les auteurs de ces infractions.

S'agissant des conditions de mise en place de cette interconnexion, le ministère de l'Intérieur considère que l'arrêté du 20 janvier 1994 portant création du fichier national des immatriculations n'a pas à faire l'objet d'une modification sur ce point puisqu'il précise que *« le présent fichier ne peut faire l'objet d'aucune interconnexion avec un autre fichier en dehors de celles prévues par le traitement objet du présent arrêté »*, à savoir la communication d'informations aux destinataires énumérés à son article 5 parmi lesquels figurent déjà les fonctionnaires habilités à constater des infractions au Code de la route.

La Commission estime toutefois nécessaire que l'interconnexion créée entre les deux fichiers apparaisse explicitement dans cet arrêté dans la mesure où la mention, au titre des destinataires, des fonctionnaires habilités à constater des infractions au Code de la route aux seules fins d'identifier les auteurs de ces infractions ne fait pas apparaître explicitement la possibilité pour ceux-ci d'interroger automatiquement le fichier national des immatriculations et de recevoir ses réponses en retour.

Sur la consultation du fichier des changements d'adresse de La Poste

Avant d'adresser au titulaire du certificat d'immatriculation du véhicule en infraction l'avis de contravention correspondant, le centre de traitement national souhaite procéder, dans le cadre de cette expérimentation, à l'interrogation du fichier des changements d'adresse de La Poste afin de s'assurer que l'adresse actuelle du titulaire de la carte grise est la même que celle figurant dans le fichier national des immatriculations.

La Commission prend acte du fait que cette consultation se fera sur une base contractuelle avec La Poste et uniquement pour les personnes qui ne seraient pas opposées à la communication de leur nouvelle adresse, conformément à ses délibérations du 15 octobre 2002 et du 11 mars 2003 relatives à la commercialisation des changements d'adresse par La Poste.

Elle observe cependant que le bien-fondé de cette vérification limitée à ces personnes n'est pas clairement établi. Elle estime donc que les avantages et les inconvénients de cette procédure supplémentaire de vérification doivent être soigneusement évalués au stade de l'expérimentation avant d'envisager d'y recourir de façon définitive.

Sur les échanges d'informations avec le Trésor public

Après avoir adressé l'avis de contravention, le centre de traitement doit, pour assurer le suivi de la procédure, obtenir des services du Trésor public les informations nécessaires quant à l'effectivité du paiement des amendes et des consignations par les débiteurs.

La gestion et le suivi du paiement des avis de contravention adressés par le centre de traitement national peuvent être gérés par le centre d'encaissement des amendes de Rennes s'agissant des amendes forfaitaires, par les directions informatiques du Trésor, s'agissant des amendes forfaitaires majorées et des opérations de recouvrement, ou par l'intermédiaire d'un dispositif de paiement à distance par internet ou par serveur vocal. Ce système de télépaiement fera l'objet d'une demande d'avis spécifique.

La Commission constate que le fondement juridique de la transmission d'informations entre le centre de traitement national et le centre de Rennes et, le cas échéant, les directions informatiques du Trésor résulte de la combinaison des articles 4 et 6 de l'arrêté du 18 juillet 1994 portant création du traitement automatisé de suivi du recouvrement des amendes et des condamnations pécuniaires.

Sur l'alimentation du système national du permis à points

À l'issue de la procédure, soit que le contrevenant ait acquitté l'amende forfaitaire, reconnaissant ainsi les faits reprochés, soit qu'il l'ait contestée et qu'il ait fait l'objet d'une décision judiciaire le condamnant, le centre de traitement national transmettra au système national du permis de conduire le nombre de points retirés.

Le fondement juridique de cet envoi résulte de l'article L. 225-1 du Code de la route.

Le ministère de l'Intérieur précise qu'il s'agit d'un envoi d'informations, du centre de traitement national vers le système national du permis de conduire et que ce dernier n'alimente pas en retour le traitement du centre de traitement national.

La Commission estime, dans la mesure où cet envoi d'informations ne constitue pas une interconnexion, qu'il convient de modifier la formule employée à l'article 1er du projet d'arrêté modificatif de l'arrêté du 29 juin 1992 portant création du système national des permis de conduire.

Sur les informations nominatives collectées et traitées

Les données collectées, énumérées à l'article 3 du projet d'arrêté portant création du traitement projeté, sont relatives à l'infraction constatée (clichés du véhicule et de ses occupants pris par les appareils de contrôle automatisé, numéro unique d'identification de l'infraction, nature, lieu et date, moyens de constatation), à l'identification du véhicule (numéro d'immatriculation) et du titulaire de son certificat d'immatriculation (nom, nom d'usage, prénoms, date et lieu de naissance, nationalité, adresse, numéro du permis de conduire), au montant de l'amende et à sa nature, au

paiement de l'amende et des consignations par les contrevenants et au retrait de points au permis de conduire.

Ces informations apparaissent pertinentes au regard de la finalité du traitement expérimental.

La Commission estime que l'article 3 du projet d'arrêté doit être complété de façon à préciser que les clichés concernent le véhicule et ses passagers.

Sur la durée de conservation des informations

En application de l'article L. 130-9 du Code de la route, la durée maximale de conservation des informations collectées est de dix ans, eu égard aux dispositions régissant le fonctionnement du permis à points, et notamment l'article L. 225-2 IV du Code de la route.

Cette même disposition prévoit également que le contrevenant peut demander au procureur de la République compétent d'ordonner l'effacement des informations le concernant lorsqu'il a récupéré le nombre de points ayant été retiré de son permis de conduire ou lorsque la procédure le concernant a donné lieu à une décision définitive de relaxe.

La Commission estime que le ministère de l'Intérieur devrait mettre à profit la phase d'expérimentation du dispositif pour évaluer la pertinence d'une durée de conservation uniforme des informations pendant dix ans.

Sur l'information des intéressés

L'information des intéressés est effectuée par l'intermédiaire d'une mention figurant sur l'avis de contravention et précisant que *« le véhicule dont le certificat d'immatriculation est établi à votre nom a fait l'objet d'un contrôle automatisé établissant la commission de l'infraction figurant ci-dessous »*.

La Commission estime que ces mesures sont satisfaisantes mais que la mention doit être modifiée de façon à préciser que le contrôle automatisé « a permis » d'établir la commission de l'infraction.

Sur le droit d'accès et de rectification

La loi du 6 janvier 1978 ne faisant aucune distinction, dans le cadre de l'exercice du droit d'accès et de rectification, selon la nature des informations concernant le titulaire de ce droit, il appartient à la Commission de prendre en compte la présence d'un cliché numérique parmi les informations collectées et traitées, l'intéressé pouvant exercer normalement son droit d'accès et de rectification aux informations d'autre nature le concernant dans les conditions prévues par les articles 34 et suivants de la loi du 6 janvier.

La Commission reconnaît que ce cliché, s'il constitue une donnée nominative au sens de la loi du 6 janvier 1978, est une donnée relative à l'infraction pénale commise dont le Code de procédure pénale ne prévoit l'accès, au titre du respect du contradictoire, qu'au cours de la phase judiciaire de contestation de l'amende selon les formes et modalités prévues par ce Code.

La Commission souligne cependant que les règles ainsi applicables ne permettent pas une contestation efficace de la sanction encourue automatiquement dès lors que le titulaire du certificat d'immatriculation n'a pas la possibilité d'accéder, dès réception de l'avis de contravention, à l'ensemble des informations le concer-

nant, y compris à la partie du cliché représentant le conducteur de son véhicule, à l'exception toutefois de la partie du cliché représentant le ou les éventuels passagers. En conséquence elle recommande que soit étudiée une modification des règles de la procédure pénale applicables à ce traitement automatisé.

En l'état du droit et dès lors que la constatation et le traitement de l'infraction relèvent de la procédure pénale, la Commission considère que le projet d'arrêté portant création du traitement expérimental envisagé doit indiquer de façon explicite que le centre de traitement national est placé sous la responsabilité du procureur de la République dont dépendent les officiers de police judiciaire en charge de la supervision du centre.

Sur les mesures de sécurité

Le dispositif envisagé relève, s'agissant de ces mesures de sécurité, du contrôle de la DCSSI et de la validation par les hauts fonctionnaires de défense des ministères.

Des mesures de sécurité physique des données sur les appareils de contrôle ont été prévues et les informations collectées par les équipements de terrain transiteront par les réseaux sécurisés soit du ministère de l'Intérieur, soit de celui de la Défense. Les mesures de sécurité logique prévues par le cahier des charges prévoient un accès authentifié à la base de certificats numériques sur la base d'une infrastructure de gestion de clés.

De même, les mesures générales décrites ou imposées au titulaire du marché, s'agissant des traitements informatiques externes à l'application mise en œuvre par le centre de traitement national et de l'externalisation potentielle de certains traitements de données, apparaissent satisfaisantes au regard de l'état de l'art en la matière ou des mesures entourant d'autres transferts de données opérés sur ces réseaux.

Sur le fonctionnement du logiciel de lecture et reconnaissance automatisée des plaques minéralogiques des véhicules en infraction

La Commission prend acte que dans les cas où les clichés représentent un véhicule dont la plaque n'aura pu être reconnue par ce logiciel, ils feront l'objet d'un traitement manuel par un officier de police judiciaire.

Il serait utile que le ministère de l'Intérieur fournisse à l'issue de cette expérimentation des statistiques détaillées sur les taux d'échec et d'erreur constatés.

Émet un avis favorable au projet d'arrêté interministériel élaboré conjointement par les ministères de la Justice, de l'Intérieur et de l'Équipement, portant création d'un traitement expérimental, dénommé « système de contrôle sanction automatique ».

Demande que :
– l'article 5 de l'arrêté du 20 janvier 1994 soit modifié afin que l'interconnexion mise en place dans le cadre de ce dispositif apparaisse clairement ;
– le ministère de l'Intérieur évalue, au cours de cette expérimentation, les avantages et les inconvénients de la procédure supplémentaire de vérification de l'adresse du contrevenant auprès du fichier des changements d'adresse de La Poste et informe la Commission des résultats de cette évaluation ;

– l'article 3 du projet d'arrêté portant création du traitement expérimental soit complété de façon à préciser que les clichés concernent le véhicule et ses passagers ;
– la mention figurant sur l'avis de contravention soit ainsi rédigée : *« Le véhicule dont le certificat d'immatriculation est établi à votre nom a fait l'objet d'un contrôle automatisé ayant permis d'établir la commission de l'infraction figurant ci-dessous »* ;
– le projet d'arrêté portant création du traitement expérimental indique explicitement que le centre de traitement national est placé sous la responsabilité du procureur de la République dont dépendent les officiers de police judiciaire en charge de la supervision du centre ;
– le ministère de l'Intérieur adresse à la Commission un bilan de cette expérimentation précisant notamment les taux d'échec et d'erreur du logiciel de reconnaissance automatisée des plaques minéralogiques.

Émet un avis favorable au projet d'arrêté modifiant l'arrêté du 29 juin 1992 portant création du système national des permis de conduire sous réserve que la rédaction prévue pour l'article 8 de l'arrêté du 29 juin 1992 par l'article 1er de ce projet de texte soit modifiée de la façon suivante : *« Le présent fichier peut être alimenté, dans les conditions prévues par l'article L. 225-1 du Code de la route, par le traitement d'informations nominatives dénommé »système contrôle sanction automatisé« ».*

Recommande que :
– soit étudiée une modification des règles de la procédure pénale applicables à ce traitement automatisé tendant à prévoir la possibilité pour le titulaire du certificat d'immatriculation du véhicule en infraction d'avoir accès, dès réception de l'avis de contravention, à l'ensemble des informations le concernant, y compris à la partie du cliché représentant le conducteur de son véhicule à l'exception toutefois de la partie du cliché représentant le ou les éventuels passagers ;
– le ministère de l'Intérieur mette à profit la phase d'expérimentation du dispositif pour évaluer la pertinence d'une durée de conservation uniforme des informations pendant dix ans.

Poste et télécommunications

Délibération n° 03-011 du 11 mars 2003 portant avis favorable sur le traitement automatisé d'informations nominatives mis en œuvre par La Poste relatif au fichier des nouveaux voisins

La Commission nationale de l'informatique et des libertés, saisie pour avis par La Poste, service national de l'adresse (SNA), d'un projet de décision du directeur général de La Poste portant création d'un traitement dénommé « fichier des nouveaux voisins ».

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu la délibération de la CNIL nº 02-071 du 15 octobre 2002 portant avis favorable sur le traitement mis en œuvre par La Poste relatif au fichier des nouveaux voisins ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Poste (service national de l'adresse), a déposé une demande d'avis relative au « fichier des nouveaux voisins » dont la finalité principale est de permettre, d'une part, la collecte des changements d'adresse des particuliers ayant souscrit auprès de La Poste un contrat de réexpédition définitive, d'autre part, la commercialisation des changements d'adresse des personnes qui ne se sont pas opposées à une telle commercialisation aux sociétés liées contractuellement avec La Poste.

Les informations enregistrées dans le traitement sont relatives à l'identité du souscripteur du contrat (nom, prénom et sexe), l'identité des personnes membres du foyer du souscripteur (nom, prénom et sexe), l'ancienne adresse, la nouvelle adresse, l'ancien numéro de téléphone (facultatif), le nouveau numéro de téléphone (facultatif), la date de souscription du contrat de réexpédition définitif, la date de fin de validité du contrat de réexpédition définitif, l'accord de la personne pour la commercialisation de la nouvelle adresse.

Ces données sont recueillies directement auprès des personnes s'étant adressées à La Poste pour souscrire un contrat de réexpédition définitive du courrier, service proposé aux particuliers pour permettre le ré-acheminement de leur courrier pendant une durée d'une année après leur déménagement.

Les destinataires de ces informations sont les services de La Poste, les services des contributions directes ainsi que le régisseur du service de la redevance de l'audiovisuel en vertu de l'article L. 5 du Code des postes et des télécommunications s'agissant des seules informations les concernant, c'est-à-dire l'identité et la nouvelle adresse ; enfin, et dans la mesure où l'intéressé ne s'y est pas opposé, les organismes

(banques, entreprises, commerces, associations, etc.) liés contractuellement à La Poste et qui ne détiennent pas obligatoirement l'ancienne adresse peuvent être destinataires de tout ou partie des données.

Les souscripteurs du contrat de réexpédition sont informés, sur le formulaire même de collecte des données, de la possibilité pour La Poste de communiquer les données ainsi recueillies, non seulement, conformément aux obligations légales, au service des contributions directes et de la redevance de l'audiovisuel pour les seules coordonnées, mais aussi aux organismes (banques, entreprises, commerces, associations, etc.) liés contractuellement à La Poste, quels qu'ils soient.

Les intéressés sont mis en mesure de s'opposer à la communication aux organismes liés contractuellement à La Poste, au moyen d'une case à cocher, sur le formulaire de collecte des données, étant précisé que *« quelle que soit votre réponse, votre changement d'adresse sera traité dans les conditions habituelles. »*

Par ailleurs, il a été constaté que La Poste, sans attendre l'avis de la CNIL, procédait à une présentation, au demeurant, inappropriée, de ce service tant dans une brochure publicitaire que sur le site internet du service national de l'adresse.

Prend acte que :

– La Poste s'est engagée :

– à modifier le site internet du Service national de l'adresse et à procéder à l'impression de nouvelles plaquettes publicitaires ;

– à ne procéder à aucun « rapprochement » des fichiers de La Poste avec des fichiers appartenant à des sociétés tierces ;

– à apposer une nouvelle mention d'information sur les contrats de souscription plus explicite s'agissant de la finalité de la cession puisqu'il sera précisé qu'il s'agira de commercialiser les données et plus simple d'utilisation pour les intéressés avec une seule case à cocher. Cette mention sera rédigée de la manière suivante : *« La Poste souhaite commercialiser tout ou partie des informations collectées sur le formulaire, aux organismes qui en feraient la demande et qui ne détiennent pas tous votre ancienne adresse (banques, entreprises, commerces, associations, etc.).*

En cas de désaccord, veuillez cocher la case ci-contre ❑

Quelle que soit votre réponse, votre changement d'adresse sera traité dans les conditions habituelles.

Les indications recueillies ci-dessus donnent lieu à l'exercice d'un droit de rectification auprès du bureau de poste de votre choix ou auprès de votre centre opérationnel de l'adresse conformément aux dispositions de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Dans tous les cas, La Poste est tenue de notifier les changements de domicile au service des contributions directes et au service de la redevance de l'audiovisuel conformément aux dispositions de l'article 92 de la loi nº 85-1407 du 30 décembre 1985 « ;

– les visas du nouveau projet de décision soumis par La Poste font désormais référence aux différentes décisions prises précédemment par La Poste dans le cadre de la gestion des contrats de réexpédition du courrier ;

– les articles 1 et 3 de la décision sont désormais rédigés conformément à la délibération nº 02-071 du 15 octobre 2002.

La délibération susvisée de la CNIL est modifiée en ce qui concerne la seule rédaction de la mention d'informations sur les contrats de souscription.

Émet un avis favorable au projet de décision présenté par le directeur général de La Poste.

Délibération n° 03-017 du 24 avril 2003 portant avis sur le projet de loi relatif aux communications électroniques

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministre délégué à l'Industrie, le 31 mars 2003, du projet de loi relatif aux communications électroniques ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret d'application du 17 juillet 1978 ;

Après avoir entendu Monsieur Marcel Pinet, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Émet l'avis suivant :

Le projet de loi relatif aux communications électroniques transpose certaines des dispositions de la directive 2002/58 relative à la protection des données à caractère personnel dans le secteur des télécommunications. L'introduction de nouvelles dispositions législatives s'accompagne d'une réorganisation du livre II, titre Ier, chapitre II du Code des postes et télécommunications. Deux sections intéressant directement la protection des données personnelles sont ainsi créées, la première relative aux « Annuaires et services de renseignements », la seconde relative à la « Protection de la vie privée des utilisateurs de réseaux et services de télécommunications », qui appellent certaines observations.

Sur les articles 3 et 93 du projet de loi

La Commission relève que certains articles du projet de loi dont elle est saisie pour avis, bien qu'ils ne concernent pas directement ou exclusivement la protection des données personnelles, mériteraient néanmoins d'être complétés.

En premier lieu, l'article 3 du projet de loi qui modifie l'article L. 32-1 du Code des postes et télécommunications énonce les objectifs devant être atteints dans le cadre général de la fourniture de services de communications électroniques. Parmi ceux-ci est dorénavant incluse l'exigence d'*« un niveau élevé de protection des données à caractère personnel »* (6°). Dès lors, il conviendrait que le premier alinéa du II de l'article L. 32-1 modifié cite la Commission nationale de l'informatique et des libertés parmi les autorités chargées de prendre, dans le cadre de leurs attributions respectives, toutes mesures visant à assurer le respect de ces principes.

En second lieu, l'article 93 du projet de loi insère un article L. 121-90 dans le Code de la consommation qui précise les informations que doit comporter tout contrat souscrit par un consommateur avec un fournisseur de services de communications électroniques. La Commission rappelle les exigences issues des articles 10 de la

directive du 24 octobre 1995 et 27 de la loi du 6 janvier 1978 en matière d'information des personnes lors de la collecte de données à caractère personnel les concernant. De plus, compte tenu de la spécificité, en termes de vie privée, des données nécessaires aux services de communications fournies par voie électronique – numéro de téléphone, adresse électronique, etc. –, la Commission recommande que soient clairement indiquées, lors de la souscription d'un contrat, les conditions d'exercice des différents droits d'opposition qui sont reconnus à l'abonné, particulièrement dans la perspective de la création d'un annuaire universel. Cette information préalable est d'ailleurs prévue à l'article 12 de la directive du 12 juillet 2002. En conséquence, la rédaction de l'article L. 121-90 du Code de la consommation devrait être modifiée afin, d'une part, d'y inclure un nouvel alinéa reprenant cette obligation et, d'autre part, de prévoir l'avis de la Commission nationale de l'informatique et des libertés concernant l'arrêté prévu au dernier alinéa de cet article.

Sur les articles 7 et 10 relatifs aux « Annuaires et services de renseignements »

L'article 7 du projet de loi crée une section relative aux « Annuaires et services de renseignements » [1]. La création d'un service de renseignements et d'annuaire d'abonnés à des services de communications électroniques est une des composantes du service universel des communications électroniques (article 17 du projet de loi).

Cette section comprend un article unique, l'article L. 34, dont la rédaction est sensiblement modifiée par l'article 10 du projet de loi. La nouvelle rédaction de cet article permet la transposition de l'article 12 de la directive du 12 juillet 2002 relatif aux annuaires d'abonnés.

Le projet de loi reconnaît le droit pour toute personne d'être mentionnée sur les listes d'abonnés publiées ou consultables ou de ne pas l'être. De manière constante, la Commission recommande que l'exercice du droit d'opposition en matière de publication ou de communication de listes d'abonnés à des services de télécommunications – devenu aujourd'hui, « services de communications électroniques » – puisse s'exercer à titre gratuit. Elle recommande ainsi que le deuxième alinéa de cet article prévoit que les droits énoncés sont *« garantis et gratuits »*.

Par ailleurs, le projet de loi prévoit que les abonnés doivent être préalablement informés des fins auxquelles sont établis les annuaires ainsi que de toute autre possibilité d'utilisation reposant sur des fonctions de recherche intégrées dans les versions électroniques. Sont clairement visées ici les fonctions de recherche inversée qui permettent, à partir du numéro de téléphone de l'abonné, de trouver son nom et son adresse. Si l'information des personnes sur ces fonctions de recherche est indispensable, il n'en demeure pas moins que de tels outils présentent des risques particuliers puisqu'ils permettent la collecte d'informations qu'une personne n'ayant laissé que son numéro de téléphone n'a pas entendu divulguer. En conséquence, il conviendrait qu'un droit d'opposition spécifique soit reconnu face à l'utilisation de tels annuaires.

En tout état de cause, la Commission relève que les modalités pratiques des droits reconnus aux abonnés dépendront, dans une large mesure, du décret d'application visé au dernier alinéa de l'article L. 34 nouveau du Code des postes et télécommunications. La Commission rappelle donc les termes de sa délibération du

1 Section 2, chapitre 2 du titre 1er du livre II du Code des postes et télécommunications.

14 mars 2002 [1] et estime qu'elle devra, le cas échéant, être saisie pour avis de tout nouveau projet de décret d'application de cet article. L'article L. 34 devrait consacrer cette saisine.

Sur les articles 8 et 11 relatifs à la « Protection de la vie privée des utilisateurs de réseaux et services de télécommunications »

L'article 8 du projet de loi crée une section relative à la « Protection de la vie privée des utilisateurs et services de télécommunications » [2]. Cette section comprend, d'une part, les dispositions relatives aux catégories des données traitées par les opérateurs de communications électroniques et à leur durée de conservation et, d'autre part, les dispositions relatives au principe du consentement préalable en matière d'opérations de prospection directe effectuées au moyen d'automates d'appel et de télécopieurs dont le champ d'application est étendu aux courriers électroniques par le projet de loi relatif à la confiance dans l'économie numérique sur lequel la Commission s'est déjà prononcée par une délibération n° 02-093 du 28 novembre 2002.

L'article L. 34-1 nouveau du Code des postes et télécommunications relatif à la conservation des données dites « de connexion » est modifié par l'article 11 du projet de loi qui introduit deux dispositions nouvelles relatives aux données de géolocalisation.

En premier lieu, cet article ajoute un paragraphe qui transpose, notamment, l'article 9 de la directive du 12 juillet 2002 relatif aux données de localisation autres que les données relatives au trafic. Le principe du consentement préalable de l'abonné en matière de traitement et de conservation de la donnée de localisation en vue de la fourniture d'un service à valeur ajoutée est posé. Il peut retirer ou suspendre à tout moment, et gratuitement, ce consentement. Ce dispositif est de nature à permettre le développement des services utilisant la donnée de localisation d'un abonné ou d'un utilisateur de service de communications électroniques. La Commission regrette cependant que la notion de proportionnalité en matière de traitement de cette donnée présente dans la directive [3] ne soit pas reprise par le projet de loi. Cette notion, centrale en matière de protection des données personnelles, devrait être réaffirmée dans le cadre de ce texte.

Ce même paragraphe prévoit une exception au principe du consentement préalable en matière de traitement de la donnée de localisation à d'autres fins que l'acheminement de l'appel. En effet, conformément à la directive du 12 juillet 2002 (article 10. b), la donnée de localisation d'un appel pourra être communiquée aux services d'urgence jusqu'à l'aboutissement de l'opération de secours et aux fins exclusives de celle-ci. La Commission, prenant en compte l'objectif de sauvegarde de la personne humaine et des biens, a déjà autorisé la présentation systématique du nom et de l'adresse à ces mêmes services d'urgence. Si la Commission ne peut être que favorable à ce que les services d'urgence, dans le cadre de leurs activités, aient accès à la donnée de localisation d'un appel, elle veillera, dans son avis sur le décret

1 Délibération n° 02-014 du 14 mars 2002 portant avis sur un projet de décret relatif à l'annuaire universel et modifiant le Code des postes et télécommunications.

2 Section 3, chapitre 2 du titre 1er du livre II du Code des postes et télécommunications.

3 Article 9 de la directive du 12 juillet 2002 : « [les données de localisation peuvent être traitées moyennant le consentement des utilisateurs ou des abonnés], *dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée* ».

relatif à l'application de cette disposition, à ce que ses modalités d'application soient très précisément encadrées.

En deuxième lieu, l'article 11 du projet de loi modifie l'article L. 34-1 nouveau en précisant que les opérateurs de communications électroniques ne peuvent conserver et traiter que les données relatives à l'identification des personnes utilisatrices de leurs services, aux caractéristiques techniques des communications assurées et à *« la localisation des équipements terminaux »*. La Commission constate que cet ajout ne fait qu'entériner une situation de fait, les opérateurs disposant déjà de cette donnée au titre des données techniques indispensables à l'acheminement d'un appel. En revanche, le projet de loi ne tranche pas la question des conditions de conservation de cette donnée, ces conditions devant être précisées par décrets en Conseil d'État pris après avis de la CNIL. En conséquence, la Commission réserve ses appréciations sur cet important point lorsqu'elle sera saisie des décrets précités.

Délibération n° 03-056 du 9 décembre 2003 portant avis sur le projet de décret relatif à la conservation des données relatives à une communication par les opérateurs de télécommunications et portant modification du Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de la Justice, le 21 octobre 2003, du projet de décret relatif à la conservation des données relatives à une communication par les opérateurs de télécommunications et portant modification du Code des postes et télécommunications ;

Vu la convention nº 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret d'application du 17 juillet 1978 ;

Vu la loi nº 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne modifiée, et notamment son article 29 ;

Vu la loi nº 2003-2390 du 18 mars 2003 pour la sécurité intérieure, et notamment ses articles 18 et 20 ;

Après avoir entendu Monsieur Marcel Pinet, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Émet l'avis suivant :

Le décret relatif à la conservation des données relatives à une communication par les opérateurs de télécommunications et portant modification du Code des postes et télécommunications doit préciser la portée et les modalités de mise en œuvre de l'article 29 de la loi nº 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (LSQ). Cet article a introduit, notamment, un article L. 32-3-1 dans le Code des postes et télécommunications qui traite de la conservation par les opérateurs de télécommunications des données de connexion, c'est-à-dire les informations qui sont produites ou nécessitées par l'utilisation de réseaux de télécommunication, qu'il s'agisse des communications téléphoniques ou des connexions au réseau internet.

L'article L. 32-3-1 du Code des postes et télécommunications pose le principe général d'un effacement ou d'une anonymisation de *« toute donnée relative à une communication dès que celle-ci est achevée »*. Trois exceptions sont prévues, d'une part, pour permettre aux opérateurs de conserver jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée (à savoir, un an [1]) certaines données nécessaires à la facturation ou au paiement des prestations fournies, d'autre part, pour leur permettre de conserver certaines données en vue d'assurer la

1 Article L. 32-3-2 du Code des postes et télécommunications.

sécurité de leurs réseaux [1] et, surtout, pour leur faire obligation de conserver pour une durée maximale d'un an certaines données *« pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations »*.

Le fait pour un opérateur de télécommunications ou ses agents de ne pas procéder aux opérations tendant à effacer ou rendre anonymes les données relatives aux communications ou de ne pas procéder à la conservation de ces données dans les cas où ces opérations sont prescrites par la loi est sanctionné dans les conditions prévues par l'article L. 39-3 du Code des postes et télécommunications.

Ce dispositif était prévu en 2001 par le projet de loi sur la société de l'information qui n'a jamais été examiné par le Parlement mais sur lequel la Commission avait été consultée et sur lequel elle avait rendu un avis [2]. Cet avis avait été l'occasion pour la CNIL de poser les termes d'un débat qui dépasse largement les spécificités de la technologie et met en cause les principes essentiels de la protection des données à caractère personnel.

Observations préliminaires :

Le dispositif prévu par l'article L. 32-3-1 du Code des postes et télécommunications a introduit une obligation nouvelle pour les opérateurs de télécommunications dont le caractère dérogatoire doit être relevé.

D'une manière générale, le traitement des données à caractère personnel est soumis au principe de finalité qui oblige à ce que les catégories de données collectées et traitées et leur durée de conservation soient déterminées par la finalité du traitement. En d'autres termes, le traitement et la conservation d'une donnée ne peuvent se justifier qu'au regard de la finalité qui préside à sa collecte. Afin de permettre le travail des autorités judiciaires, les législations de protection des données à caractère personnel leur ont reconnu, dans le strict cadre défini par la procédure pénale, la possibilité d'accéder à ces informations tant que celles-ci sont conservées dans un fichier ou un traitement.

Ce schéma a été modifié en matière de traitement des données dites « de connexion » par l'article 29 de la loi du 15 novembre 2001 dans un sens qui a conduit la Commission à souligner *« le caractère inédit du dispositif retenu »* [3]. En effet, en dérogation au principe d'effacement ou d'anonymisation posé par la loi et à côté des exceptions légitimes au regard de leurs activités [4], l'article L. 32-3-1 du Code des postes et télécommunications impose aux opérateurs une obligation de conserver certaines données aux fins exclusives de faciliter l'activité des autorités judiciaires.

On doit relever que cette obligation ne répond pas à des besoins spécifiques ou ponctuels qui seraient la nécessité d'identifier les auteurs de contenus illégaux ou attentatoires aux droits des tiers, l'interception de messages utilisant les réseaux des opérateurs de télécommunications ou la préservation du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs. Ces

1 Cette possibilité a été introduite par l'article 20 de la loi n° 2003-2390 du 18 mars 2003 pour la sécurité intérieure.

2 Délibération n° 01-018 du 3 mai 2001 portant avis sur le projet de loi sur la société de l'information.

3 *Cf.* avis de la CNIL sur le projet de loi sur la société de l'information précité.

4 À savoir, dans un premier temps, la conservation des données nécessaires en cas de contestation de la facturation ou du paiement des prestations fournies puis, dans un second temps, celles nécessaires pour assurer la sécurité de leurs réseaux.

possibilités sont, en effet, prévues respectivement par les lois du 1er août 2000 [1], du 10 juillet 1991 [2] et du 18 mars 2003.

L'obligation générale de conserver des catégories de données qui se rapportent à l'ensemble des personnes utilisant les services des opérateurs de télécommunications et dont la conservation ne présente aucune utilité pour les opérateurs est, en ce sens, dérogatoire aux principes généraux de la protection des données à caractère personnel.

Il doit être précisé que la directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit ce type de disposition. En effet, l'article 13 de cette directive prévoit explicitement que les États membres peuvent déroger au principe d'une durée de conservation limitée à la durée nécessaire à la réalisation des finalités pour lesquelles des données à caractère personnel sont collectées ou pour lesquelles elles sont traitées ultérieurement, lorsqu'une telle dérogation est prévue par la loi et constitue une mesure nécessaire, notamment, à la sûreté de l'État, la défense, la sécurité publique ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Cette disposition est également prévue par la directive 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques dont l'article 15 prévoit explicitement que les États membres peuvent adopter des mesures législatives prévoyant la conservation des données de connexion pendant une durée limitée lorsque cela constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique pour sauvegarder notamment la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques.

L'article L. 32-3-1 du Code des postes et télécommunications précise en outre que les données visées *« ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications »*.

Le Conseil constitutionnel a ainsi considéré à propos de l'article 29 de la loi du 15 novembre 2001 que le législateur avait mis en œuvre, en les conciliant, l'ensemble des exigences constitutionnelles [3].

Cependant, il doit être souligné, comme l'a indiqué la Commission lors de la présentation du dispositif législatif [4], que cette obligation *« déroge aux principes fondamentaux de protection des libertés individuelles »* et nécessite donc une mise en œuvre stricte et précise qui est l'objet du projet de décret.

Observations générales :

Sur le champ d'application du décret

Les opérateurs disposent de deux catégories de données se rapportant aux utilisateurs de leurs réseaux : celles, administratives, relatives à leurs clients qu'ils

1 Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

2 Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications.

3 Décision n° 2001-457 DC du 27 décembre 2001.

4 *Cf.* avis précité.

traitent dans le cadre général de leur relation commerciale (les nom, prénom, adresse, mode de paiement de l'abonnement, etc.) et celles, techniques, relatives aux communications émises par leurs clients qu'ils transmettent par leurs réseaux (numéros de téléphone appelant et appelé, date et durée de l'appel ou de la connexion, identifiant de l'appareil utilisé par leurs clients, etc.).

L'article 29 de la loi relative à la sécurité quotidienne pose le principe d'un effacement ou d'une anonymisation de *« toute donnée relative à une communication »*, c'est-à-dire la deuxième catégorie de données visée ci-dessus à savoir, toute donnée technique issue de l'utilisation de leurs réseaux qui est automatiquement générée et collectée par l'opérateur à l'occasion d'une communication.

En même temps qu'est posé ce principe, la loi fait obligation aux opérateurs de conserver certaines catégories de ces données techniques et de pouvoir les rattacher à la personne à l'origine de la communication qui a donné lieu à la création de ces données.

Le projet de décret dont la Commission est saisie tend à déterminer le cadre dans lequel doit s'opérer la conservation de *« toute information disponible au regard des procédés de télécommunications* [...] *susceptible d'être enregistrée par l'opérateur à l'occasion des communications dont il assure la transmission et pertinente au sens de* [...] *l'article L. 32-3-1 du Code des postes et télécommunications »* (article R. 9-1 du Code des postes et télécommunications introduit par l'article 2 du décret).

La loi et le décret ne visent donc pas à déterminer le cadre dans lequel doivent être conservées les données issues de la relation commerciale de la prestation de service assurée par l'opérateur. Le projet de décret prévoit ainsi explicitement que sont exclues de son champ d'application les données relatives à l'abonné ou à l'utilisateur détenues par l'opérateur dans le cadre de la relation contractuelle, *« indépendantes de toute communication »* (alinéa 2 de l'article R. 9-1 nouveau du Code des postes et télécommunications) et qui sont traitées selon le régime du droit commun, notamment en matière de protection des données à caractère personnel.

En effet, les données relatives au nom, prénom, adresse, mode de paiement ou toute autre information utile dans le cadre de la relation contractuelle ne sont pas *« enregistrées par l'opérateur à l'occasion d'une communication »* mais sont fournies par l'abonné au moment de la souscription du contrat qui le lie avec son opérateur. Si, par exemple, une communication téléphonique permet à l'opérateur téléphonique de collecter des données concernant la communication en elle-même (quel numéro de téléphone est à l'origine de l'appel ? Quel numéro de téléphone est appelé ? Pour combien de temps ? etc.), elle ne lui permet pas de collecter des données se rapportant à la personne qui a passé cette communication (son nom, son adresse, son âge, etc.).

L'article 29 de la loi relative à la sécurité quotidienne et son décret d'application se limitent à définir le régime dérogatoire dans lequel doit s'effectuer la conservation de *« toute donnée relative à une communication »*, dite donnée « de connexion ». Ainsi, les données ne se rapportant pas à l'établissement d'une communication ne sont pas concernées par ce dispositif.

En conséquence, la Commission estime que les données se rapportant à l'utilisateur (et non à ses communications) – à savoir les nom, prénom, adresse, mode de paiement, adresse IP de création et courrier électronique de confirmation, identifiant de session de connexion, mot de passe et informations associées, adresse du courrier électronique et les adresses associées – n'ont pas à figurer dans le projet de décret qui n'a vocation à traiter que de la conservation des données dites « de connexion ».

L'extension faite par le projet de décret du régime dérogatoire issu de l'article 29 de la loi relative à la sécurité quotidienne aux données relatives aux clients est de plus contraire aux directives communautaires du 24 octobre 1995 et du 12 juillet 2002 qui prévoient explicitement que seules des mesures législatives peuvent déroger aux principes généraux de la protection des données à caractère personnel.

Les données relatives à l'utilisateur en tant que client d'un opérateur sont traitées et conservées dans le cadre de la relation commerciale entre l'opérateur de télécommunications et l'utilisateur de ses services. Pour autant, les autorités judiciaires pourront avoir accès à ces données dont, cependant, la conservation devra s'effectuer selon le régime de droit commun de la protection des données à caractère personnel et non dans le cadre dérogatoire du décret pris en application de l'article 29 de la loi relative à la sécurité quotidienne.

Si la conservation de certaines de ces données peut être incontestablement utile dans le cadre de la facturation comme dans celui de la recherche, de la constatation et de la poursuite des infractions pénales, le régime applicable aux conditions dans lesquelles elles doivent être conservées ne relève manifestement pas de l'objet du présent décret.

Sur la détermination et la définition des catégories de données visées par le décret

Les catégories de données visées aux articles R. 9-1-1 et R. 9-1-2 nouveaux du Code des postes et télécommunications doivent être conservées en dérogation au principe général d'effacement ou d'anonymisation posé par l'article L. 32-3-1 du Code des postes et télécommunications. À ce titre, l'emploi du terme *« notamment »* par le projet de décret dans la définition de ces données introduit un élément d'incertitude qui peut conduire les opérateurs à ne pas mesurer précisément l'obligation qui leur est faite. En conséquence, il appartient au décret de fixer très précisément les catégories de données que les opérateurs doivent conserver en dérogation à ce principe d'effacement.

Les informations visées par le projet de décret sont susceptibles de concerner aussi bien une communication adressée à une personne physique, l'envoi d'un courrier électronique par exemple, que la connexion à un serveur distant (accès à un site web, par exemple). Pour autant, la loi a limité l'application du décret aux données portant exclusivement, d'une part, sur l'identification des personnes utilisatrices des services fournis par les opérateurs de télécommunications et, d'autre part, sur les caractéristiques techniques des communications assurées par ces derniers.

En conséquence, il convient de définir de manière restrictive certaines catégories de données visées par le projet de décret afin que le contenu de celles-ci se limite aux objectifs précis d'identification de la personne utilisatrice et d'apporter des éléments sur les caractéristiques techniques des communications passées. Ainsi faudrait-il que le décret définisse plus précisément les termes de *« services complémentaires demandés ou utilisés »* ou *« données relatives aux en-têtes de message de courrier électronique permettant d'identifier l'ensemble des destinataires »* afin que les données conservées à ces titres ne concernent que l'identification des personnes et les éléments sur les caractéristiques techniques des communications qu'elles auront passées.

Sur l'application de la loi « informatique et libertés » aux données visées par le décret

Le législateur n'a pas entendu instaurer un régime d'exception sur les conditions de traitement des données techniques relatives à une communication puisque l'article L. 32-3-1 du Code des postes et télécommunications prévoit que *« la conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés »*.

À ce titre, la Commission souligne deux conséquences qui s'attachent à l'application de la loi « informatique et libertés » au projet de décret qui lui est soumis.

En premier lieu, le principe de finalité interdit qu'une donnée conservée dans le cadre d'une finalité précise visée par le projet de décret ne soit utilisée dans le cadre d'une autre finalité. Ainsi, une donnée conservée au titre de la sécurité des réseaux des opérateurs de télécommunications ne pourra être utilisée pour justifier d'une facturation, alors même que l'opérateur dispose de cette donnée au titre de la première finalité.

En second lieu, il convient de rappeler que les autorités de police ne pourront avoir accès aux informations visées dans le projet de décret que si elles agissent en flagrant délit ou sur commission rogatoire d'un juge d'instruction. Dans ces deux cas, en effet, les prérogatives particulières qu'elles tiennent du Code de procédure pénale leur confèrent, ainsi que les administrations fiscales et douanières et les enquêteurs de l'autorité des marchés financiers pour l'exercice de leurs missions de contrôle, la qualité de « tiers autorisés » au regard de la loi « informatique et libertés ».

C'est donc à la lumière des principes généraux relatifs à la protection des données personnelles – notamment les principes relatifs à la finalité et à la proportionnalité des données – que la Commission doit examiner le projet de décret, quand bien même certaines d'entre elles (les données conservées aux fins exclusives de permettre la recherche, la constatation et la poursuite des infractions pénales) seraient conservées sur la base d'un régime dérogatoire à ces principes.

Sur les catégories de données conservées pour les besoins de la facturation et du paiement des prestations de télécommunications

En application du III. de l'article L. 32-3-1 du Code des postes et télécommunications, l'article 2 du projet de décret introduit un article R. 9-1-1 dans le Code des postes et télécommunications dont les 1°, 2° et 3° traitent des catégories de données techniques qui peuvent être conservées par les opérateurs de télécommunications pour les besoins de la facturation et du paiement des prestations de télécommunications.

1) Le législateur a choisi de renvoyer à un décret le soin de fixer la liste limitative des catégories de données qui peuvent être conservées par les opérateurs en exception au principe général d'effacement ou d'anonymisation des données relatives à une communication. La Commission relève, dès lors, que ce choix a pour conséquence d'empêcher les opérateurs de conserver – notamment à des fins de preuve en matière de contestation de la facturation ou du paiement des prestations – une donnée qui ne serait pas à l'origine prévue par le décret mais dont la conservation pourrait être rendue nécessaire par l'évolution technique de leurs services. Cette possibilité d'évolution d'ailleurs est implicitement prévue par la directive du 12 juillet

2002 qui, à la différence de la directive du 15 décembre 1997 [1] qu'elle abroge et remplace [2], ne précise plus limitativement les données pouvant être conservées au titre des données de connexion, dites « données relatives au trafic », mais se contente de les définir de manière générique en tant que *« données traitées en vue de l'acheminement d'une communication par un réseau de communication par un réseau de communications électroniques ou de sa facturation »* [3].

Une évolution législative modifiant ce schéma pourrait prévoir, par dérogation au principe d'anonymisation et d'effacement, un mécanisme de déclaration préalable soumis au contrôle de la CNIL pour les données nécessaires à la facturation. À défaut, la Commission recommande aux pouvoirs publics de porter une attention toute particulière aux futurs besoins des opérateurs afin de permettre, le cas échéant, une adaptation du décret.

Les données visées par le décret qui peuvent être conservées par les opérateurs tendent à permettre aux opérateurs de télécommunications de justifier la facturation de la communication passée ou des services rendus dans le cadre de cette communication.

La Commission relève que la donnée relative au numéro appelé et aux services complémentaires qui peuvent affecter un appel (renvoi, transfert ou ré-acheminement) ne sont pas prévus dans le cadre de l'article R. 9-1-1. Il conviendrait, dès lors, que ces informations – indispensables, par exemple, lorsqu'un opérateur téléphonique doit justifier le montant d'une facture – soient présentes au titre des données qui peuvent être traitées par les opérateurs.

De la même façon, les informations relatives à l'heure du début et de fin de la session de connexion à internet doivent pouvoir être conservées par les fournisseurs d'accès afin que ceux-ci puissent utiliser ces informations dans le cadre de la facturation.

2) La loi précise que ces données ne peuvent être utilisées et conservées que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, à savoir un an à compter du jour du paiement. Cette disposition, qui s'applique à l'ensemble des opérateurs de télécommunications, écarte les règles applicables en matière de prescription commerciale (dix ans) ou fiscale (de trois à six ans).

Sur les catégories de données conservées en vue d'assurer la sécurité des réseaux des opérateurs de télécommunications et sur leur durée de conservation

En application du III. de l'article L. 32-3-1 du Code des postes et télécommunications, l'article 2 du projet de décret introduit un article R. 9-1-1 dans le Code des postes et télécommunications dont le 4° traite des catégories de données techniques qui peuvent être conservées par les opérateurs de télécommunications au titre de la sécurité de leurs réseaux et installations.

1 Article 6 paragraphe 2 de la directive 97/66/CE du Parlement européen et de Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

2 La directive du 15 décembre 1997 n'a donc plus lieu d'être visée dans les visas du décret.

3 Article 2 de la directive du 12 juillet 2002 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

1) Les données visées par le projet de décret n'appellent pas d'observation de la part de la Commission.

2) La durée de conservation fixée à trois mois par le décret paraît proportionnée à la finalité de sécurité des réseaux des opérateurs de télécommunications.

Sur les catégories de données conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et sur leur durée de conservation

En application du II. de l'article L. 32-3-1 du Code des postes et télécommunications, l'article 2 du projet de décret introduit un article R. 9-1-2 dans le Code des postes et télécommunications qui traite des catégories de données techniques qui doivent être conservées par les opérateurs de télécommunications pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, ainsi que de leur durée de conservation, de l'évaluation et de la compensation des surcoûts issus de cette obligation.

1) La Commission rappelle que le décret doit indiquer de manière précise les catégories de données que les opérateurs doivent conserver pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales puisque cette conservation se fait en dérogation au principe général d'effacement ou d'anonymisation de ces données, la responsabilité pénale des opérateurs ou de leurs agents pouvant, à double titre, être engagée.

Certaines des données qui doivent être conservées par les opérateurs de télécommunications au titre de l'article R. 9-1-2 du Code des postes et télécommunications appellent les observations suivantes.

En premier lieu, le décret précise que les données relatives aux en-têtes de message des courriers électroniques doivent permettre *« d'identifier l'ensemble des destinataires »*. La Commission souhaite que soit précisée la portée de cette disposition. En effet, la conservation du nom de domaine du serveur de l'ensemble des messages électroniques qu'une personne aura écrits (par exemple, de nombreux messages adressés à des personnes titulaires d'une adresse électronique du type nom.prénom@syndicat.fr) peut être de nature à dévoiler des informations exclues par le champ d'application du décret. En tout état de cause, les dispositions législatives interdisent que soient conservées les informations relatives au contenu ou au titre du courrier électronique.

En second lieu, l'obligation faite aux opérateurs de télécommunications de conserver la donnée relative à l'adresse IP du terminal de l'usager exclut, pour ceux d'entre eux qui utiliseraient des serveurs « proxies », de conserver les informations relatives aux pages internet consultées par leurs clients. La conservation de telles données serait, en effet, contraire à l'article L. 32-3-1 du Code des postes et télécommunications. En conséquence, les fournisseurs d'accès auront l'obligation de scinder les données éventuellement enregistrées dans leurs serveurs « proxies » afin de ne conserver que les données relatives aux adresses IP de leurs clients, à l'exclusion de toute autre donnée qui pourrait en être issue.

2) L'article L. 32-3-1 introduit par la loi sur la sécurité quotidienne pose le principe d'une durée maximale d'un an pour la conservation par les opérateurs de télécommunications des données nécessaires à la recherche, la constatation et la poursuite d'infractions pénales. La durée précise de conservation est fixée par le projet de décret au maximum légal possible, à savoir un an.

Dans son avis relatif au projet de loi sur la société de l'information, la Commission avait estimé, qu'eu égard au caractère exceptionnel et dérogatoire du dispositif retenu, *« un délai de conservation de trois mois serait parfaitement proportionné et adapté aux intérêts en cause »*.

La Commission avait justifié sa position par le caractère largement dérogatoire aux principes généraux relatifs à la protection des données à caractère personnel d'une disposition qui oblige les opérateurs à conserver des données se rapportant à l'ensemble des personnes utilisant leurs services et qui ne présentent aucune utilité pour eux. Elle avait considéré, faisant application du principe de finalité, qu'une durée de trois mois serait adaptée aux objectifs d'intérêts publics poursuivis par le dispositif visé. Il y a lieu, dès lors, de s'interroger sur les circonstances de droit ou de fait qui seraient de nature à modifier cette position.

Il est incontestable que les infractions commises à l'aide des technologies de l'information ou directement liées à ces technologies ont fortement progressé lors de ces dernières années. De même, l'internationalisation de plus en plus fréquente de ces infractions impose sans aucun doute que les autorités judiciaires disposent des moyens adaptés à l'évolution de la criminalité. La Commission relève que la coopération internationale se renforce dans ce domaine afin de faciliter le rapprochement d'informations nécessaires aux enquêtes judiciaires. Pour autant, elle rappelle que l'objectif de lutte contre la criminalité et le terrorisme doit s'inscrire dans le respect des principes relatifs à la protection des données à caractère personnel.

À ce titre, la Commission estime qu'une durée de conservation limitée à trois mois par les opérateurs de télécommunications serait de nature à réduire les risques induits par un dispositif qui déroge aux règles applicables à la protection des données à caractère personnel, tout en permettant aux autorités judiciaires d'exercer leurs activités dans des conditions acceptables, étant entendu qu'elles peuvent toujours, dans le cadre d'une enquête, obtenir la préservation de certaines données.

Prospection commerciale

Délibération n° 03-040 du 23 septembre 2003 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

Vu la convention nº 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret d'application nº 78-774 du 17 juillet 1978 ;

Après avoir entendu Monsieur Maurice Benassayag en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Saisie par une association d'anciens élèves d'une plainte concernant la commercialisation par la société AlinéA d'un accès, via son site internet, à son fichier regroupant des données à caractère personnel concernant d'anciens élèves de grandes écoles ;

Émet les observations suivantes :

L'instruction de cette saisine fait apparaître que la société AlinéA ne dispose pas d'un accord avec l'ensemble des associations d'anciens élèves dont les annuaires sont exploités. Ainsi, il semble que le fichier mis en cause soit le résultat d'opérations consistant à scanner les annuaires papiers des associations d'anciens élèves.

S'il n'appartient pas à la Commission de régler un litige quant aux conditions commerciales d'utilisation de bases de données, il lui revient de veiller au respect des dispositions de la loi « informatique et libertés » lorsque ces bases contiennent des données nominatives. En l'occurrence, le mode de collecte des données ci-dessus exposé se trouve en contradiction avec certaines dispositions de la loi du 6 janvier 1978.

La collecte auprès de tiers d'informations nominatives n'est pas nécessairement déloyale. Cette pratique est courante en matière de marketing lors, par exemple, de l'achat ou de la location d'une base de données à des fins de prospection commerciale.

Le comportement fautif ici réside dans le fait de collecter des informations concernant une personne qui se serait opposée à une telle collecte. En effet, une personne a pu lors de son inscription sur un annuaire s'opposer légitimement, conformément à l'article 26 de la loi du 6 janvier 1978, à toute transmission à des tiers des informations la concernant.

Le fait de collecter à partir d'un fichier qui prend en l'occurrence la forme d'un annuaire des informations nominatives de personnes sans s'assurer que celles-ci n'ont pas exercé leur droit d'opposition à ce que ces informations soient transmises à des tiers revient à opérer une collecte déloyale et frauduleuse interdite par l'article 25 de la loi du 6 janvier 1978 et sanctionnée par l'article 226-18 du Code pénal qui dispose que *« le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende »*.

L'attention de la société AliNéA a été appelée sur le caractère déloyal et illicite de cette collecte, aussi bien lors de l'instruction de la déclaration du fichier mis en œuvre (courrier du 15 juin 1998) qu'à de nombreuses reprises lors de l'instruction de la saisine (courriers du 5 novembre 2001, du 20 février 2002, du 30 septembre 2002, du 1er janvier 2003). Ne contestant pas cette analyse, la société AliNéA s'est contentée d'indiquer qu'elle a contacté l'ensemble des personnes présentes dans la base de données dont elle commercialise l'accès afin de leur permettre d'exercer leurs droits d'opposition ou de modification sans pour autant s'engager à modifier sa méthode de collecte.

La Commission a alors, dans un courrier du 26 mai 2003, demandé à la société AliNéA d'apporter, dans un délai de quinze jours, les éléments précis et probants relatifs aux conditions de réalisation de l'opération relative au recueil du consentement de toutes les personnes dont la société traite les données et de s'engager à respecter le droit des personnes dont elle envisagerait, à l'avenir, de traiter les données.

Ce courrier est resté, à ce jour, sans réponse.

La Commission n'est ainsi pas en mesure d'assurer pleinement la mission d'instruction des plaintes et réclamations qu'elle reçoit compte tenu du comportement de l'organisme incriminé, susceptible de constituer le délit d'entrave pénalement sanctionné par l'article 43 de la loi du 6 janvier 1978 qui dispose que : *« Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :*
– soit en s'opposant à l'exercice des vérifications sur place ;
– soit en refusant de communiquer à ses membres, à ses agents ou aux magistrats mis à sa disposition, les renseignements et documents utiles à sa mission qui leur est confiée par la Commission ou en dissimulant lesdits documents ou renseignements, ou encore en les faisant disparaître ;
– soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements au moment où la demande a été formulée ou qui ne le présentent pas sous une forme directement intelligible. »

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet :
– l'opération de collecte illicite et déloyale de données à caractère personnel réalisée par la société AliNéA à partir d'annuaires sans s'assurer auprès des éditeurs de ces annuaires que les personnes auxquelles ces données se rattachent n'ont pas exercé leur droit d'opposition à ce que ces informations soient transmises à des tiers, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;
– le silence gardé par la société AliNéA suite au courrier de la Commission en date du 26 mai 2003 qui la mettait en demeure, dans un délai de quinze jours, d'une part, d'apporter, eu égard au mode de collecte initial, les preuves du recueil du consentement des personnes dont elle traite les données et, d'autre part, de se conformer à l'avenir aux dispositions de la loi « informatique et libertés », fait susceptible de constituer l'infraction visée par l'article 43 de la loi du 6 janvier 1978.

Et **transmet au parquet** les éléments du dossier.

Délibération n° 03-057 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie de deux plaintes par des personnes physiques qui ont reçu de la société Euro-Fax des télécopies publicitaires sans avoir exprimé leur consentement à être ainsi démarchées ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société Euro-Fax le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par deux personnes de plaintes concernant la réception de télécopies publicitaires qui leur ont été adressées sans leur consentement préalable par la société Euro-Fax.

Les plaignants ont indiqué qu'ils avaient reçu deux télécopies de la société Euro-Fax.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission et, depuis lors, cinq nouvelles plaintes ont été adressées à la CNIL par des personnes physiques qui ont reçu cinq télécopies de la société Euro-Fax.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télé-

communications a inséré dans le Code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société Euro-Fax a adressé des télécopies à des personnes physiques, qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait pour la société Euro-Fax d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments des différents dossiers de saisine reçus par la Commission.

Délibération n° 03-058 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie de six plaintes par des personnes physiques qui ont reçu de la société Datexia des télécopies publicitaires sans avoir exprimé leur consentement à être ainsi démarchée ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société Datexia le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par plusieurs personnes de plaintes concernant la réception de télécopies publicitaires qui leur ont été adressées sans leur consentement préalable par la société Datexia.

Les plaignants ont indiqué qu'ils avaient reçu quatorze télécopies de la société Datexia.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission et, depuis lors, huit nouvelles plaintes ont été adressées à la CNIL par des personnes physiques qui ont reçu vingt-trois télécopies de la société Datexia.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télécommunications a inséré dans le Code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société Datexia a adressé des télécopies à des personnes physiques qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société Datexia, d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments des différents dossiers de saisine reçus par la Commission.

Délibération n° 03-059 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie de deux plaintes par des personnes physiques qui ont reçu de la société CECOP des télécopies publicitaires sans avoir exprimé leur consentement à être ainsi démarchées ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société CECOP le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par deux personnes de plaintes concernant la réception de télécopies publicitaires qui leur ont été adressées sans leur consentement préalable par la société CECOP.

Les plaignants ont indiqué qu'ils avaient reçu deux télécopies de la société CECOP.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission et, depuis lors, une nouvelle plainte a été adressée à la CNIL par une personne physique qui a reçu deux télécopies de la société CECOP.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télécommunications a inséré dans le Code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société CECOP a adressé des télécopies à des personnes physiques qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société CECOP, d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments des différents dossiers de saisine reçus par la Commission.

Délibération n° 03-060 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par une personne physique qui a reçu de la société Groupe Nicolas Miguet une télécopie publicitaire sans avoir exprimé son consentement à être ainsi démarchée ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société Groupe Nicolas Miguet le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par une personne d'une plainte concernant la réception d'une télécopie publicitaire qui lui a été adressée sans son consentement préalable par la société Groupe Nicolas Miguet.

Le plaignant a indiqué qu'il avait reçu une télécopie de la société Groupe Nicolas Miguet.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission et, depuis lors, cinq nouvelles plaintes ont été adressées à la CNIL par des personnes physiques qui ont reçu neuf télécopies de la société Groupe Nicolas Miguet.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télécommunications a inséré dans le Code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société Groupe Nicolas Miguet a adressé des télécopies à des personnes physiques, qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société Groupe Nicolas Miguet, d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de transmettre au parquet les éléments des différents dossiers de saisine reçus par la Commission.

Délibération n° 03-061 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie de trois plaintes par des personnes physiques qui ont reçu de la société IMedia des télécopies publicitaires sans avoir exprimé leur consentement à être ainsi démarchées ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société IMedia le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par trois personnes de plaintes concernant la réception de télécopies publicitaires qui leur ont été adressées sans leur consentement préalable par la société IMedia.

Les plaignants ont indiqué qu'ils avaient reçu trois télécopies de la société IMedia.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission et, depuis lors, six nouvelles plaintes ont été adressées à la CNIL par des personnes physiques qui ont reçu six télécopies de la société IMedia.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télécommunications a inséré dans le Code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société IMedia a adressé des télécopies à des personnes physiques, qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société IMedia, d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments des différents dossiers de saisine reçus par la Commission.

Délibération n° 03-062 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie de deux plaintes par des personnes physiques qui ont reçu de la société Le Parisien Emploi des télécopies publicitaires sans avoir exprimé leur consentement à être ainsi démarchées ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société Le Parisien Emploi le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par deux personnes de plaintes concernant la réception de télécopies publicitaires qui leur ont été adressées sans leur consentement préalable par la société Le Parisien Emploi.

Les plaignants ont indiqué qu'ils avaient reçu six télécopies de la société Le Parisien Emploi.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance nº 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télé-

communications a inséré dans le code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualit de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société Le Parisien Emploi a adressé des télécopies à des personnes physiques, qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société Le Parisien Emploi, d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments des différents dossiers de saisine reçus par la Commission.

Délibération n° 03-063 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par une personne physique qui a reçu de la société Stratégies LRA Reed Business Information des télécopies publicitaires sans avoir exprimé son consentement à être ainsi démarchée ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société Stratégies LRA Reed Business Information le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par une personne d'une plainte concernant la réception d'une télécopie publicitaire qui lui a été adressée sans son consentement préalable par la société Stratégies LRA Reed Business Information.

Le plaignant a indiqué qu'il avait reçu une télécopie de la société Stratégies LRA Reed Business Information.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance nº 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télé-

communications a inséré dans le code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction de la plainte dont a été saisie la Commission fait apparaître que la société Stratégies LRA Reed Business Information a adressé une télécopie à une personne physique, qui déclare n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort de la copie adressée à la Commission par le plaignant que la télécopie litigieuse a été adressée postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, la personne qui a saisi la Commission agit *a priori* en tant que personne physique directement destinataire des télécopies et non pas comme le représentant d'une personne morale.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société Stratégies LRA Reed Business Information, d'avoir adressé à une personne physique, postérieurement au 6 août 2003, une télécopie publicitaire sans avoir obtenu son consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments du dossier de saisine reçu par la Commission.

Délibération n° 03-064 du 9 décembre 2003 portant dénonciation au parquet d'infractions au Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie d'une plainte par une personne physique qui a reçu de la société Xalis des télécopies publicitaires sans avoir exprimé son consentement à être ainsi démarchée ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 21, pris ensemble le décret d'application 78-774 du 17 juillet 1978 ;

Vu l'article L. 33-4-1 du Code des postes et télécommunications ;

Vu l'article L. 121-20-5 du Code de la consommation ;

Vu l'article R. 10-1 du Code des postes et télécommunications ;

Vu le règlement intérieur de la Commission, et notamment son article 57 ;

Vu le courrier adressé par la Commission à la société Xalis le 15 octobre 2003 ;

Après avoir entendu Monsieur Didier Gasse, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur les plaintes reçues par la Commission

La Commission a été saisie par une personne d'une plainte concernant la réception d'une télécopie publicitaire qui lui a été adressée sans son consentement préalable par la société Xalis.

Le plaignant a indiqué qu'il avait reçu une télécopie de la société Xalis.

La Commission a, par une lettre en date du 15 octobre 2003, rappelé à cette société les règles applicables, tout en lui demandant de lui faire connaître ses observations et de lui indiquer les mesures prises pour ne plus démarcher les personnes qui n'auraient pas exprimé leur consentement préalable à recevoir ses télécopies publicitaires.

Elle lui rappelait enfin qu'en application de l'article 21-4° de la loi du 6 janvier 1978, dans l'exercice de ses pouvoirs, la Commission adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance.

Cette société n'a pas répondu au courrier de la Commission et, depuis lors, quatre nouvelles plaintes ont été adressées à la CNIL par des personnes physiques qui ont reçu cinq télécopies de la société Xalis.

Sur les règles applicables en matière de télécopies non sollicitées

L'ordonnance nº 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télé-

communications a inséré dans le Code des postes et télécommunications un nouvel article L. 33-4-1 aux termes duquel *« est interdite la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Parallèlement, l'ordonnance n° 2001-741 du 23 août 2001 portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation a inséré un nouvel article L. 121-20-5 qui interdit *« la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels »*.

Enfin, le décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le Code des postes et télécommunications a modifié l'article R. 10-1 de ce Code en introduisant dans son deuxième alinéa une disposition selon laquelle la prospection directe des personnes physiques en violation des dispositions du premier alinéa de l'article L. 33-4-1 du Code *« est punie, pour chaque communication, de l'amende prévue par les contraventions de la quatrième classe, sous réserve de l'application du premier alinéa de l'article 226-18 du Code pénal »*.

Sur l'absence de consentement préalable et la qualité de personne physique des destinataires des télécopies

L'instruction des plaintes dont a été saisie la Commission fait apparaître que la société Xalis a adressé des télécopies à des personnes physiques, qui déclarent n'avoir pas donné un consentement rendu obligatoire par les articles précités du Code des postes et télécommunications et du Code de la consommation, fait désormais sanctionné par l'article R. 10-1 du Code des postes et télécommunications si la personne démarchée est une personne physique.

Il ressort des copies adressées à la Commission par les plaignants que les télécopies litigieuses ont été adressées postérieurement au 6 août 2003, date à laquelle le décret précité, modifiant l'article R. 10-1 du Code des postes et télécommunications, a été publié au *Journal officiel*.

Par ailleurs, selon les correspondances reçues, les personnes qui ont saisi la Commission agissent *a priori* en tant que personnes physiques directement destinataire des télécopies et non pas comme les représentants de personnes morales.

Constate que les faits portés à la connaissance de la Commission semblent réunir les éléments de l'infraction réprimée par l'article R. 10-1 du Code des postes et télécommunications, à savoir la prospection directe par télécopie de personnes physiques sans avoir obtenu leur consentement préalable.

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet le fait, pour la société Xalis, d'avoir adressé à des personnes physiques, postérieurement au 6 août 2003, des télécopies publicitaires sans avoir obtenu leur consentement préalable, fait susceptible de constituer l'infraction visée par l'article R. 10-1 du Code des postes et télécommunications, et de **transmettre au parquet** les éléments des différents dossiers de saisine reçus par la Commission.

Santé

Délibération n° 03-053 du 27 novembre 2003 portant adoption d'une recommandation relative aux traitements de données à caractère personnel mis en œuvre par les registres du cancer

La Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu les articles 226-13 et 226-14 du Code pénal relatifs au secret professionnel ;

Vu le décret nº 95-100 du 6 septembre 1995 portant code de déontologie médicale ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 ;

Vu l'arrêté du 6 novembre 1995 modifié relatif au Comité national des registres ;

Après avoir entendu Monsieur Pierre Leclercq, commissaire, en son rapport et Madame Pozzo di Borgo, commissaire-adjoint du Gouvernement, en ses observations ;

Formule les observations suivantes :

Les systèmes d'information mis en œuvre par les registres du cancer pour assurer le recueil continu, dans une zone géographique déterminée, de données personnelles de santé auprès des structures de soins qui participent au diagnostic de cancer et à la prise en charge des patients concernés constituent un fondement essentiel de la surveillance épidémiologique du cancer et s'inscrivent au cœur de la politique de lutte contre le cancer affirmée par les pouvoirs publics comme une priorité nationale en matière de santé publique.

L'efficacité de ce mode de surveillance épidémiologique implique que tous les professionnels de santé concernés participent à l'enrichissement des données gérées par les registres et qu'ils soient informés régulièrement des résultats de leur contribution.

Pour assurer la fiabilité et la qualité scientifique des statistiques produites, les registres du cancer doivent disposer de données individuelles qui permettent d'éliminer les doubles enregistrements, de rassembler et de vérifier sur un patient déterminé les renseignements obtenus, de suivre, cas par cas, l'évolution d'une pathologie ou d'une thérapeutique et de réaliser, le cas échéant, des enquêtes complémentaires.

À cet égard, la CNIL rappelle que la loi autorise les médecins qui participent au diagnostic et à la prise en charge des patients en cancérologie à transmettre des données nominatives à des personnes nommément désignées et astreintes au secret professionnel tel que défini par l'article 226-13 du Code pénal au sein des registres du cancer.

Les données personnelles de santé, parce qu'elles relèvent de l'intimité de la vie privée doivent faire l'objet d'une protection particulière, qu'imposent tant l'article 6 de la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel que l'article 8 de la directive européenne du 24 octobre 1995.

Après avoir procédé à une évaluation générale auprès des registres du cancer des modalités prévues pour assurer le respect des droits des personnes et des dispositions mises en œuvre pour garantir la confidentialité des données, la Commission estime nécessaire d'adopter les recommandations suivantes.

Sur l'information des personnes concernées

La Commission rappelle qu'en application de l'article 40-5 de la loi du 6 janvier 1978, les personnes dont les données sont transmises aux registres du cancer doivent être, avant le début du traitement de ces données, individuellement informées de la nature des informations transmises, de la finalité du traitement des données, des personnes physiques ou morales destinataires des données et des modalités d'exercice du droit d'accès, de rectification et de leur droit d'opposition.

L'obligation d'une information individuelle et personnalisée

La Commission estime qu'il appartient à chaque registre du cancer de définir les mesures appropriées afin que les malades concernés soient individuellement informés des conditions dans lesquelles certaines informations les concernant sont susceptibles d'être transmises au registre.

La Commission considère que seul le médecin, responsable de la prise en charge thérapeutique, en contact direct avec le patient est en mesure de procéder, au moment qu'il estimera le plus opportun et en conscience à cette information.

L'annonce d'un diagnostic de cancer constituant pour le patient un traumatisme grave, il appartient en effet au médecin de délivrer, dans l'intérêt du malade, une information adaptée et personnalisée tenant compte de son état psychologique.

Dans un souci de clarté des textes, la Commission estime que la rédaction des dispositions du III de l'article 25-20 du décret n° 78-774 du 17 juillet 1978 pourrait utilement être précisée de façon à indiquer que c'est le professionnel de santé en contact direct avec le patient et effectivement chargé de la prise en charge thérapeutique qui procède à l'information exigée par la loi.

Le contenu de l'information

La Commission considère que cette information doit permettre au malade de connaître le nom du registre du cancer, son adresse et les objectifs de santé publique qu'il poursuit. Le patient doit également être informé de la nature des informations transmises aux registres et des conditions dans lesquelles il peut refuser cette transmission.

La Commission préconise qu'à l'appui de cette information, une note reprenant l'ensemble de ces précisions soit remise au patient. La possibilité d'obtenir communication des données doit également lui être rappelée.

La CNIL recommande donc aux registres du cancer de mettre en place une procédure de rappel systématique aux professionnels de santé concernés de la nécessité d'informer individuellement les personnes tout en leur laissant le choix de

déterminer le moment qu'ils estimeront en conscience le plus opportun pour le patient.

La Commission souhaite que lorsqu'une prise en charge individualisée est proposée dans le cadre d'un réseau régional de soins en cancérologie, le document d'information qui doit être, à ce titre, remis à la personne et signé par elle mentionne aussi l'activité du registre du cancer.

Elle considère également que des réunions associant l'ensemble des acteurs locaux qui participent au fonctionnement des registres du cancer devraient être organisées afin de procéder à une information sur l'activité épidémiologique du registre, de rappeler la nécessité de l'information individuelle des malades et de définir en concertation les modalités pratiques de celle-ci.

La CNIL rappelle qu'une information générale sur l'existence du registre et ses principes de fonctionnement doit être diffusée dans les établissements de santé où s'exercent des activités de diagnostic et de soins donnant lieu à la transmission de données nominatives.

Sur la confidentialité des données

S'il est dans l'intérêt de la santé publique de disposer de statistiques fiables sur l'évolution du cancer en France et donc, de faire appel à des systèmes fondés sur le recueil à la source de données directement nominatives, il demeure que, eu égard à la sensibilité des informations traitées, toutes garanties doivent être prises pour assurer la confidentialité des informations.

Il convient que des mesures de sécurité physiques appropriées soient prises afin de contrôler l'accès aux locaux du registre et prévoir en particulier que les supports d'information ayant permis la collecte des données soient conservés dans des conditions de nature à garantir leur confidentialité (armoires fermées à clef par exemple).

Les conditions d'accès au système informatique doivent être arrêtées en particulier par une définition précise des modalités d'identification des personnes habilitées à accéder aux données. Dès lors, il importe qu'une politique de gestion des mots de passe individuels soit définie en fonction des habilitations reconnues à chacun et qu'un dispositif de déconnexion automatique en cas d'absence ou de frappes incorrectes du mot de passe soit instauré.

Il convient qu'un système de journalisation des connexions soit mis en place afin de permettre la détection d'éventuelles intrusions dans le système. Ce système devra également permettre de contrôler les éditions de listes effectuées à partir de données directement nominatives.

La base de données nominatives doit être chiffrée par un algorithme public réputé « fort ».

En cas de recours pour la maintenance à un prestataire extérieur au registre, il est nécessaire que le contrat de maintenance comporte une clause spécifique sur la confidentialité des données afin que l'accès à la base de données soit entouré de toutes les garanties. À cet effet, un registre de maintenance devra être mis en place et indiquer les dates et heures d'intervention ainsi que l'identité de la personne ayant effectué l'opération de maintenance et les raisons l'ayant justifiée.

De façon plus générale, il appartient à chaque registre du cancer de formaliser dans une charte de sécurité l'ensemble des mesures prises pour assurer la confidentialité des données. Ce document devrait être porté à la connaissance de chaque personne appelée à travailler au sein du registre.

Social

Délibération n° 03-002 du 21 janvier 2003 portant avis sur un projet de décret en Conseil d'État relatif à l'échantillon interrégimes de cotisants et à l'échantillon interrégimes de retraités et sur un projet d'arrêté relatif à l'échantillon interrégimes de cotisants

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis d'un projet de décret en Conseil d'État relatif à l'échantillon interrégimes de cotisants et à l'échantillon interrégimes de retraités et d'un projet d'arrêté interministériel relatif à l'échantillon interrégimes de cotisants (demande d'avis n° 829439) ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et notamment ses articles 15, 18 et 19 ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour son application ;

Vu l'article 1er de la loi n° 84-575 du 9 juillet 1984 portant diverses dispositions d'ordre social et création de l'échantillon interrégimes de retraités ;

Vu l'article 27 de la loi n° 2000-1257 du 23 décembre 2000 de financement de la sécurité sociale pour 2001 portant création de l'échantillon interrégimes de cotisants modifiée ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 00-041 du 21 septembre 2000 portant avis sur un projet de disposition législative relative à la création d'un répertoire national des retraites et des pensions et d'un échantillon interrégimes de cotisants ;

Après avoir entendu Monsieur Maurice Viennois, commissaire en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Sur les finalités poursuivies

La Commission nationale de l'informatique et des libertés est saisie par le ministère des Affaires sociales, du Travail et de l'Emploi d'une demande d'avis concernant la constitution, par la direction de la recherche, des études, de l'évaluation et des statistiques (DREES), d'un échantillon national interrégimes de cotisants et sa mise en œuvre conjointe avec un échantillon national interrégimes de retraités, afin de permettre aux pouvoirs publics d'évaluer les perspectives d'évolution de la situation des cotisants et des retraités au regard de leurs droits à retraite et les conséquences des réformes conduites dans ce domaine.

Les conditions de mise en œuvre de l'échantillon interrégimes de retraités, créé par l'article 1er de la loi nº 84-575 du 9 juillet 1984, ont été définies par les arrêtés du 17 mars 1988 et du 29 janvier 1993 modifiés pris après avis de la CNIL.

La mise en œuvre conjointe de l'échantillon interrégimes de cotisants et de l'échantillon interrégimes de retraités a pour finalité la constitution d'un système permanent d'informations statistiques relatif aux retraites.

Ces échantillons permettront notamment de mieux comprendre l'évolution des droits acquis à pension au cours d'une carrière professionnelle, ainsi que le rapport entre le montant des droits acquis ou de pensions de retraite d'une part et les rémunérations et revenus de remplacement perçus d'autre part.

Ponctuellement, les données de l'échantillons interrégimes de cotisants pourront être, sur la base d'une convention, mises à disposition des organismes participants – régimes de retraite obligatoire, UNEDIC, INSEE, direction générale de la comptabilité publique (DGCP), secrétariat général pour l'administration (SGA) du ministère de la Défense – ou à des organismes d'étude aux fins d'étude statistique et de recherche en matière de retraite conformément aux objectifs ci-dessus exposés.

La Commission considère cependant que les dispositions de l'article 10 de l'arrêté relatif à l'échantillon interrégimes de cotisants devraient être complétées de façon à prévoir que chaque convention précisera les finalités statistiques poursuivies dans le cadre de la mise à disposition de l'échantillon et contiendra l'engagement de l'organisme destinataire de ne pas traiter les données à d'autres fins et d'en assurer la sécurité.

La Commission souhaite également que soit inséré au projet d'arrêté un article prévoyant expressément que les données statistiques résultant des échantillons ou des enquêtes effectuées ne doivent pas pouvoir permettre l'identification directe ou indirecte, en particulier par recoupement d'informations, des personnes concernées.

Les échantillons interrégimes de cotisants et de retraités pourront également servir de base de sondage pour la réalisation, au bénéfice de la DREES, d'enquêtes statistiques dans le but d'affiner l'analyse découlant des seuls indicateurs présents dans ces échantillons.

La Commission prend acte que la réalisation de telles enquêtes ne pourra s'effectuer qu'après avis de la CNIL.

La Commission estime, sous les réserves ci-dessus énoncées, que les finalités ainsi poursuivies, qui s'inscrivent dans le cadre des objectifs définis par l'article 27 de la loi de financement de la sécurité sociale pour 2001 modifié et par l'article 1er de la loi du 9 juillet 1984, sont légitimes.

Sur les modalités de transmission et de traitement des informations

La mise en œuvre de chaque échantillon sera réalisée en trois étapes.

La première étape reposera sur la constitution, par l'INSEE, d'un « fichier d'identification de l'échantillon » contenant, d'une part, des informations extraites du répertoire national d'identification des personnes physiques (numéro d'inscription au répertoire NIR, nom patronymique, prénoms, sexe, date et lieu de naissance) et, d'autre part, un numéro d'ordre personnel propre à l'échantillon ainsi qu'un indicateur de repérage des individus dans la version précédente de l'un ou l'autre des échantillons.

S'agissant du fichier d'identification constitué dans le cadre de l'échantillon interrégimes de cotisants, il concernera, selon les années, les personnes nées dans une période comprise entre le 1er et le 12 du mois d'octobre des années 1934, 1938, 1942, 1950, 1954, 1958, 1962, 1966 ou 1970.

L'INSEE transmettra ce fichier aux régimes gestionnaires de retraite participants, à l'UNEDIC, à la Direction générale de la comptabilité publique, et au Secrétariat général pour l'administration du ministère de la Défense, selon des modalités assurant la confidentialité des données.

L'INSEE transmettra également à la DREES un fichier dit de « validation », permettant le contrôle par la DREES des fichiers qui lui seront ultérieurement transmis par les organismes participants, ainsi qu'un fichier dit « des personnes décédées » permettant le suivi des disparitions entre les tirages successifs de chaque échantillon.

Lors de la deuxième étape, les données du fichier d'identification seront appariées à l'aide du NIR avec celles détenues par les organismes gestionnaires dans leurs propres fichiers de gestion, afin de collecter les informations nécessaires à la constitution des échantillons, et en particulier les éléments de la carrière professionnelle nécessaires au calcul de la pension de retraite, ainsi que la nature et le montant des avantages de retraite et les conditions de liquidation des droits.

Les organismes participants transmettront ensuite à la DREES les données contenues dans les fichiers ainsi constituées.

La Commission prend acte de ce que le NIR ne sera utilisé que pour apparier les données sélectionnées contenues dans les fichiers de gestion des organismes participants, et que ni ce numéro, ni l'identité des personnes, pas plus que leur jour de naissance ne figureront dans les fichiers transmis à la DREES.

La troisième étape consistera en l'appariement par la DREES des fichiers transmis par les organismes participants au dispositif, grâce aux seuls numéros d'ordre personnels propres à l'échantillon. Ces numéros d'ordre personnels constitueront la seule information susceptible de permettre à la fois le chaînage des données dans le temps et la constitution, par la DREES, de bases de sondage pour la réalisation d'enquêtes auprès des personnes composant l'échantillon.

En cas de transmission – prévue par convention – d'une copie de l'échantillon à des services statistiques ou d'études ministériels ou à des organismes d'études, la DREES « anonymisera » la base de données en supprimant le numéro d'ordre personnel de l'échantillon.

La Commission estime que les modalités de transmission de ces données garantissent de façon satisfaisante leur confidentialité et l'anonymat des échantillons.

Sur l'information et le droit d'accès des personnes concernées par le traitement

La Commission prend acte de l'engagement de la DREES à ce que l'ensemble des organismes partenaires de l'échantillon procède à une information à caractère général sur la mise en œuvre de l'échantillon, notamment par affichage dans les locaux de ces organismes.

Le droit d'accès s'exercera auprès de la DREES par l'intermédiaire des organismes partenaires pour les fichiers qu'ils détiennent dans le cadre de la mise en œuvre de l'échantillon.

Compte tenu de ces observations :
– **émet un avis favorable** au projet de décret en Conseil relatif à l'échantillon interrégimes de cotisants et à l'échantillon interrégimes de retraités ;
– **émet un avis favorable** au projet d'arrêté interministériel présenté en application de l'article 15 de la loi du 6 janvier 1978, sous la réserve que l'article 10 de l'arrêté soit modifié de façon à prévoir que chaque convention précisera les finalités statistiques poursuivies dans le cadre de la mise à disposition de l'échantillon et contiendra l'engagement de l'organisme destinataire de ne pas traiter les données à d'autres fins et d'en assurer la sécurité ; et que soit inséré au projet d'arrêté un article prévoyant expressément que les données statistiques résultant des échantillons ou des enquêtes effectuées ne doivent pas pouvoir permettre l'identification directe ou indirecte, en particulier par recoupement d'informations, des personnes concernées.

Statistiques

Délibération n° 03-003 du 28 janvier 2003 portant avis sur la mise en œuvre, par l'INSEE, de la collecte des données lors du recensement des personnes résidant dans les communautés

La Commission nationale de l'informatique et des libertés, saisie pour avis par le directeur général de l'INSEE d'un projet d'arrêté autorisant l'INSEE à procéder à la collecte des données du recensement des personnes résidant dans les communautés ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi n° 2002-276 du 27 février 2002 relative à la démocratie de proximité, notamment son titre V ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi du 6 janvier 1978 susvisée ;

Vu sa délibération n° 02-111 du 19 décembre 2002 portant avis sur le projet de décret en Conseil d'État pris pour l'application du titre V de la loi n° 2002-276 du 27 février 2002 ;

Vu le projet d'arrêté portant création du traitement ;

Après avoir entendu Monsieur Guy Rosier, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

La Commission est saisie par l'INSEE de la mise en œuvre de la collecte des informations nominatives à l'occasion du recensement des personnes vivant dans les communautés présentes en métropole, dans les départements d'outre-mer et à Saint-Pierre-et-Miquelon.

Sont ainsi concernés les services de moyen ou long séjour des établissements publics ou privés de santé, les établissements sociaux de moyen et long séjour, les maisons de retraite, les foyers et résidences sociales ou assimilés ; les communautés religieuses ou assimilées ; les casernes, camps militaires ou assimilés ; les établissements hébergeant des élèves ou des étudiants ; les établissements pénitentiaires ; les établissements sociaux de court séjour.

Les informations recueillies auprès des personnes résidant dans les communautés, à l'exception de celles vivant dans les logements de fonction, sont relatives aux personnes physiques : date et lieu de naissance, sexe, nationalité, situation familiale, niveau et nature de la formation, études, activités professionnelles, lieu de résidence, lieu d'étude ou de travail, résidence antérieure, moyens de transport. Les

questions concernant les activités professionnelles ne sont pas posées aux personnes résidant dans les établissements pénitentiaires. Les personnes vivant dans les logements de fonction sont recensées la même année, lors de l'enquête de recensement effectuée dans la commune où est située la communauté. Les questions qui leur sont posées portent sur les personnes physiques et également sur les conditions de logement (conditions d'occupation des logements, caractéristiques et éléments de confort) et les immeubles bâtis (année de construction, caractéristiques d'équipement).

Les destinataires des données sont les agents habilités des directions régionales de l'INSEE concernées en métropole, dans les DOM et à Saint-Pierre-et-Miquelon.

Le droit d'accès et de rectification prévu par l'article 34 de la loi du 6 janvier 1978 s'exerce auprès des directions régionales de l'INSEE précitées.

Émet un avis favorable au projet d'arrêté qui lui est présenté sous réserve de la publication du décret en Conseil d'État pris pour l'application du titre V de la loi n° 2002-276 du 27 février 2002, tel qu'il a été examiné par la Commission.

Délibération n° 03-004 du 28 janvier 2003 portant avis sur le traitement automatisé d'informations nominatives, constitué par l'INSEE, à partir des fichiers de la taxe d'habitation

La Commission nationale de l'informatique et des libertés, saisie pour avis par le directeur général de l'INSEE d'un projet d'arrêté portant création d'un traitement automatisé d'informations nominatives à partir des fichiers de la taxe d'habitation ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi nº 2002-276 du 27 février 2002 relative à la démocratie de proximité, notamment son titre V ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi du 6 janvier 1978 susvisée ;

Vu sa délibération nº 02-111 du 19 décembre 2002 portant avis sur le projet de décret en Conseil d'État pris pour l'application du titre V de la loi nº 2002-276 du 27 février 2002 ;

Vu l'arrêté du 8 mars 1996 régissant le traitement informatisé de la taxe d'habitation à la direction générale des impôts ;

Vu le projet d'arrêté portant création du traitement ;

Après avoir entendu Monsieur Guy Rosier, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

La Commission est saisie par l'INSEE d'un projet d'arrêté portant création d'un traitement automatisé d'informations nominatives à partir de l'exploitation des données issues des fichiers de la taxe d'habitation (FTH).

Le traitement a pour objet de contrôler l'exhaustivité de la collecte des données du recensement de la population, de procéder à des estimations de population et de mettre à jour le répertoire des immeubles localisés, à l'exclusion de toute autre utilisation.

La Commission relève que cette mise à disposition de l'INSEE des données des fichiers de la taxe d'habitation est effectuée conformément aux dispositions de l'article 5 de l'arrêté susvisé du 8 mars 1996.

Les informations enregistrées sont les suivantes : le code département, le code INSEE commune (avec arrondissement pour Paris, Lyon, Marseille), le libellé de voie ou du lieudit, le code Rivoli, la section cadastrale (numéro de section et numéro de plan dans la section), le numéro de voie, l'indice de répétition (pour bis, ter, quater…), le complément d'adresse s'il existe, le bâtiment, l'escalier, le niveau, le code local (numéro du local par niveau), la nature du local, la superficie du local, le

nombre de pièces habitables (pour sélectionner les locaux qui ont au moins une pièce habitable), le code affectation (habitation, autres...), le code occupation (propriétaire, locataire, vacant...), le code taxation (résidence principale, résidence secondaire...), l'indicateur de lien entre locaux dont dispose une même personne à la même adresse, la discordance éventuelle entre la taxe d'habitation et le fichier des propriétés bâties pour ce local, le nombre de personnes à charge au sens de la taxe d'habitation, le nombre de personnes à charge au sens de l'impôt sur le revenu, le nom de l'occupant ainsi qu'un identifiant du local.

La Commission considère que ces données sont pertinentes, adéquates et non excessives au regard de la finalité poursuivie par le traitement.

Elle relève que le fichier fait l'objet d'une mise à jour annuelle et qu'il est détruit au bout de six ans, soit un an après la fin d'un cycle de recensement, lequel est quinquennal. Elle considère que cette opération doit être mentionnée dans un deuxième alinéa à l'article 2 du projet d'arrêté.

Seuls, les agents habilités de l'INSEE, soumis au respect du secret statistique, ont connaissance des informations et documents établis lors de ce traitement.

Le droit d'accès s'exerce auprès des directions générales de l'INSEE concernées.

Émet un avis favorable au projet d'arrêté qui lui est présenté sous réserve de l'insertion d'un deuxième alinéa à l'article 2 concernant la durée de conservation du fichier et de la publication du décret en Conseil d'État pris pour l'application du titre V de la loi nº 2002-276 du 27 février 2002, tel qu'il a été examiné par la Commission.

Délibération n° 03-005 du 28 janvier 2003 portant avis sur la mise en œuvre, par l'INSEE, d'une enquête cartographique dans les départements d'outre-mer

La Commission nationale de l'informatique et des libertés, saisie pour avis par le directeur général de l'INSEE d'un projet d'arrêté concernant la création d'un traitement automatisé d'informations nominatives dénommé « enquête cartographique dans les départements d'outre-mer » ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi nº 2002-276 du 27 février 2002 relative à la démocratie de proximité, notamment son titre V ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi du 6 janvier 1978 susvisée ;

Vu l'arrêté du ministre de l'Économie, des Finances et de l'Industrie du 19 juillet 2000, portant création d'un traitement automatisé d'informations individuelles relatif à la constitution et à la mise à jour par l'INSEE du Répertoire d'immeubles localisés (RIL) ;

Vu sa délibération nº 02-111 du 19 décembre 2002 portant avis sur le projet de décret en Conseil d'État pris pour l'application du titre V de la loi nº 2002-276 du 27 février 2002 ;

Vu le projet d'arrêté portant création du traitement ;

Après avoir entendu Monsieur Guy Rosier, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

La Commission est saisie par l'INSEE de la création d'un traitement automatisé dénommé « enquête cartographique » qui a pour finalité la localisation des immeubles dans les communes des départements d'outre-mer.

Ce traitement, dont l'utilisation est envisagée jusqu'à la fin de l'année 2008, doit permettre d'une part de contrôler l'exhaustivité de la collecte et d'autre part d'alimenter, dans les communes de 10 000 habitants et plus le répertoire des immeubles localisés de l'INSEE.

Les données de localisation des immeubles enregistrées dans le traitement sont relatives à :

– en ce qui concerne les immeubles bâtis : les coordonnées géographiques, le type et le nom de la voie, le numéro dans la voie, un complément d'adresse si nécessaire, le type d'immeuble, la date de construction, la date d'entrée dans le RIL, la date de dernière modification ou de destruction, l'aspect du bâti, le nombre de logements, le

nombre d'étages, le nombre de communautés, le nombre d'établissements, le nombre d'équipements urbains ;
– en ce qui concerne le logement : l'immeuble auquel ce logement appartient, l'étage, la position dans l'étage, le numéro de porte, le nom de l'occupant principal.

Ces données de localisation sont, en application de l'article 156 de la loi susvisée du 27 février 2002, nécessaires à la réalisation des enquêtes de recensement. Les données relatives aux immeubles sont identiques à celles figurant dans le répertoire des immeubles localisés de l'INSEE.

S'agissant de la mention du nom de l'occupant principal, au titre des données de localisation des logements, la Commission relève que cette information est utile pour identifier avec certitude les logements recensés et assurer ainsi l'exhaustivité de la collecte.

Les destinataires de l'ensemble des données sont les agents habilités de l'INSEE. Les informations relatives à la localisation des immeubles, qui sont nécessaires à la préparation et à la réalisation des enquêtes de recensement, sont librement échangées entre l'INSEE, les communes et les établissements publics de coopération intercommunale concernés.

Le droit d'accès et de rectification prévu par l'article 34 de la loi du 6 janvier 1978 s'exerce auprès de la direction régionale de l'INSEE pour la Réunion et auprès de la direction interrégionale des Antilles-Guyane de l'INSEE pour la Guadeloupe, la Martinique et la Guyane.

Émet un avis favorable au projet d'arrêté qui lui est présenté sous réserve de la publication du décret en Conseil d'État pris pour l'application du titre V de la loi n° 2002-276 du 27 février 2002, tel qu'il a été examiné par la Commission.

Délibération n° 03-068 du 18 décembre 2003 portant avis sur le projet d'arrêté portant création, par l'INSEE, d'un traitement automatisé pour la saisie et l'exploitation des données collectées lors du recensement général de la population

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis d'un projet d'arrêté par le directeur général de l'INSEE ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi nº 69-3 du 3 janvier 1969 modifiée relative à l'exercice des activités ambulantes et au régime applicable aux personnes circulant en France sans domicile ni résidence fixe ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi nº 2002-276 du 27 février 2002 relative à la démocratie de proximité, notamment son titre V ;

Vu le décret nº 78-774 du 17 juillet 1979 modifié portant application de la loi du 6 janvier 1978 susvisée ;

Vu le décret nº 2003-485 du 5 juin 2003 relatif au recensement de la population, notamment son article 33 ;

Vu l'arrêté du 23 mai 1984 relatif à l'échantillon démographique permanent ;

Vu l'arrêté du 26 juin 2003 modifié autorisant la mise en œuvre d'une collecte d'informations auprès des personnes résidant dans les communautés ;

Après avoir entendu M. Guy Rosier, commissaire en son rapport et Mme Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Commission est saisie par l'INSEE, en application de l'article 33 du décret nº 2003-485 du 5 juin 2003, de la mise en œuvre de traitements à l'occasion de la phase de saisie et d'exploitation des données collectées chaque année, à compter de 2004, pour le recensement de la population.

Les données sont recueillies d'une part, par les communes et les établissements publics de coopération intercommunale lors des enquêtes de recensement menées auprès des logements, les personnes sans abri et les personnes résidant habituellement dans des habitations mobiles terrestres, d'autre part, par l'INSEE, pour ce qui concerne les communautés.

La phase de saisie et d'exploitation des données suppose différentes étapes : « l'acquisition » sur support informatique par lecture optique des données, la mesure de la qualité de l'acquisition des données, le contrôle de la cohérence des questionnaires et le redressement des non-réponses, la validation des données.

Pour la réalisation du traitement destiné à l'acquisition sur support informatique des images des questionnaires et à la constitution par saisie ou reconnaissance

automatique de caractères, à partir des images et ensuite pour le contrôle de la qualité du travail effectué, l'INSEE fera appel à deux sous-traitants.

Les données traitées sont, à l'exception du nom et des prénoms, issues des bulletins individuels et des feuilles de logement, conformément aux dispositions des articles 26 et 38 du décret précité de 2003, complétées pour ce qui concerne les communautés, par l'article 2 de l'arrêté du 26 juin 2003 susvisé.

Ces données sont les suivantes :
– s'agissant des personnes physiques : la date et le lieu de naissance, le sexe, la nationalité, la situation familiale, le niveau et la nature de la formation, les études, les activités professionnelles, le lieu de résidence, le lieu d'étude ou de travail, la résidence antérieure, les moyens de transport, les conditions de logement et l'équipement en véhicules automobiles ;
– s'agissant des logements : les caractéristiques de confort et d'occupation, l'immeuble auquel appartient le logement et l'étage du logement ;
– s'agissant des immeubles : les coordonnées géographiques des immeubles bâtis, le type et le nom de la voie, le numéro dans la voie, un complément d'adresse si celui-ci est nécessaire, le type d'immeuble, la date de construction, la date d'entrée dans le répertoire d'immeubles localisés, la date de dernière modification (ou de destruction), l'aspect du bâti, le nombre de logements, le nombre d'étages, le nombre de communautés, le nombre d'établissements, le nombre d'équipements urbains ;
– un code à barres, apposé automatiquement sur chaque questionnaire lors de leur impression, qui comporte dix chiffres : le premier désigne le millésime de l'enquête de recensement, le second donne le type de questionnaire, les huit derniers chiffres composent un numéro d'ordre non significatif.

Ce code à barres permet à l'INSEE, lors de la réception des questionnaires d'établir un lien entre le code à barres de la feuille de logement et celui de chacun des bulletins individuels qui lui sont rattachés.

À l'issue de la phase d'acquisition des données et de contrôle de la qualité de cette saisie, sont constitués deux fichiers de données et une base d'images :
– le fichier « complet anonyme », qui comporte toutes les données, à l'exception du nom et des prénoms des personnes. Il est complété par l'INSEE, pour les personnes ayant une activité salariée et pour les entrepreneurs individuels, par les mentions de l'activité économique, de la catégorie juridique, de la tranche d'effectif, de la localisation de l'établissement concerné. L'exploitation de ce fichier permettra à l'INSEE d'élaborer les résultats du recensement de la population ;
– le fichier de l'échantillon démographique permanent, qui intègre les nom, prénom, sexe, date et lieu de naissance, code à barres issus des bulletins individuels des personnes nées entre le 1er et le 4 octobre chaque année, qui de ce fait, appartiennent à l'échantillon permanent. Ce fichier est destiné à la mise à jour de l'échantillon démographique permanent ;
– la base image « adresses issues de la feuille de logement », qui reprend les données de localisation, telles que prévues par l'article 26 du décret du 5 juin 2003 ainsi que le code à barres. Cette base servira à préparer les enquêtes statistiques ultérieures menées par l'INSEE.

Dès réception des fichiers, l'INSEE réalise un travail de codification des données et de redressement des non-réponses traditionnellement réalisé.

L'INSEE procède par ailleurs, afin de calculer la population comptée à part des communes, au rapprochement de la liste des personnes rattachées administrativement à une commune dans les conditions prévues par la loi du 3 janvier 1969 susvisée avec les bulletins individuels des personnes résidant dans une habitation

mobile et ceux des personnes sans abri recensées sur le territoire de cette commune. Ce rapprochement réalisé manuellement ne donne lieu à aucune saisie nominative.

Le seul destinataire de l'ensemble des données est l'INSEE. Les Archives de France, moyennant la signature de protocoles d'accord avec l'INSEE, lesquels seront soumis à la CNIL ainsi que s'y est engagé l'INSEE, pourront recevoir des documents, des fichiers et des bases d'images.

L'INSEE détruira le fichier de l'échantillon démographique permanent au plus tard à la fin de l'année suivant celle de sa réception définitive ; la base « adresse des logements » sera, pour sa part, supprimée au plus tard à la fin de la sixième année suivant celle de sa réception définitive.

Les bases images échantillon réalisées lors du contrôle de la qualité de la saisie seront détruites par l'INSEE dans les deux jours ouvrés qui suivent la notification de la réception définitive du fichier complet anonyme par les sous-traitants. Ces derniers détruiront, dans ce même délai, toutes les données en leur possession à l'exclusion des questionnaires qui seront retournés à l'INSEE.

Les mesures spécifiques de sécurité ont été définies par l'INSEE dans les marchés signés avec les sous-traitants. Elles portent sur le transport et le stockage des documents, les locaux, les procédures, les matériels et logiciels utilisés, les contrôles exercés par l'INSEE. Elles font l'objet d'annexes détaillées jointes au dossier de demande d'avis déposé par l'INSEE auprès de la CNIL.

Émet un avis favorable au projet d'arrêté qui lui a été présenté.

Transports

Délibération n° 03-008 du 27 février 2003 portant avis sur un traitement de la Régie autonome des transports parisiens ayant pour finalité l'exploitation des données de validation des passes Navigo

La Commission nationale de l'informatique et des libertés ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978, pris pour l'application de la loi susvisée ;

Vu la demande d'avis nº 826335 relative au traitement ayant pour finalité l'exploitation des données de validation des passes « Navigo » présenté par la RATP ;

Vu le projet d'acte réglementaire du président-directeur général de la RATP portant création du traitement ;

Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport et Madame Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement, en ses observations ;

Formule les observations suivantes :

La RATP a saisi la Commission le 22 avril 2002 d'une demande d'avis concernant la mise en œuvre d'un traitement de statistiques de validation et de détection de titres frauduleux dans le cadre du dispositif de télébillettique dénommé « Navigo ». La Commission a examiné ce traitement lors de la séance plénière du 27 juin 2002 et a estimé devoir différer son avis définitif sur la demande dont elle était saisie, dans l'attente de compléments d'informations.

Ainsi à la suite de nombreux entretiens, la RATP a fait parvenir à la CNIL, le 5 novembre 2002, un dossier exposant les modifications proposées au traitement télébillettique « Navigo ».

Le passe « Navigo » est un système de billettique qui s'inscrit dans le contexte de la généralisation de la télébillettique en Ile-de-France, devant à terme être mise en œuvre par toutes les entreprises de transport en commun de la région, sous le pilotage du syndicat des transports d'Ile-de-France (STIF).

Il s'agit d'une carte à puce permettant le passage des contrôles d'accès « sans contact » grâce à une transmission radio. La télétransmission des données s'effectue à distance, lorsque l'on approche la carte de la cible de validation repérée sur les tourniquets et portillons. Ce titre de transport devrait, selon les responsables du projet, apporter une amélioration notable du service rendu aux voyageurs par l'utilisation du même passe quel que soit le transporteur (train, métro ou bus) et un passage plus fluide aux tourniquets, les usagers n'ayant plus à introduire un ticket.

La diffusion du passe sans contact Navigo doit s'échelonner jusqu'en 2007, avec trois phases principales : conversion, initiée dès 2002, des abonnements annuels de type carte « Intégrale » et carte « Imagine R » réservée aux moins de 26 ans, puis celle des abonnements mensuels et hebdomadaires d'ici 2004 et enfin celle des billets à la journée et carnets d'ici 2007.

Dans le cadre de cette généralisation, la RATP a saisi la Commission d'une demande d'avis qui, au-delà de l'objectif ci-dessus rappelé, a pour finalité d'assurer les opérations d'après-vente et le contrôle des titres de transport, de mesurer la qualité du fonctionnement du système en vue d'en améliorer le fonctionnement, d'établir des statistiques d'utilisation des réseaux, de détecter la contrefaçon éventuelle des titres de transport et d'une manière générale toute fraude technologique.

Les données contenues dans le passe « Navigo » sont le numéro de série du passe et sa période de validité, le numéro d'abonnement, le type de contrat, sa validité temporelle et géographique, la date, l'heure et lieu des trois dernières validations, et enfin en cas de refus de validation, la date, l'heure, le lieu, et le motif du refus.

S'agissant des données remontant vers le système central, les valideurs, tourniquets et portillons communiquent les informations vers un serveur chargé de trier et redistribuer les données vers les différents serveurs du système central en fonction des traitements à appliquer. Ainsi, ce serveur reçoit les données relatives au numéro de série du passe, la date, l'heure, le lieu, le contrat concerné, l'authentifiant du passe, l'identifiant anonyme du passe, le type d'événement (entrée, sortie, correspondance, réseau) et le résultat de la validation.

Les destinataires des données diffèrent en fonction des traitements appliqués : d'une manière générale, il s'agit du responsable de l'ingénierie et de la maintenance, de la cellule surveillance de la fraude, des contrôleurs et des agents de guichet, ces derniers n'ayant accès qu'au numéro du passe et n'étant pas en mesure de faire la corrélation entre le numéro du passe et le numéro de dossier client contenant les informations nominatives.

Il n'est pas prévu de faire de rapprochement entre les historiques de validation des passes (numéro de passe et données de géolocalisation) et les porteurs propriétaires de ces passes.

Les traitements programmés pour la gestion des fraudes sont le contrôle de cohérence entre le numéro de contrat et le numéro de série de la carte, la vérification de la validité de l'authentifiant et le contrôle visant à identifier une utilisation anormale du passe.

Le système est paramétré afin d'invalider les cartes en cas de perte ou de vol de celles-ci, de cessation de paiement ou de duplication de la carte. Aucune action automatique ne découle d'un traitement informatique car toute invalidation de la carte appelle une intervention humaine.

S'agissant du traitement portant sur les données de validation, les problèmes liés à la traçabilité, à l'anonymat des déplacements et à la mise sous surveillance d'une carte aux fins de suivre son porteur ont été résolus de la manière suivante dans la nouvelle version du dossier présenté par la RATP : le traitement indirectement nominatif des données relatives aux déplacements des individus est exclusivement limité à une finalité de lutte contre la fraude, la RATP ayant, suite aux recommandations de la CNIL, décidé d'intégrer un identifiant anonyme du passe afin de rendre tous les autres traitements anonymes.

En effet, c'est uniquement dans le cadre du traitement de détection de la fraude que les données de validation, contenant des informations relatives aux

déplacements des personnes, sont associées au numéro de carte, information indirectement nominative puisque pouvant être rattachée à l'identité d'un usager. Pour tous les autres traitements, le numéro de série de la carte est remplacé par un « identifiant anonyme du passe », à définir par le STIF, calculé à partir du numéro de série de la carte et de l'authentifiant du passe inscrit en usine au moyen d'une fonction de « hachage » ne permettant pas le calcul inverse.

Afin de rendre impossible l'accès aux données relatives aux déplacements des personnes associées au numéro de la carte en dehors du traitement de la fraude, les conditions d'accès à ces données ont été renforcées et les données transitant sur le serveur chargé de la redistribution des données sont effacées en fin de journée qu'elles aient pu être redistribuées dans les différentes parties du système central ou non.

Enfin, la RATP garantit que les usagers auront toujours la possibilité de continuer à voyager anonymement tout en bénéficiant d'un titre télébillettique.

S'agissant de l'adéquation du dispositif par rapport à la finalité de contrôle de la fraude, la Commission estime que cette préoccupation est légitime mais elle s'interroge toutefois sur la nécessité de faire remonter les informations relatives aux déplacements. Elle estime dès lors nécessaire qu'une étude de faisabilité soit réalisée sur la mise en place d'un procédé technique permettant d'éviter la remontée de telles informations.

Par ailleurs, au-delà de la lutte contre la fraude et compte tenu des nombreuses expérimentations poursuivies par la RATP depuis 1992 en matière de « passe sans contact », il n'est pas douteux que cette solution technique soit appelée à se développer en direction de partenariats de nature commerciale visant les usagers. Le traitement sur lequel se prononce la Commission ne traite aucunement de ces aspects qui feront l'objet d'une attention toute particulière de sa part.

S'agissant de la durée de conservation des données relatives aux déplacements, les données de validation associées au numéro de carte ne sont conservées qu'une journée plus une au maximum (J +1) et ceci dans la seule finalité d'un traitement de la fraude, tous les autres traitements étant anonymisés. Les informations relatives aux cartes ayant donné lieu à une alarme sont conservées deux semaines pour analyse et jusqu'à six mois en cas de fraude avérée, hors procédure judiciaire.

Cette durée limitée à un jour plus un au maximum paraît de nature à empêcher les détournements de finalité.

S'agissant de la durée de conservation sur le passe lui-même, les données de validation s'écrasent au fur et à mesure et seuls les trois derniers déplacements sont lisibles sur le passe.

S'agissant de l'exercice du droit d'accès et conformément aux recommandations de la Commission, l'accès aux données contenues dans le passe s'effectuera désormais uniquement auprès des guichets de la RATP, ce qui permettra aux agents de la RATP de s'assurer, par un contrôle visuel, qu'ils délivrent les informations au véritable titulaire du passe « Navigo » dont la photo figure sur le passe.

Enfin, un accès aux données relatives aux « listes noires » est aménagé ; il s'exercera en s'adressant au département commercial de la RATP.

S'agissant de la période transitoire, la RATP prévoit une période transitoire jusqu'en fin 2003 en vue d'assurer une mise en œuvre optimum du système, de procéder aux corrections nécessaires et permettre au syndicat des transports d'Ile-de-France (STIF) de définir la fonction de « hachage » devant conduire, au plus tard, à partir de 2004, à anonymiser les traitements.

Pour faire suite aux recommandations de la Commission, la RATP a procédé à la modification des traitements envisagés pendant cette période. En effet, pour les traitements, autres que la lutte contre la fraude, nécessitant la remontée du numéro de carte, seule la date du trajet figurera dans le système, le lieu étant systématiquement occulté ce qui apparaît satisfaisant au regard de la liberté d'aller et venir, étant observé que, après la mise en place du « hachage », la donnée « lieu » sera uniquement collectée pour les relevés statistiques anonymes.

Le dispositif ainsi mis en œuvre apparaît dès lors adapté et proportionné aux objectifs poursuivis par la RATP. Toutefois, la Commission souhaite pouvoir se prononcer à titre définitif à l'issue de la phase transitoire et devra donc être saisie d'un nouveau dossier avant la fin de l'année 2003.

Émet un avis favorable au projet présenté sous réserve :
1) que l'article 1 du projet d'acte réglementaire précise que le traitement envisagé ne concerne que les abonnements annuels et est établi jusqu'à la fin de l'année 2003 ;
2) que soit précisé, à l'article 2 du projet d'acte réglementaire que l'exploitation de la mention « lieu » au titre des données contenues dans les systèmes centraux – transaction de validation – n'aura pas lieu, hormis pour le traitement de la fraude, pendant la phase transitoire (donc jusqu'à la fin de 2003) et ne sera effective qu'à compter de l'anonymisation des traitements.

Demande :
1) que la Commission soit saisie dans les meilleurs délais d'une demande de conseil afin de pouvoir évaluer la fonction de « hachage » devant être définie par le STIF ;
2) qu'une étude de faisabilité sur la mise en place d'un procédé technique permettant d'éviter la remontée dans les systèmes centraux d'informations relatives aux points d'entrée et de sortie des usagers soit réalisée ;
3) qu'un bilan quantitatif et qualitatif soit établi sur les conditions de déploiement du passe sans contact Navigo à l'issue de la phase transitoire.

Délibération n° 03-012 du 11 mars 2003 portant recommandation relative à la gestion de fichiers de personnes à risques par les loueurs de véhicules

La Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pris ensemble le décret d'application du 17 juillet 1978 ;

Vu le Code de la consommation, notamment l'article L. 122-1 ;

Après avoir entendu Monsieur Guy Rosier commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Saisie de plaintes par plusieurs personnes qui se voient refuser la location d'un véhicule, la Commission a procédé à plusieurs vérifications sur place auprès des principales sociétés exerçant cette activité et de leur chambre syndicale, le Conseil national des professions de l'automobile – branche loueurs –.

Des constats opérés lors de ces missions, il apparaît que les loueurs de véhicules gèrent un fichier nominatif, le plus souvent informatisé, et, sur la base des informations ainsi collectées, décident de refuser la location d'un véhicule ; il appartient dès lors à la Commission de faire part des préconisations suivantes aux responsables des traitements automatisés d'informations nominatives concernés.

Sur la création et la tenue de fichiers de personnes à risques

La Commission rappelle qu'aux termes de l'article 2 alinéa 2 de la loi du 6 janvier 1978, *« aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé »*.

La décision d'inscrire une personne dans un fichier spécifique ou l'enregistrement de données la concernant dans un fichier clientèle qui pourrait conduire à lui refuser la location d'un véhicule devrait relever des agents ayant compétence pour vérifier le caractère certain du préjudice subi et habilités à cet effet par la société ou l'organisme concerné.

La Commission rappelle également qu'aux termes des dispositions du Code de la consommation, il est interdit de refuser à un consommateur la vente d'un produit ou la prestation d'un service, sauf motif légitime. En outre, selon l'article 5c) de la convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être pertinentes, adéquates et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées.

En conséquence, l'inscription d'une personne dans un fichier spécifique ou l'enregistrement de données la concernant dans un fichier clientèle qui conduit à refu-

ser la location d'un véhicule doit reposer sur des motifs objectifs opposables à la personne concernée, faisant abstraction de tout jugement de valeur ou d'une appréciation de son comportement. La Commission recommande qu'une liste des motifs d'inscription soit pré-établie et que toute inscription sans indication de motif soit exclue.

La Commission recommande qu'une distinction soit établie entre les motifs d'inscription résultant du comportement d'un conducteur employé par une société ou un organisme et les motifs d'inscription imputables à ladite société ou audit organisme.

Par ailleurs, la Commission appelle l'attention des responsables des sociétés de location de véhicules sur la nécessité d'adopter des mesures permettant de pallier tout risque d'homonymie, notamment dans des cas signalés d'usurpation d'identité.

Sur la durée de conservation des données

La Commission rappelle qu'aux termes de l'article 5e) de la convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ces données ne doivent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire aux finalités pour lesquelles elles sont enregistrées.

Il appartient en conséquence aux responsables des sociétés ou organismes concernés de fixer des durées de conservation des données enregistrées, directement ou indirectement nominatives, adaptées aux différents motifs d'inscription, et de mettre en œuvre des procédures de mise à jour et de suppression des informations. Ainsi, les données enregistrées à la suite d'un impayé devraient être supprimées dès lors que le montant de la facture est réglé ou, à défaut, à l'expiration d'un délai déterminé.

Sur l'information des personnes

En application de l'article 27 de la loi du 6 janvier 1978, les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées :
– du caractère obligatoire ou facultatif des réponses ;
– des conséquences à leur égard d'un défaut de réponse ;
– des personnes physiques ou morales destinataires des informations ;
– de l'existence d'un droit d'accès et de rectification.

Lorsque de telles informations sont recueillies par voie de questionnaires, ceux-ci doivent porter mention de ces prescriptions.

La Commission rappelle en outre qu'aux termes de l'article 26 de la loi précitée, toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement.

La Commission recommande que les personnes soient systématiquement informées par les sociétés ou organismes concernés de l'existence d'un fichier spécifique ou de la possibilité d'enregistrer dans un fichier clientèle des données qui conduisent à refuser la location d'un véhicule, des motifs d'inscription, des destinataires des données, – information qui revêt une importance particulière lorsque les données sont mutualisées – et de leur faculté d'exercer leur droit d'accès, conformément à l'article 34 de la loi du 6 janvier 1978. La Commission rappelle que la communica-

tion des informations doit s'effectuer en langage clair et être conforme au contenu des enregistrements.

La Commission recommande en outre que, sauf exception légitime, toute personne inscrite sur un fichier spécifique ou faisant l'objet de l'enregistrement de données conduisant à lui refuser la location d'un véhicule en soit informée dès son inscription, afin qu'elle soit en mesure de présenter alors ses éventuelles observations.

Sur la sécurité et la confidentialité des données

La Commission rappelle qu'aux termes de l'article 29 de la loi du 6 janvier 1978, tout responsable de traitement automatisé d'informations nominatives s'engage vis-à-vis des personnes concernées à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

En conséquence, elle appelle l'attention des responsables des traitements automatisés d'informations nominatives concernés sur la nécessité de veiller à ce que, sous réserve de l'application de l'article 27 de la loi, les données ne soient communiquées qu'aux seuls professionnels de la location de véhicules, et ce par des moyens sécurisés (fichier ou mèl crypté).

Délibération n° 03-038 du 16 septembre 2003 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques

La Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 précitée ;

Vu l'article 9 du Code civil ;

Vu les articles 226-16 à 226-24 du Code pénal ;

Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations.

Formule les observations suivantes :

La modernisation des transports collectifs a conduit de nombreuses sociétés à proposer de nouveaux titres de transport à leurs usagers, reposant sur l'utilisation de cartes nominatives, magnétiques ou à puce. Il en découle la mise en œuvre par ces sociétés de traitements automatisés d'informations nominatives, au sens de l'article 5 de la loi du 6 janvier 1978. Ces outils billettiques sont conçus pour faciliter l'accès et les déplacements des voyageurs et leur proposer des services complémentaires.

La Commission constate que l'utilisation de ces cartes nominatives entraîne la collecte, à l'occasion de la validation, c'est-à-dire la présentation de la carte devant une borne de contrôle en entrée, sortie du réseau, ainsi qu'à l'occasion d'une correspondance, des trajets effectués par le titulaire. Vont ainsi être mémorisés, tant sur la carte que dans l'ordinateur central de la société de transport, les date, heure et lieu des passages ainsi que le numéro de carte utilisé. Or, ce numéro de carte est indirectement nominatif au sens de l'article 4 de la loi du 6 janvier 1978 car il rend possible l'identification du titulaire de la carte dont les coordonnées figurent dans le fichier clientèle.

Dès lors, les traitements automatisés mis en œuvre pour assurer le bon fonctionnement de ces titres billettiques créent un risque sérieux en matière de protection des données personnelles. En effet, les déplacements des personnes utilisant ces cartes peuvent être reconstitués et ne sont plus anonymes, ce qui est de nature à porter atteinte tant à la liberté, fondamentale et constitutionnelle, d'aller et venir, qu'au droit à la vie privée qui constitue également un principe de valeur constitutionnelle.

La Commission nationale de l'informatique et des libertés, qui est chargée de veiller à ce que l'informatique ne porte atteinte ni à la vie privée ni aux libertés individuelles ou publiques, considère qu'il y a lieu d'attacher un soin particulier à la mise en œuvre de tels traitements.

Cette recommandation est applicable quelle que soit la forme sous laquelle les informations relatives aux déplacements des personnes sont conservées, qu'il

s'agisse de traitements automatisés d'informations nominatives ou de fichiers manuels ou mécanographiques.

Recommande :

Sur les finalités du traitement

En application de l'article 5 b) et c) de la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel : *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont* […] *enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités, et sont* […] *adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ».*

Les finalités justifiant la mise en œuvre des traitements de billettique doivent être clairement indiquées et détaillées parmi les cinq catégories suivantes :

• Délivrance et utilisation des titres de transport :
– gestion des abonnements et délivrance des titres de transport ;
– gestion des opérations de contrôle des titres de transport ;
– gestion des opérations du service après vente.

• Gestion et suivi des relations commerciales :
– gestion des offres commerciales (partenariats, personnalisation des offres…) ;
– gestion des programmes de fidélisation.

• Gestion de la fraude :
– détection de la contrefaçon et de la fraude technologique ;
– instruction des dossiers de fraude technologique ;
– gestion des cartes mises en liste noire suite à une perte ou un vol ;
– gestion des cartes mises en liste noire suite à la détection d'un usage abusif ;
– gestion des cartes mises en liste noire suite à un incident de paiement.

• Analyses statistiques d'utilisation des réseaux :
– analyses statistiques du trafic ;
– analyses statistiques de la nature des titres de transport délivrés ;
– analyses statistiques d'utilisation par type de titres de transport.

• Mesure de la qualité du fonctionnement du système :
– analyses des problèmes techniques liés à la carte ;
– analyses des problèmes techniques liés aux valideurs ;
– détection des anomalies fonctionnelles du système d'information.

Sur la nature des informations collectées

La collecte et le traitement des données relatives aux déplacements des personnes, sous la forme de la date, de l'heure et du lieu de la validation du titre de transport via une borne de contrôle en entrée ou sortie du réseau de transport, sont susceptibles de porter atteinte à la liberté d'aller et venir et au droit à la vie privée lorsque ces données sont associées à un élément permettant d'identifier la personne concernée, en l'occurrence le numéro de la carte.

Les traitements appliqués aux données relatives aux déplacements des personnes devraient donc être anonymisés, à l'exception de ce qui relève de la gestion de la lutte contre la fraude.

En toute hypothèse, il est hautement souhaitable que la possibilité de circuler de façon anonyme, au moyen d'un titre billettique ou non, soit maintenue.

Le nombre d'événements de validation enregistrés dans la carte, qui varie actuellement entre deux et six, devrait, à l'occasion du passage à la prochaine génération de carte, être limité à quatre.

La collecte de la photographie devant figurer sur le support du titre de transport doit être accompagnée de la possibilité, pour l'usager, de s'opposer à sa conservation, sous une forme numérique.

Sur la durée de conservation des données relatives aux déplacements des personnes dans le cadre de la lutte contre la fraude

Il paraît nécessaire de distinguer deux délais, selon qu'il s'agit de détecter la fraude dans l'ensemble des cartes utilisées ou, une fois qu'une fraude est détectée, d'en traiter les suites.

Les données relatives aux déplacements des personnes, sous la forme d'une indication de la date, de l'heure et du lieu, associées à un élément permettant d'identifier la personne à laquelle elles sont rattachées, tels un numéro de carte, ne devraient être conservées que le temps nécessaire à la détection de la fraude. Ce délai ne devrait pas excéder deux jours consécutifs y compris le délai de sauvegarde.

Suite à la détection d'une fraude, les données susmentionnées ne devraient être conservées que le temps de déterminer s'il s'agit d'une fraude avérée et dans un tel cas, le temps de l'instruction de l'affaire par les autorités judiciaires.

Sur l'information des personnes concernées

En application des articles 26 et 27 de la loi du 6 janvier 1978, toute personne peut s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement et doit être informée de ses droits d'accès et de rectification. En outre, l'article 10 de la directive 95-46 du 24 octobre 1995 dispose que les personnes dont les données à caractère personnel font l'objet du traitement doivent également être informées de l'identité du responsable du traitement ainsi que des finalités du traitement auquel les données sont destinées.

Dès lors, les personnes concernées par les traitements billettiques doivent être informées que des données relatives à leurs déplacements sont collectées, les finalités de traitements mis en œuvre doivent leur être précisées et la possibilité d'utiliser des titres de transports anonymes doit être portée à leur connaissance.

Les personnes concernées doivent également être informées des destinataires des données, notamment dans le cadre d'une intermodalité développée entre différents réseaux de transports.

Sur le droit d'accès et de rectification

Toute personne utilisant une carte nominative doit être clairement informée des modalités d'exercice du droit d'accès et obtenir toutes les informations la concernant, qu'elles se situent dans le système central ou au sein de la carte.

Le droit d'accès s'applique à l'ensemble des informations relatives à la personne, qu'il s'agisse d'informations collectées directement auprès des personnes concernées ou d'informations éventuellement collectées auprès de tiers.

Sur les formalités préalables à l'automatisation

En application des articles 15 et 16 de la loi du 6 janvier 1978, les traitements automatisés d'informations nominatives mis en œuvre par les entreprises de transports collectifs doivent préalablement faire l'objet d'une demande d'avis, en cas de délégation de service public ou d'une déclaration ordinaire dans les autres cas, auprès de la Commission nationale de l'informatique et des libertés, l'omission de ces formalités préalables étant passible des sanctions prévues à l'article 226-16 du Code pénal.

Sur les mesures de sécurité et de confidentialité

En application des articles 29 et 45 de la loi du 6 janvier 1978, les entreprises de transports collectifs ordonnant ou effectuant un traitement d'informations nominatives s'engagent, vis-à-vis des personnes concernées, à prendre toutes mesures utiles afin de préserver la sécurité et la confidentialité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

S'agissant des données enregistrées au sein même de la carte, qu'elle soit à puce ou magnétique, le responsable du traitement doit mettre en œuvre les moyens nécessaires afin de s'assurer que, en dehors des nécessités de contrôle du titre de transport, seul le titulaire de ce titre a accès à ces données.

Sur les dispositions particulières à prendre en cas de mise en œuvre d'un traitement mutualisé par plusieurs transporteurs relatif à la détection de la fraude et à la gestion des pertes ou vols des supports des titres de transport

Les personnes concernées doivent être informées au moment de la collecte des données de l'existence du traitement mis en œuvre, de sa finalité, des destinataires des données et de l'existence d'un droit d'accès et de rectification.

Les motifs d'inscription dans le fichier doivent être objectifs, clairs et prédéterminés.

Une gestion rigoureuse des habilitations et des contrôles d'accès (codes de six à huit caractères alphanumériques) afin de se prémunir contre les risques d'intrusion et de détournement, ainsi que la définition d'algorithmes de chiffrement avancés (norme SSL 128 bits) devraient être mis en place.

Ces mêmes recommandations s'appliquent à la mise en œuvre d'un traitement mutualisé d'incidents de paiement. Dans un tel cas, seules les créances présentant un caractère certain devraient faire l'objet d'une inscription et les cas de contestation sérieuse et étayée devraient suspendre l'inscription ou au minimum être signalés par un astérisque.

De même, l'inscription devrait être précédée par une notification préalable accompagnée d'un délai de régularisation permettant d'éviter l'inscription dans une telle base de données.

Délibération n° 03-044 du 7 octobre 2003 portant avis favorable à la mise en place par la société Cofiroute d'un dispositif expérimental de lecture et de reconnaissance automatisées de la plaque minéralogique permettant d'alerter les conducteurs de véhicule dépassant la vitesse maximale autorisée

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis, en application de l'article 15 de la loi du 6 janvier 1978, par la société Cofiroute, d'un projet d'acte réglementaire portant création d'un dispositif expérimental de lecture et de reconnaissance automatisées de la plaque minéralogique permettant d'alerter les conducteurs de véhicule dépassant la vitesse maximale autorisée ;

Vu la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 ;

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et le décret nº 78-774 du 17 juillet 1978 pris pour son application ;

Après avoir entendu Monsieur Guy Rosier, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La compagnie financière et industrielle des autoroutes (Cofiroute) a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis relative à une expérimentation permettant, par lecture et reconnaissance automatisées des plaques minéralogiques, le contrôle des vitesses moyennes des automobilistes circulant entre deux points kilométriques de l'autoroute A10 (entre Saint-Arnoult-en-Yvelines et Orléans).

Cette expérimentation, mise en œuvre pour une durée de six mois, repose sur six caméras reliées à deux ordinateurs placés en bord de voie et mis en relation par un réseau privé de fibre optique et un logiciel de reconnaissance de caractère. Les trois premières caméras, installées au-dessus des voies de circulation au premier point kilométrique (le site « amont »), captent les numéros de plaque minéralogique de l'ensemble des véhicules circulant sur l'autoroute et passant dans leur champ. Le logiciel de reconnaissance de caractères identifie les numéros de plaque minéralogique et associe cette identification à un « horodatage ». Lorsque les véhicules passent dans le champ des trois autres caméras installées au deuxième point kilométrique (le site « aval » situé à 10 km) et si leur plaque est reconnue, leur vitesse moyenne est calculée.

En cas de dépassement de la vitesse maximale autorisée, le numéro de plaque minéralogique du contrevenant, accompagné d'un message de prudence, s'affiche en clair sur un panneau à message variable.

Les images captées par les caméras sont uniquement transmises au site « aval » pour permettre le calcul de la vitesse moyenne des véhicules, ces informa-

tions, une fois ce calcul effectué, n'étant ni conservées au-delà du temps nécessaire au calcul de la vitesse des véhicules ni retransmises. Le déclarant conserve toutefois dans sa base les deux derniers caractères des plaques minéralogiques captées, qu'il s'agisse de véhicules français ou étrangers, afin de pouvoir effectuer des études statistiques.

Les automobilistes sont informés de la mise en œuvre de ce dispositif par un panneau situé 500 m avant les trois caméras du site « amont » et indiquant : *« Pour votre sécurité, vitesse contrôlée par caméra »*.

Le dispositif a ainsi pour objet de sensibiliser les automobilistes sur leur vitesse moyenne, dans un but pédagogique et d'autorégulation.

La Commission considère que la liberté d'aller et venir et le droit à la vie privée supposent que les personnes puissent notamment se déplacer de manière anonyme ; que tel ne serait plus le cas si les sociétés d'autoroutes collectaient et traitaient systématiquement la totalité des numéros de plaques d'immatriculation des véhicules empruntant leur réseau.

Elle prend acte qu'en l'espèce ni les numéros de plaques minéralogiques ni les autres informations enregistrées (date et heure de passage, vitesse) ne sont conservés au-delà du temps nécessaire au calcul de la vitesse des véhicules et ne sont retransmis à des tiers.

Elle considère en conséquence que le dispositif mis en place par la société Cofiroute peut être admis à titre expérimental dès lors que cette société s'engage à prendre toutes dispositions pour informer clairement les usagers, avant qu'ils n'entrent sur le tronçon de l'A 10 concerné, des modalités de déroulement de cette opération et de son caractère expérimental par la remise de dépliants explicatifs aux gares de péage et par la diffusion d'une annonce sur la radio locale de l'autoroute.

Émet un avis favorable à la mise en œuvre par la société Cofiroute, à titre expérimental, d'un dispositif de lecture et de reconnaissance automatisées de la plaque minéralogique sous réserve que la société Cofiroute prenne toutes dispositions pour informer clairement les usagers, avant qu'ils n'entrent sur le tronçon de l'A 10 concerné, des modalités de déroulement de cette opération et de son caractère expérimental par la remise de dépliants explicatifs aux gares de péage et par la diffusion d'une annonce sur la radio locale de l'autoroute.

Demande à être rendue destinataire d'un bilan de cette expérimentation et notamment des enseignements qu'en tirera Cofiroute tout particulièrement quant au comportement des automobilistes et à la pérennisation, voire à l'extension de ce dispositif à d'autres points de l'autoroute A 10.

Travail et emploi

Délibération n° 03-031 du 5 juin 2003 portant avis sur la mise en œuvre, par l'Agence nationale pour l'emploi, d'un traitement automatisé d'informations indirectement nominatives dénommé « système d'information d'aide à la décision » (SIAD)

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par l'Agence nationale pour l'emploi, en application de l'article 15 de la loi du 6 janvier 1978 d'un projet de délibération du conseil d'administration de l'ANPE portant création d'un traitement automatisé d'informations nominatives dénommé « système d'information d'aide à la décision » ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil en date du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et le décret nº 78-774 du 17 juillet 1978 pris pour son application ;

Après avoir entendu Monsieur Hubert Bouchet, commissaire en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Le « système d'information d'aide à la décision » (SIAD) a pour objet de mettre à la disposition des responsables de l'ANPE des indicateurs statistiques permettant d'une part d'avoir une meilleure connaissance des demandeurs d'emploi et d'autre part, d'évaluer et d'orienter les actions menées auprès des demandeurs d'emploi dans le cadre en particulier du suivi de la mise en œuvre du projet d'action personnalisé (PAP).

Ce traitement repose sur la création d'une base de données nationale à partir des informations extraites d'applications exploitées par l'ANPE, notamment : les applications de gestion de la demande d'emploi, des prestations et des mesures pour l'emploi, et du rapprochement de l'offre et de la demande d'emploi.

Ce système d'information est consultable par les responsables de l'ANPE (direction générale, directions régionales, directions déléguées et directeurs des agences locales).

Les informations contenues dans le traitement sont accessibles sous forme de restitutions statistiques agrégées et anonymes.

Le système donne toutefois la possibilité, au travers de certaines fonctionnalités et dans une optique d'éclairage des résultats statistiques, de procéder à des tris et des recherches croisées sur certains critères aboutissant à des restitutions sous forme de tableaux comportant des données individuelles par demandeur d'emploi.

La Commission relève que les informations relatives aux demandeurs d'emploi enregistrées dans le traitement SIAD sont les suivantes : date de naissance,

tranche d'âge, sexe, nationalité, adresse (canton, commune, code postal ou cedex) ; numéros de référence : numéro identifiant Assedic, numéro de prise en charge par l'Assedic ; situation familiale ; bénéficiaire du RMI (oui/non) ; moyen de locomotion et permis de conduire ; catégorie de travailleur handicapé Cotorep (1, 2 ou 3) ; caractéristiques de la formation : niveau de formation et de la qualification ; vie professionnelle : inscription, indemnisation, emploi recherché, expérience professionnelle, entretiens proposés ou réalisés, mises en relation effectuées, mesures obtenues, prestations réalisées.

Les données ainsi traitées apparaissent pertinentes au regard des finalités statistiques poursuivies.

La Commission relève que, pour assurer l'anonymat, les numéros identifiants et la date de naissance seront occultés lors de la consultation des données.

La Commission prend acte de ce que l'ANPE s'engage à réaliser dans un délai d'un an, le transcodage, par l'application d'un algorithme dit de « hachage », des numéros identifiants.

La Commission prend également acte de ce que l'ANPE s'engage en outre, dans un délai d'un an, à mettre en place un dispositif de journalisation des requêtes.

Émet un avis favorable au projet de délibération du conseil d'administration de l'ANPE portant création d'un traitement automatisé d'informations nominatives dénommé « système d'information d'aide à la décision ».

Demande a être saisie dans un délai d'un an des modalités de mise en œuvre des mesures techniques complémentaires de sécurisation et d'anonymisation du traitement ainsi que du descriptif complet des données individuelles susceptibles d'être ajoutées à l'application quand le caractère anonyme de celle-ci aura été renforcé.

Délibération n° 03-047 du 23 octobre 2003 portant avertissement à l'Union fédérale autonome pénitentiaire

La Commission nationale de l'informatique et des libertés ;

Saisie de réclamations relatives à la diffusion sur internet de la liste des propositions de titularisations, promotions ou mutations des surveillants de l'administration pénitentiaire examinées lors des commissions administratives paritaires ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 modifié ;

Vu le décret n° 82-451 du 28 mai 1982 relatif aux commissions administratives paritaires ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 87-25 du 10 février 1987 fixant le règlement intérieur de la CNIL, et notamment son article 54 ;

Vu le courrier adressé par la CNIL à l'UFAP le 19 septembre 2003, et les observations reçues en réponse ;

Après avoir entendu Monsieur Patrick Delnatte, commissaire, en son rapport, et Madame Charlotte Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le 25 octobre 2001, la CNIL a été saisie d'une plainte relative à la diffusion, sur le site internet de l'Union fédérale autonome pénitentiaire (UFAP) – syndicat de personnels de l'administration pénitentiaire – des propositions de titularisations, promotions ou mutations des surveillants de l'administration pénitentiaire examinées lors de la commission administrative paritaire d'octobre 2001.

Il ressort du décret n° 82-451 du 28 mai 1982 relatif aux commissions administratives paritaires que *« les séances des commissions administratives paritaires ne sont pas publiques »* et que *« les membres des commissions administratives sont soumis à l'obligation de discrétion professionnelle en ce qui concerne tous les faits et documents dont ils ont eu connaissance en cette qualité »*.

Dès lors, les propositions de titularisations, promotions ou mutations des surveillants de l'administration pénitentiaire examinées lors des commissions administratives paritaires ne peuvent être régulièrement diffusées au public sur internet par une organisation syndicale.

Sur demande de la CNIL, l'UFAP a effectué, le 19 mars 2002, conformément aux dispositions de l'article 16 de la loi du 6 janvier 1978, la déclaration de son site internet et s'est engagée à ménager un accès restreint aux résultats des commissions administratives paritaires mises en ligne sur son site, l'accès à ces informations étant réservé aux seuls membres de l'administration pénitentiaire adhérents de l'UFAP, après communication d'un mot de passe.

La CNIL, estimant que cette diffusion en accès restreint n'appelait pas d'observation au regard des dispositions de la loi du 6 janvier 1978, a procédé à la clôture de la plainte le 7 août 2002.

Le 27 mars 2003, la CNIL a été à nouveau saisie de faits similaires, concernant la diffusion de nouveaux résultats de commissions administratives paritaires, sur le site internet d'une association.

L'instruction de cette nouvelle réclamation a permis d'établir que les responsables de ce site internet avaient pu se procurer les listes en cause, sur le site internet de l'UFAP, puis les avaient diffusées sur son propre site.

Les informations mises en ligne par l'UFAP sur son site internet, auxquelles l'accès aurait dû être restreint comme cette organisation syndicale l'avait indiqué dans la déclaration de son site internet, étaient, techniquement, librement accessibles sur internet, grâce notamment aux moteurs de recherche.

L'UFAP, saisie par la CNIL sur ce point, a indiqué, dans un courrier du 8 juillet 2003, qu'elle suspendait la diffusion des résultats des commissions administrative paritaires et a proposé la mise en place de nouvelles mesures techniques relatives à l'accès restreint à ces documents.

Les nouvelles propositions de l'UFAP ne permettant pas de garantir la confidentialité des informations mises en ligne et mettant en évidence une méconnaissance du fonctionnement d'internet et des moteurs de recherche, la CNIL a, le 19 septembre 2003, adressé un courrier à cette organisation lui demandant de faire valoir ses observations sur ce dossier, la Commission envisageant de faire application de l'article 21-4° de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'UFAP a indiqué en réponse renoncer à la diffusion sur son site internet des résultats des commissions administratives paritaires.

Il ressort de l'instruction de cette plainte par la CNIL que la mise en ligne des résultats de commissions administratives paritaires effectuée par l'UFAP sur son site internet, initialement en accès libre, puis en accès restreint mais sans que des précautions suffisantes aient été prises, a eu pour effet de porter à la connaissance du public des informations nominatives concernant les propositions de titularisations, promotions ou mutations des surveillants de l'administration pénitentiaire examinées lors des commissions administratives paritaires.

Or, l'article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que le maître du traitement s'engage *« vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés »*.

Le non-respect de ces dispositions est puni par l'article 226-17 du Code pénal de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Les informations nominatives en cause sont par ailleurs issues d'un traitement automatisé ayant fait l'objet d'une déclaration auprès de la CNIL par la direction de l'administration pénitentiaire du ministère de la Justice.

Cette déclaration, effectuée en application de l'article 17 de la loi du 6 janvier 1978, par référence à la norme simplifiée n° 37 (délibération de la CNIL n° 93-021 du 2 mars 1993), relative à la gestion des personnels de l'État, concerne un traitement ayant la finalité suivante « Système de gestion automatisée et de préparation des commissions administratives paritaires ».

La norme simplifiée n° 37, à laquelle la déclaration fait référence, prévoit que peuvent seuls être destinataires éventuels des informations enregistrées, les agents chargés des opérations administratives et comptables concernant les intéressés, les agents responsables de la gestion des personnels en cause et les membres

des commissions administratives et techniques, les supérieurs hiérarchiques des intéressés et les membres des services d'inspection.

L'UFAP, en tant qu'organisation syndicale, est membre des commissions administratives paritaires, et a, à ce seul titre, eu connaissance des propositions de mutations.

Cette organisation syndicale ne pouvait pas en faire un quelconque autre usage, sans encourir les sanctions prévues l'article 226-21 du Code pénal qui incrimine le fait de *« par toute personne détentrice d'informations nominatives à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par* [...] *les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende »*.

Si les faits imputables à l'UFAP paraissent susceptibles de constituer les infractions prévues par les articles 226-17 et 226-21 du Code pénal, il ressort de deux arrêts du Conseil d'État en date du 27 octobre 1999 et du 30 juillet 2003 que la CNIL conserve la possibilité, même lorsqu'elle estime qu'une infraction est constituée, d'apprécier si les faits dont elle a connaissance lui paraissent suffisamment établis et s'ils portent une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'application.

Or, les éléments recueillis au cours de l'instruction de ce dossier montrent que l'UFAP a bien eu l'intention de prendre les mesures de sécurité requises, mais qu'à la suite d'une méconnaissance technique d'internet, ces mesures n'ont pas été efficaces. Les termes des courriers adressés par l'UFAP à la CNIL attestent d'une telle méconnaissance.

L'UFAP indique en outre suspendre toute diffusion des résultats des commissions administratives paritaires.

Dans ces conditions, un avertissement à l'Union fédérale autonome pénitentiaire est la mesure appropriée.

Décide, faisant application des dispositions de l'article 21.4° de la loi du 6 janvier 1978, d'adresser à cet effet **un avertissement** à l'Union fédérale autonome pénitentiaire, dont le siège est situé 85 route de Grigny à Ris-Orangis (91130).

Vote électronique

Délibération n° 03-019 du 24 avril 2003 relative aux projets de décret et d'un projet d'arrêté, présentés par le ministère des Affaires étrangères, relatifs au vote par correspondance électronique des électeurs inscrits dans les circonscriptions des États-Unis d'Amérique pour les élections au Conseil supérieur des Français de l'étranger le 1er juin 2003

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère des Affaires étrangères le 18 avril 2003 d'un projet de décret et d'un projet d'arrêté relatifs au vote par correspondance électronique des électeurs inscrits dans les circonscriptions des États-Unis d'Amérique pour les élections au Conseil supérieur des Français de l'étranger le 1er juin 2003 ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive n° 95/46/CE du Parlement européen et du Conseil de l'Union européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 82-471 du 7 juin 1982 relative au Conseil supérieur des Français de l'étranger, modifiée par la loi n° 2003-277 du 28 mars 2003 tendant à autoriser le vote par correspondance électronique des Français établis hors de France pour les élections du Conseil supérieur des Français de l'étranger ;

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère des Affaires étrangères souhaite mettre en place un dispositif de vote électronique par internet qui permettrait aux Français établis aux États-Unis de participer à la désignation de leurs représentants au Conseil supérieur des Français de l'étranger.

Cette application est mise en œuvre par un prestataire technique sur des serveurs situés aux États-Unis.

Le projet repose sur le dispositif suivant :

Le vote par internet se déroulera du 19 mai à 12 heures, heure locale jusqu'au 31 mai à 12 heures, heure locale. Les urnes virtuelles ne seront accessibles par les électeurs qu'à partir de l'heure d'ouverture de l'endroit où se trouve le consulat dont ils dépendent. L'électeur ne pourra accéder qu'au bureau de vote virtuel correspondant à sa circonscription.

L'électeur se connectera au site de vote en mode sécurisé (protocole SSL qui assure le chiffrement des envois). Il entrera son identifiant et son mot de passe qui, transmis au serveur de vote, permettront de vérifier si l'électeur n'a pas déjà voté. Les listes de candidats seront alors présentées à l'écran sous leur titre dans l'ordre d'ins-

cription sur les listes de candidatures auprès de leurs circonscriptions respectives (deux en l'espèce) ainsi que la possibilité de voter blanc. En cliquant sur le nom de la liste, l'électeur verra apparaître à l'écran un fac-similé du bulletin de vote avec les noms des candidats de la liste. Il choisira la liste pour laquelle il vote (ou choisira de voter blanc) et validera son choix en cliquant sur le bouton correspondant. Cette opération déclenchera l'envoi du bulletin de vote virtuel vers le serveur. Une fois qu'il aura validé son vote, l'électeur visualisera un écran lui confirmant la prise en compte de son vote. À réception par le serveur, ce bulletin fera l'objet d'un chiffrement et sera stocké dans un « fichier des votes » séparé du « fichier des électeurs, selon les termes du décret et de l'arrêté soumis à l'avis de la CNIL.

À l'ouverture du scrutin sur place le 1er juin, une liste papier des personnes ayant voté par internet sera fournie à chaque bureau de vote afin que la mention « VCE » (vote par correspondance électronique) soit reportée manuellement par le président du bureau de vote ou son assesseur sur la liste générale. Pour le dépouillement des votes, chaque consul responsable d'un bureau de vote recevra deux plis du prestataire technique, chacun contenant un des deux codes (clés) nécessaires au déverrouillage de l'urne électronique. Le consul ne remettra ces clés aux assesseurs qu'à la fin du scrutin (en toute hypothèse, elles ne seront pas utilisables avant l'heure de fin du scrutin). Ces clés seront ensuite saisies sur un PC relié par internet au serveur de vote et permettront ainsi le déchiffrement des votes, leur comptabilisation et l'affichage des résultats. Ils seront imprimés et ajoutés aux votes papier.

Les fichiers supports seront conservés pendant un mois par le maître d'œuvre sous le contrôle des commissions électorales dans des conditions garantissant le secret du vote. Ils pourront, le cas échéant, être transférés au chef de poste consulaire. Sauf action contentieuse née avant l'épuisement des délais de recours, il est procédé à la destruction de ces supports sous le contrôle de la commission électorale locale.

La Commission constate que le législateur a autorisé, par la loi du 29 mars 2003 susvisée, le vote par correspondance électronique des Français établis hors de France pour les élections au Conseil supérieur des Français de l'étranger et a marqué sa volonté, ainsi que cela ressort des travaux parlementaires préparatoires de cette loi, d'expérimenter cette modalité de vote à l'occasion des élections pour le renouvellement partiel du Conseil dans les circonscriptions électorales des États-Unis le 1er juin 2003.

Elle prend acte des modalités d'organisation du dispositif de vote par correspondance électronique qui ont été retenues par le ministère des Affaires étrangères et qui, compte tenu de la brièveté des délais, ont d'ores et déjà commencé à être mises en œuvre par lui et par le prestataire technique qu'il a choisi. À cet égard, elle regrette que ces modalités d'organisation n'aient pas pu faire l'objet d'une instruction plus approfondie par le ministère des Affaires étrangères.

La Commission considère que le recours à des dispositifs de vote électronique doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle *a posteriori* par le juge de l'élection peuvent assurer. Bien qu'elle ne puisse avoir la certitude que ces principes sont en l'espèce garantis, elle estime néanmoins ne pas pouvoir, en raison des conditions dans lesquelles cette expérimentation a été décidée et organisée, émettre un avis défavorable aux projets de décret et d'arrêté qui lui sont soumis mais se doit de formuler des recommandations au sujet du déroulement des opérations électorales.

La mise en œuvre du dispositif expérimenté dans la circonscription des États-Unis d'Amérique lors des élections du 1er juin 2003 devrait respecter les conditions suivantes :

1) Le fichier des électeurs comportant les identifiants et les mots de passe des électeurs devrait faire l'objet d'un chiffrement et la procédure d'impression de ces codes personnels sur les courriers envoyés aux électeurs devrait être conçue de façon à ce que l'imprimeur ne puisse accéder en clair à ces codes.

2) La procédure prévue pour adresser à l'électeur ses codes personnels d'accès ne devrait pas se limiter à l'envoi d'un simple courrier où figurent ces informations, certes masquées, dans la mesure où une telle procédure comporte le risque qu'un tiers puisse ainsi en disposer et voter à la place de l'électeur. Or, dans cette hypothèse, l'électeur ne disposerait plus de la possibilité de voter par des moyens traditionnels puisqu'il est techniquement impossible d'annuler le bulletin émis par correspondance électronique, celui-ci ne pouvant être retiré et décompté du fichier des votes électroniques.

En conséquence, pour limiter ce risque, l'envoi des codes d'accès à l'électeur devrait s'effectuer sous pli recommandé avec accusé de réception ou, mieux, l'électeur devrait pouvoir bénéficier d'un dispositif d'authentification certifié, ces procédures étant de nature à constituer un commencement de preuve en cas de contestation du vote d'un électeur.

3) Devrait être prévue la possibilité dans chaque bureau de vote de consigner les réclamations des électeurs n'ayant pu voter par internet ou contestant un vote émis en leur nom par internet.

4) La mise en œuvre de ce dispositif de vote électronique devrait être assurée sous le contrôle effectif soit des représentants du ministère des Affaires étrangères soit d'experts désignés par lui et toutes mesures devraient être prises pour leur permettre de vérifier l'effectivité des dispositifs de sécurité prévus pour assurer le secret du vote, et en particulier les mesures prises respectivement, pour garantir la confidentialité du fichier des électeurs comportant les identifiants et les codes d'accès des électeurs, procéder au chiffrement des bulletins de vote et à leur conservation dans un traitement distinct de celui mis en œuvre pour assurer la tenue du fichier des électeurs, assurer la conservation des différents supports d'information pendant et après le déroulement du scrutin.

5) Toutes les facilités devraient être accordées aux scrutateurs, s'ils le souhaitent, pour pouvoir contrôler le bon déroulement du vote par correspondance électronique.

La Commission **considère** que ces recommandations énoncées dans le cadre d'une expérimentation à caractère limité ne préjugent pas d'autres recommandations qu'elle serait amenée à formuler lors de l'extension à l'ensemble des circonscriptions électorales du Conseil supérieur des Français de l'étranger, en application de la loi du 29 mars 2003. À cet égard elle **demande** à être saisie des textes réglementaires qui seraient pris pour réaliser une telle extension.

Afin de se préparer à cette consultation, la Commission **demande** qu'un bilan technique de la mise en œuvre du dispositif de vote électronique utilisé dans la circonscription des États-Unis soit établi à brève échéance suivant le déroulement de l'élection et lui soit adressé. Elle **recommande** que le système développé par le prestataire technique choisi par le ministère des affaires étrangères fasse l'objet d'une expertise menée par la direction centrale des sécurités des systèmes d'information (DCSSI) et demande que le rapport d'expertise lui soit communiqué.

Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

La Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pris ensemble le décret d'application nº 78-774 du 17 juillet 1978 ;

Vu le Code électoral ;

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Commission constate le développement de systèmes de vote électronique sur place ou à distance tendant à faciliter l'expression du vote et les opérations matérielles de dépouillement.

Le recours à de tels systèmes qui nécessitent la mise en œuvre de traitements automatisés d'informations nominatives, au sens de l'article 5 de la loi du 6 janvier 1978, pour le fichier informatique des électeurs, le traitement automatisé des résultats (pour les données nominatives relatives aux candidats) ou la constitution de la liste d'émargement doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle *a posteriori* par le juge de l'élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

La présente recommandation porte sur les conditions techniques propres à garantir les principes fondamentaux préalablement énumérés et à assurer la sécurité des systèmes de vote électronique. Il appartient au législateur de définir les conditions juridiques de la mise en œuvre du vote électronique.

Elle a pour champ d'application les dispositifs de vote électronique sur place et à distance, en particulier par internet. Elle ne concerne pas les dispositifs de vote par codes-barres et les dispositifs de vote par téléphone fixe ou mobile sur lesquels la Commission sera amenée à se prononcer.

La recommandation prend appui essentiellement sur les dossiers qui ont été soumis à la Commission dans le cadre des formalités préalables prévues par la loi du 6 janvier 1978. Elle constitue une première approche de systèmes qui sont encore en pleine évolution. Elle est destinée à orienter cette évolution dans le sens du respect des principes de protection des données personnelles et à éclairer les responsables des scrutins pour le choix des dispositifs de vote électronique.

Compte tenu de ces observations préalables, la Commission émet les recommandations suivantes :

Sur les exigences préalables à la mise en œuvre des systèmes de vote électronique

L'expertise du système de vote électronique

Tout système de vote électronique devrait faire l'objet :
– d'une procédure d'agrément par le ministère de l'intérieur pour les machines à voter définies par le code électoral ;
– d'une expertise indépendante pour les autres systèmes.

Le rapport d'expertise devra être joint aux formalités préalables à accomplir auprès de la CNIL.

La Commission estime que dans le cas d'une élection organisée par une collectivité publique, le code source des logiciels utilisés par le système de vote électronique devrait être accessible sans restriction, afin de permettre la réalisation de toutes les expertises jugées nécessaires.

Dans l'hypothèse de l'utilisation d'un logiciel libre, quelle que soit la personne mettant en œuvre le traitement, ce logiciel doit être expertisé.

Afin de garantir un contrôle effectif des opérations électorales, le prestataire technique doit mettre à disposition des représentants de l'organisme responsable du traitement, des experts, des membres du bureau de vote, des délégués des candidats et des scrutateurs tous documents utiles et assurer une formation de ces personnes au fonctionnement du dispositif de vote électronique.

La séparation des données nominatives des électeurs et des votes

Le secret du vote doit être garanti par la mise en œuvre de procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote. Il en résulte que la gestion du fichier des votes et celle de la liste d'émargement doivent être faites sur des systèmes informatiques distincts, dédiés et isolés. Ces fichiers doivent faire l'objet de mesures de chiffrement selon un algorithme public réputé « fort ».

Les sécurités informatiques

Il convient que toutes les mesures physiques (contrôle d'accès, détermination précise des personnes habilitées à intervenir…) et logiques (*firewall*, protection d'accès aux applicatifs…) soient prises tant au niveau des serveurs du dispositif que sur les postes accessibles au public afin de garantir la sécurité et la confidentialité des données personnelles en particulier contre les intrusions venant de l'extérieur. Les algorithmes de chiffrement, de signature électronique et les fonctions de hachage doivent être des algorithmes publics réputés « forts ».

Le scellement du dispositif de vote électronique

Les systèmes de vote électronique expertisés et utilisés doivent faire l'objet d'un scellement c'est-à-dire d'un procédé permettant de déceler toute modification de ce système. Le procédé de scellement doit lui-même être agréé. La vérification du scellement devrait pouvoir se faire à tout moment, y compris durant le déroulement du scrutin et par tout électeur.

L'existence d'une solution de secours

Tout système de vote électronique devrait comporter un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques.

La surveillance effective du scrutin

La mise en œuvre du système de vote électronique doit être opérée sous le contrôle effectif, tant au niveau des moyens informatiques centraux que de ceux, éventuellement, déployés sur place, de représentants de l'organisme mettant en place le vote ou d'experts désignés par lui. Dès lors, il importe que toutes les mesures soient prises pour leur permettre de vérifier l'effectivité des dispositifs de sécurité prévus pour assurer le secret du vote et, en particulier, les mesures prises respectivement pour :
– garantir la confidentialité du fichier des électeurs comportant les éléments d'authentification ;
– procéder au chiffrement des bulletins de vote et à leur conservation dans un traitement distinct de celui mis en œuvre pour assurer la tenue du fichier des électeurs ;
– assurer la conservation des différents supports d'information pendant et après le déroulement du scrutin.

Toutes les facilités devraient être accordées aux membres du bureau de vote et aux délégués des candidats, s'ils le souhaitent, pour pouvoir assurer une surveillance effective de l'ensemble des opérations électorales et, en particulier, de la préparation du scrutin, du vote, de l'émargement et du dépouillement.

La localisation du système informatique central

Il paraît hautement souhaitable que les serveurs et les autres moyens informatiques centraux du système de vote électronique soient localisés sur le territoire national afin de permettre un contrôle effectif de ces opérations par les membres du bureau de vote et les délégués ainsi que l'intervention, le cas échéant, des autorités nationales compétentes.

Sur le scrutin

Sur les opérations précédant l'ouverture du scrutin

. La confidentialité des données

Les fichiers nominatifs des électeurs constitués aux fins d'établir la liste électorale, d'adresser le matériel de vote et de réaliser les émargements ne peuvent être utilisés qu'aux fins précitées et ne peuvent être divulgués sous peine des sanctions pénales encourues au titre des articles 226-17 et 226-21 du Code pénal.

La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance du système informatique.

Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement/déchiffrement et le contenu de l'urne ne doivent pas être accessibles, de même que la liste d'émargement, sauf aux fins de contrôle de l'effectivité de l'émargement des électeurs.

En cas de recours à un prestataire extérieur, celui-ci doit s'engager contractuellement à respecter ces dispositions par la signature d'une clause de confidentialité et de sécurité et à fournir le descriptif détaillé du dispositif technique mis en œuvre pour assurer cette confidentialité. Le prestataire doit également s'engager à restituer

les fichiers restant en sa possession à l'issue des opérations électorales et à détruire toutes les copies totales ou partielles qu'il aurait été amené à effectuer sur quelque support que ce soit.

Le recours à une télémaintenance des matériels et logiciels ne devrait pas être possible durant tout le scrutin et jusqu'à l'épuisement des délais légaux de recours contentieux.

. Les procédés d'authentification de l'électeur

La Commission estime que dans le cas d'élections où un vote à distance a été prévu par le législateur, une authentification de l'électeur sur la base d'un certificat électronique constitue la solution la plus satisfaisante en l'état de la technique. Le tiers certificateur doit être un organisme indépendant professionnellement reconnu.

Dans l'état actuel des textes, le recours à l'enregistrement de données biométriques à des fins de constitution d'un fichier électoral pour s'assurer de l'identité de l'électeur et de l'unicité de son vote ne peut s'envisager que si la donnée biométrique figure dans la catégorie de celles ne laissant pas de traces ou que si cet enregistrement s'effectue sur un support individuel détenu par l'électeur et ne donne pas lieu à la constitution d'un fichier de données biométriques.

À défaut de recourir aux solutions précitées, dans le cas de la génération d'identifiants et de mots de passe à partir de la liste électorale, le fichier ainsi créé doit faire l'objet d'un chiffrement. Les modalités de génération et d'envoi des codes personnels doivent être conçues de façon à garantir leur confidentialité et en particulier que les divers prestataires éventuels ne puissent en prendre connaissance.

Dans le cas où le vote s'opérerait par l'enregistrement d'un identifiant permanent apposé sur une carte ou tout autre document ainsi qu'un mot de passe envoyé à chaque vote, la génération de ces identifiants et mots de passe devrait se faire dans les mêmes conditions de sécurité que celles énumérées ci-dessus. Il en va de même de l'envoi du mot de passe.

L'authentification de l'électeur peut être renforcée par un dispositif de type défi/réponse, c'est-à-dire l'envoi par le serveur d'authentification d'une question dont l'électeur devrait connaître la réponse.

. L'information des électeurs

Il convient de fournir aux électeurs en temps utile une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote électronique.

. Le test du système avant l'ouverture du scrutin

Un test du système de vote électronique doit être organisé avant l'ouverture du scrutin et en présence des scrutateurs afin de constater la présence du scellement, le bon fonctionnement des machines, la remise à zéro du compteur des voix et que l'urne électronique destinée à recevoir les votes est bien vide et scellée.

. Les clés de dépouillement de vote

La génération des clés destinées à permettre le dépouillement des votes à l'issue du scrutin doit être publique et se dérouler le jour du dépouillement. Cette procédure devrait être conçue de manière à prouver de façon irréfutable que seuls le président du bureau et ses assesseurs prennent connaissance de ces clés, à l'exclusion de toute autre personne y compris les personnels techniques chargés du déploie-

ment du système de vote. La Commission estime que le nombre de clés de chiffrement doit être au minimum de trois, la présence de deux titulaires de ces clés étant indispensable pour autoriser le dépouillement. Elle considère que les clés doivent ensuite être conservées sous pli scellé sous la responsabilité du président du bureau de vote qui les remet, lors de la clôture du scrutin, aux membres du bureau désignés, contre accusé de réception.

Le système de vote doit garantir que des résultats partiels (hormis le nombre de votants) ne seront pas accessibles durant le déroulement du vote.

Sur le déroulement du vote

Le vote

Les heures d'ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Pour se connecter à distance ou sur place au système de vote, l'électeur doit se faire reconnaître par un dispositif d'authentification établi conformément à la présente recommandation, permettant au serveur de vérifier son identité et s'il n'a pas déjà voté.

L'électeur accède aux listes ou aux candidats officiellement retenus et dans l'ordre officiel. Le vote blanc doit être prévu lorsque la loi l'autorise.

L'électeur doit pouvoir choisir une liste, un candidat ou un vote blanc de façon à ce que ce choix apparaisse clairement à l'écran indépendamment de toute autre information. Il devrait avoir la possibilité de revenir sur ce choix.

Il valide ensuite son choix et cette opération déclenche l'envoi du bulletin de vote dématérialisé vers le serveur des votes.

L'électeur devrait recevoir immédiatement confirmation de son vote et avoir la possibilité de conserver une trace de cette confirmation.

Le chiffrement du bulletin de vote

Le bulletin de vote doit être chiffré par un algorithme public réputé « fort » dès son émission sur la machine à voter ou le terminal d'accès à distance et être stocké sur le serveur des votes sans que ce chiffrement n'ait été à aucun moment interrompu. La liaison entre le terminal de vote de l'électeur et le serveur des votes doit faire l'objet d'un chiffrement pour assurer la sécurité tant du procédé d'authentification de l'électeur que la confidentialité de son vote.

L'émargement

L'émargement doit se faire dès la validation du vote de façon à ce qu'un autre vote ne puisse intervenir à partir des éléments d'authentification de l'électeur déjà utilisés. L'émargement comporte un horodatage. La liste d'émargement doit être située sur un système distinct de celui contenant l'urne électronique. Cette liste, aux fins de contrôle de l'émargement, ainsi que le compteur des votes ne doivent être accessibles qu'aux membres du bureau de vote et aux personnes autorisées.

La liste d'émargement doit être enregistrée sur un support scellé, non réinscriptible, rendant ainsi son contenu inaltérable et probant.

Le dépouillement

Le dépouillement est actionné par les clés de déchiffrement, remises par le président du bureau de vote après la clôture des opérations de vote aux membres du bureau dûment désignés au moment de la génération de ces codes. Les membres du bureau doivent actionner publiquement le processus de dépouillement.

Les décomptes des voix par candidat ou liste de l'élection doivent apparaître lisiblement à l'écran et faire l'objet d'une édition sécurisée pour être portés au procès-verbal de l'élection. Le cas échéant, l'envoi des résultats à un bureau centralisateur à distance devrait s'effectuer selon une liaison sécurisée empêchant toute captation ou modification des résultats.

Le système de vote électronique doit être bloqué après le dépouillement de sorte qu'il soit impossible de reprendre ou de modifier les résultats après la décision de clôture du dépouillement prise par la commission électorale.

Sur le contrôle des opérations de vote *a posteriori* par le juge électoral

Les garanties minimales pour un contrôle a posteriori

Pour les besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote électronique doit être capable de fournir les éléments techniques permettant au minimum de prouver de façon irréfutable que :
– durant le scrutin le procédé de scellement est resté fiable ;
– les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls titulaires ;
– le vote est anonyme ;
– la liste d'émargement ne comprend que les électeurs ayant voté ;
– l'urne dépouillée est bien celle contenant les votes des électeurs et elle ne contient que ces votes ;
– aucun décompte partiel n'a pu être effectué durant le scrutin ;
– la procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau.

La conservation des données portant sur l'opération électorale

Tous les fichiers supports (copies des programmes sources et exécutables, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu'à l'épuisement des délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote. Obligation doit être faite, le cas échéant, au prestataire de service de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation des supports. Lorsqu'aucune action contentieuse n'a été engagée avant l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

Dans la phase d'expérimentation des systèmes de vote électronique, la CNIL demandera qu'un bilan de la mise en œuvre du dispositif de vote électronique utilisé soit établi à brève échéance suivant le déroulement de l'élection et lui soit adressé.

Délibération n° 03-049 du 20 novembre 2003 portant avis sur le projet de décret modifiant le décret n° 91-739 du 18 juillet 1991 relatif aux chambres de commerce et d'industrie, aux chambres régionales de commerce et d'industrie, à l'assemblée des chambres françaises de commerce et d'industrie et aux groupements interconsulaires

La Commission nationale de l'informatique et des libertés ;

Saisie par le secrétaire d'État aux petites et moyennes entreprises, au commerce et à l'artisanat, aux professions libérales et à la consommation d'un projet de décret en Conseil d'État modifiant le décret nº 91-739 du 18 juillet 1991 relatif aux chambres de commerce et d'industrie (CCI), aux chambres régionales de commerce et d'industrie, à l'assemblée des chambres françaises de commerce et d'industrie et aux groupements interconsulaires ;

Vu la directive nº 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu l'article 19 de la loi nº 2003-591 du 2 juillet 2003 habilitant le Gouvernement à simplifier le droit ;

Vu l'ordonnance nº 2003-1067 du 12 novembre 2003 relative à l'élection des membres des chambres de commerce et d'industrie, à la prorogation des mandats des délégués consulaires et modifiant le Code de commerce ;

Vu le Code pénal ;

Vu le Code de procédure pénale ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu la délibération nº 03-036 du 1er juillet 2003 de la Commission nationale de l'informatique et des libertés portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique ;

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Les modifications apportées au décret nº 91-739 du 18 juillet 1991 précité concernent tant l'organisation et le fonctionnement des CCI que les élections des membres des CCI. Le chapitre II est notamment consacré à l'élection des membres de chambres de commerce et d'industrie et porte sur l'établissement des listes électorales, les candidatures, les opérations électorales, le vote par correspondance, le vote par internet à distance et la proclamation des résultats.

Au-delà de la seule opération de vote par voie électronique, le processus de dématérialisation concerne les diverses phases de l'organisation des élections consulaires, qu'il s'agisse de la collecte des renseignements nécessaires à la constitution des listes électorales, la mise à disposition de la liste électorale par des voies déma-

rialisées, les modalités pratiques du vote lui-même, la gestion de la liste d'émargement et les opérations de dépouillement. Le décret renvoie à un arrêté, pris après avis de la CNIL, le soin d'apporter les précisions nécessaires sur les modalités de mise en œuvre de ces dispositions.

Le projet reprend les recommandations relatives à la sécurité des systèmes de vote électronique émises par la Commission nationale de l'informatique et des libertés. Ainsi, le projet de décret prévoit que :

– L'envoi aux ressortissants des CCI des questionnaires destinés au recensement des électeurs et leur retour (article 15-1 – alinéa 2) par voie électronique s'effectuera dans des conditions de sécurité et selon des modalités prévues par un arrêté du ministre chargé de la tutelle administrative des chambres de commerce et d'industrie qui sera pris après avis de la Commission nationale de l'informatique et des libertés.

– La mise à disposition par des voies dématérialisées de la liste électorale aux seuls électeurs (article 17 alinéa 2) sera assurée dans des conditions de sécurité assurant le respect du Code électoral, la mise en ligne n'étant pas limitée au seul réseau internet mais à tout réseau accessible aux électeurs.

– Le système de vote électronique fera l'objet d'une expertise préalablement à son utilisation (article 34).

– L'électeur disposera d'outils d'authentification garantissant la confidentialité et l'unicité du vote selon des exigences de sécurité et des modalités définies par un arrêté du ministre chargé de la tutelle administrative des chambres de commerce et d'industrie pris après avis de la Commission nationale de l'informatique et des libertés (article 29).

– L'électeur recevra confirmation de la prise en compte de son vote et de l'émargement (article 30).

– La sécurité et la confidentialité du contenu de l'urne électronique et du fichier des électeurs seront assurées par la mise en œuvre de traitements automatisés effectués sur des systèmes informatiques non seulement distincts mais également dédiés et isolés, ainsi que le chiffrement du contenu de l'urne électronique (article 31).

– L'état du scellement du système de vote devra pouvoir être contrôlé avant de procéder au dépouillement (article 32).

– Le contrôle *a posteriori* du juge est rendu possible dans la mesure où le système de vote électronique devra permettre de prouver, dans des conditions à définir par arrêté que :
– tous les votes ont été pris en compte ;
– le procédé de scellement est resté fiable durant le scrutin ;
– le vote est resté anonyme ;
– la liste d'émargement ne comprend que les électeurs ayant voté ;
– l'urne dépouillée est bien celle contenant les votes des électeurs et ne contient que ces votes ;
– aucun dépouillement partiel n'a pu être effectué durant le scrutin.

Prend acte de ce que le projet renvoie à un arrêté qui sera pris après avis de la CNIL le soin de déterminer les modalités pratiques de mise en œuvre de ces dispositifs de vote électronique, notamment les règles à respecter pour assurer la sécurité et la confidentialité des informations.

Souhaite que l'article 30 du projet de décret qui vise « l'authentification de l'électeur » soit clarifié pour faire apparaître la prise en compte par le système de vote des quatre étapes suivantes : identification du votant, expression du vote, confir-

mation des choix par les outils d'authentification et confirmation de l'inscription sécurisée du vote.

Émet un avis favorable au projet de décret modifiant le décret nº 91-739 du 18 juillet 1991.

ANNEXES

Composition de la CNIL

Composition de la Commission au 26 février 2004

Président : **Alex TÜRK**, sénateur du Nord

Vice-président délégué : **Hubert BOUCHET**, membre du Conseil économique et social

Vice-président : **Guy ROSIER**, conseiller-maître honoraire à la Cour des comptes

Membres :

François BERNARD, conseiller d'État honoraire

Jean-Marie COTTERET, professeur émérite des universités

Anne DEBET, professeur des universités

Emmanuel de GIVRY, conseiller à la Cour de cassation

Francis DELATTRE, député du Val-d'Oise

Patrick DELNATTE, député du Nord

Jean-Pierre de LONGEVIALLE, conseiller d'État

Isabelle FALQUE-PIERROTIN, conseiller d'État

Didier GASSE, conseiller-maître à la Cour des comptes

François GIQUEL, conseiller-maître à la Cour des comptes

Philippe LEMOINE, président-directeur général de Laser, membre du directoire des Galeries Lafayette

Philippe NOGRIX, sénateur de l'Ille-et-Vilaine

Bernard PEYRAT, conseiller à la Cour de cassation

Pierre SCHAPIRA, adjoint au maire de Paris, chargé des relations internationales, vice-président du Conseil économique et social

Commissaires du Gouvernement :
Charlotte-Marie PITRAT
Catherine POZZO DI BORGO, adjoint

Composition de la Commission au 31 décembre 2003

Président : **Michel GENTOT**, président de section au Conseil d'État

Vice-président délégué : **Hubert BOUCHET**, membre du Conseil économique et social

Vice-président : **Alex TÜRK**, sénateur du Nord

Commissaires :
Cécile ALVERGNAT, consultant et formatrice NTIC
Maurice BENASSAYAG, conseiller d'État

Francis DELATTRE, député du Val-d'Oise

Patrick DELNATTE, député du Nord

Didier GASSE, conseiller-maître à la Cour des comptes

François GIQUEL, conseiller-maître à la Cour des comptes

Pierre LECLERCQ, conseiller honoraire à la Cour de cassation

Philippe LEMOINE, président-directeur général de Laser, membre du directoire des Galeries Lafayette

Jean-Pierre de LONGEVIALLE, conseiller d'État honoraire

Philippe NOGRIX, sénateur de l'Ille-et-Vilaine

Marcel PINET, conseiller d'État honoraire

Guy ROSIER, conseiller-maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social, adjoint au maire de Paris, chargé des relations internationales

Maurice VIENNOIS, conseiller-doyen honoraire à la Cour de cassation

Commissaires du Gouvernement :
Charlotte-Marie PITRAT
Catherine POZZO DI BORGO, adjoint

Répartition des secteurs d'activité

La répartition des compétences au sein de la CNIL

Chacun des dix-sept membres de la CNIL, en dehors du président, est plus particulièrement chargé de suivre un secteur d'activité. La répartition des compétences est fixée par le président.

Finances publiques	Jean-Pierre de LONGEVIALLE
Collectivités locales — audiovisuel	Jean-Marie COTTERET
Libertés publiques	Isabelle FALQUE-PIERROTIN
Justice	Patrick DELNATTE
Sécurité	François GIQUEL
Affaires culturelles	Francis DELATTRE
Affaires sociales	Pierre SCHAPIRA
Santé	François BERNARD
Travail	Hubert BOUCHET
Commerce	Bernard PEYRAT
Gestion des risques et des droits	Emmanuel de GIVRY
Monnaie et crédit	Philippe NOGRIX
Télécommunications et réseaux	Didier GASSE
Affaires économiques	Guy ROSIER
International	Anne DEBET
Technologie	Philippe LEMOINE

Annexe 3

Organisation des services au 26 février 2004

Président : **Alex TÜRK**

Secrétaire général, chargé des affaires juridiques : **Christophe PALLEZ**

Le budget de la CNIL

Les crédits alloués à la CNIL au titre de la loi de finances initiale s'élevaient à 6 478 844 euros en 2003.

Budget	2003
Rémunération des personnels	3 828 156 euros
Vacations et autres rémunérations	550 366 euros
Fonctionnement	2 100 322 euros
Total	**6 478 844 euros**

Liste chronologique des délibérations adoptées par la CNIL en 2003

Les délibérations sont publiées dans la deuxième partie du rapport. Elles sont signalées dans le tableau suivant, par un renvoi à la page concordante.

Le texte intégral de l'ensemble des délibérations de la CNIL, depuis 1978, est accessible par internet sur le site http://www.legifrance.gouv.fr

Numéro Date	Objet
03-001 9 janvier 2003 (*cf.* p. 299)	Délibération portant avis conforme sur le projet de décret en Conseil d'État portant création du système d'information judiciaire « JUDEX » et faisant application à ce traitement des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978
03-002 21 janvier 2003 (*cf.* p. 364)	Délibération portant avis sur un projet de décret en Conseil d'État relatif à l'échantillon interrégimes de cotisants et à l'échantillon interrégimes de retraites et sur un projet d'arrêté relatif à l'échantillon interrégimes de cotisants
03-003 28 janvier 2003 (*cf.* p. 368)	Délibération portant avis sur la mise en œuvre, par l'INSEE, de la collecte des données lors du recensement des personnes résidants dans les communautés
03-004 28 janvier 2003 (*cf.* p. 370)	Délibération portant avis sur le traitement automatisé d'informations nominatives, constitué par l'INSEE, à partir des fichiers de la taxe d'habitation
03-005 28 janvier 2003 (*cf.* p. 372)	Délibération portant avis sur la mise en œuvre, par l'INSEE, d'une enquête cartographique dans les départements d'outre-mer
03-006 28 janvier 2003 (*cf.* p. 306)	Délibération portant avis sur le projet d'arrêté du maire de Roubaix portant création d'un traitement d'informations nominatives ayant pour objet de permettre la localisation et la cartographie des phénomènes de délinquance sur le territoire de la commune

Numéro Date	Objet
03-007 4 février 2003 (*cf.* p. 282)	Délibération portant avis sur le projet de décret en Conseil d'État, présenté par le ministère de la Santé, de la Famille et des Personnes handicapées, pris en application de l'article L. 147-11 du Code de l'action sociale et des familles et portant création d'un traitement automatisé d'informations nominatives pour la gestion des missions du Conseil national pour l'accès aux origines personnelles
03-008 27 février 2003 (*cf.* p. 377)	Délibération portant avis sur un traitement de la Régie autonome des transports parisiens ayant pour finalité l'exploitation des données de validation des passes Navigo
03-009 27 février 2003 (*cf.* p. 287)	Délibération concernant la mise en place par la direction générale des impôts d'un serveur professionnel des données cadastrales consultable par internet
03-010 11 mars 2003	Délibération décidant une mission de contrôle
03-011 11 mars 2003 (*cf.* p. 328)	Délibération portant avis sur le traitement automatisé d'informations nominatives mis en œuvre par La Poste relatif au fichier des nouveaux voisins
03-012 11 mars 2003 (*cf.* p. 381)	Délibération portant recommandation relative à la gestion de fichiers de personnes à risques par les loueurs de véhicules
03-013 27 mars 2003 (*cf.* p. 272)	Délibération portant avis sur le projet d'arrêté présenté par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche concernant la modification du traitement SISE
03-014	Numéro non utilisé
03-015 24 avril 2003 (*cf.* p. 278)	Délibération portant avis sur les articles 4 et 5 d'un projet de loi relatif à l'immigration
03-016 24 avril 2003 (*cf.* p. 309)	Délibération portant avis sur un projet du préfet de Haute-Savoie relatif à un traitement automatisé ayant pour finalité la constitution d'un fichier des personnes titulaires d'un badge permanent d'entrée dans le périmètre de protection du sommet des chefs d'État (G8)

Numéro Date	Objet
03-017 24 avril 2003 (*cf.* p. 330)	Délibération portant avis sur le projet de loi relatif aux communications électroniques
03-018 24 avril 2003 (*cf.* p. 237)	Délibération portant avertissement à Fortis Banque
03-019 24 avril 2003 (*cf.* p. 395)	Délibération relative aux projets de décret et d'un projet d'arrêté, présentés par le ministère des Affaires étrangères, relatifs au vote par correspondance électronique des électeurs inscrits dans les circonscriptions des États-Unis d'Amérique pour les élections au Conseil supérieur des Français de l'étranger le 1er juin 2003
03-020 29 avril 2003	Délibération décidant une mission de contrôle
03-021 29 avril 2003	Délibération décidant une mission de contrôle
03-022 29 avril 2003	Délibération décidant une mission de contrôle
03-023 29 avril 2003	Délibération décidant une mission de contrôle
03-024 29 avril 2003	Délibération décidant une mission de contrôle
03-024 bis 29 avril 2003	Délibération décidant une mission de contrôle
03-025 29 avril 2003	Délibération décidant une mission de contrôle
03-025 bis 29 avril 2003	Délibération décidant une mission de contrôle
03-026 29 avril 2003	Délibération décidant une mission de contrôle

Numéro Date	Objet
03-027 22 mai 2003 (*cf.* p. 251)	Délibération portant avis sur le projet d'arrêté du ministère de la Justice portant création d'une application informatique destinée à vérifier l'identité des détenus en établissement par reconnaissance de la morphologie de la main
03-028 27 mai 2003 (*cf.* p. 233)	Délibération portant avis sur le projet d'arrêté du ministre des Affaires étrangères modifiant l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires
03-029 22 mai 2003 (*cf.* p. 311)	Délibération concernant la création par la direction générale des douanes et droits indirects d'un système d'information de lutte contre la fraude
03-030 27 mai 2003 (*cf.* p. 265)	Délibération relative à la demande d'avis présentée par la communauté urbaine de Lyon concernant la constitution d'un traitement automatisé de données nominatives ayant pour finalité l'envoi d'informations aux Lyonnais habitant Paris et la région parisienne
03-031 5 juin 2003 (*cf.* p. 390)	Délibération portant avis sur la mise en œuvre par l'Agence nationale pour l'emploi d'un traitement automatisé d'informations indirectement nominatives dénommé « système d'information d'aide à la décision » (SIAD)
03-032 5 juin 2003 (*cf.* p. 253)	Délibération portant avis sur le projet d'arrêté du ministre de la Justice portant création dans certains établissements pénitentiaires d'un traitement automatisé de données nominatives ayant pour objet la gestion des personnes placées sous surveillance électronique
03-033 19 juin 2003 (*cf.* p. 240)	Délibération portant avertissement à la caisse régionale du Crédit agricole mutuel du Nord
03-034 19 juin 2003 (*cf.* p. 267)	Délibération portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance
03-035 1er juillet 2003	Délibération décidant une mission de contrôle

Numéro Date	Objet
03-036 1er juillet 2003 (*cf.* p. 398)	Délibération portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique
03-037 16 septembre 2003 (*cf.* p. 274)	Délibération relative à la demande d'avis présentée par le ministère de l'Éducation nationale concernant le traitement « I-prof » proposant à chaque enseignant un ensemble de services internet sécurisés et personnalisés relatifs à sa carrière administrative
03-038 16 septembre 2003 (*cf.* p. 384)	Délibération portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques
03-039 19 juin 2003	Délibération décidant une mission de contrôle
03-040 23 septembre 2003 (*cf.* p. 343)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
03-041 23 septembre 2003 (*cf.* p. 321)	Délibération portant avis sur un projet d'arrêté interministériel portant création d'un dispositif expérimental visant à automatiser la constatation de certaines infractions routières et l'envoi de l'avis de contravention correspondant et modifiant l'arrêté du 29 juin 1992 portant création du système national des permis de conduire
03-042 23 octobre 2003	Délibération décidant une mission de contrôle
03-043 7 octobre 2003 (*cf.* p. 256)	Délibération portant avis sur un projet de décret modifiant le Code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques
03-044 7 octobre 2003 (*cf.* p. 388)	Délibération portant avis favorable à la mise en place par la société Cofiroute d'un dispositif expérimental de lecture et de reconnaissance automatisées de la plaque minéralogique permettant d'alerter les conducteurs de véhicule dépassant la vitesse maximale autorisée

Numéro Date	Objet
03-045 23 septembre 2003	Délibération décidant une mission de contrôle
03-046 23 septembre 2003	Délibération décidant une mission de contrôle
03-047 23 octobre 2003 (*cf.* p. 392)	Délibération portant avertissement à l'Union fédérale autonome pénitentiaire
03-048 30 octobre 2003 (*cf.* p. 291)	Délibération concernant la mise en place par la direction générale des impôts d'une base nationale de recensement des liens d'intérêts existant entre personnes physiques et sociétés
03-049 20 novembre 2003 (*cf.* p. 404)	Délibération portant avis sur le projet de décret modifiant le décret n° 91-739 du 18 juillet 1991 relatif aux chambres de commerce et d'industrie, aux chambres régionales de commerce et d'industrie, à l'assemblée des chambres françaises de commerce et d'industrie et aux groupements interconsulaires
03-050 20 novembre 2003 (*cf.* p. 243)	Délibération portant avis sur le projet de règlement modifié n° 90.05 du 11 avril 1990 du Comité de la réglementation bancaire relatif au Fichier des incidents de remboursement des crédits aux particuliers
03-051 20 novembre 2003 (*cf.* p. 246)	Délibération portant avertissement au Crédit immobilier de France
03-052 20 novembre 2003 (*cf.* p. 248)	Délibération portant avertissement au Crédit Mutuel du grand Cronenbourg
03-053 27 novembre 2003 (*cf.* p. 361)	Délibération portant adoption d'une recommandation relative aux traitements de données à caractère personnel mis en œuvre par les registres du cancer
03-054 27 novembre 2003 (*cf.* p. 229)	Délibération portant avis sur les dispositions relatives au développement de l'administration électronique de l'avant-projet de loi habilitant le Gouvernement à simplifier le droit par voie d'ordonnances

Numéro Date	Objet
03-055 27 novembre 2003	Délibération décidant une mission de contrôle
03-056 9 décembre 2003 (*cf.* p. 334)	Délibération portant avis sur le projet de décret relatif à la conservation des données relatives à une communication par les opérateurs de télécommunications et portant modification du Code des postes et des télécommunications
03-057 9 décembre 2003 (*cf.* p. 345)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-058 9 décembre 2003 (*cf.* p. 347)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-059 9 décembre 2003 (*cf.* p. 349)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-060 9 décembre 2003 (*cf.* p. 351)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-061 9 décembre 2003 (*cf.* p. 353)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-062 9 décembre 2003 (*cf.* p. 355)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-063 9 décembre 2003 (*cf.* p. 357)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications
03-064 9 décembre 2003 (*cf.* p. 359)	Délibération portant dénonciation au parquet d'infractions au Code des postes et télécommunications

Numéro Date	Objet
03-065 16 décembre 2003 (*cf.* p. 263)	Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par la mairie de Levallois-Perret, destiné à contrôler l'accès au « roller-parc » par la reconnaissance des empreintes digitales
03-066 18 décembre 2003 (*cf.* p. 235)	Délibération portant avis sur un projet de décret du ministre des Affaires étrangères relatif à l'inscription au registre des Français hors de France
03-067 18 décembre 2003 (*cf.* p. 296)	Délibération relative à la gestion et aux négociations des biens immobiliers (norme simplifiée n° 21)
03-068 18 décembre 2003 (*cf.* p. 374)	Délibération portant avis sur le projet d'arrêté portant création, par l'INSEE, d'un traitement automatisé pour la saisie et l'exploitation des données collectées lors du recensement général de la population

Questions parlementaires

Sénat

Question n° : 1780 de M. **Mathieu Serge**, ministère interrogé : Justice, ministère attributaire : Premier ministre
Réponse publiée au *JO* le 2 janvier 2003 (page 24)

Informations nominatives dans les bases de données juridiques

Question : M. Serge Mathieu demande à M. le garde des Sceaux, ministre de la Justice, de lui préciser la suite qu'il envisage de réserver à la délibération n° 2001-057 du 29 novembre 2001 de la Commission nationale de l'informatique et des libertés (CNIL), s'inquiétant de la présence d'informations nominatives relatives à des personnes parties prenantes aux procès et à des témoins, dans les bases de données juridiques, toujours plus nombreuses et plus importantes.

Réponse : la constitution de bases de données juridiques permettant à un large public de consulter les textes normatifs et la jurisprudence a pour objet de faciliter l'accès au droit d'un large public. Elle contribue ainsi à la mise en œuvre du principe d'accessibilité et de lisibilité du droit, dont le Conseil constitutionnel a jugé, par sa décision n° 99-421 DC du 16 décembre 1999, qu'il avait valeur constitutionnelle. Elle répond, plus largement, à un souci de démocratie. Telles sont les raisons pour lesquelles le Gouvernement, par décret du 7 août 2002, a créé un nouveau service public de la diffusion du droit sur l'internet qui permet, notamment, une consultation facile et gratuite des principales décisions rendues par les juridictions des différents ordres. Le Gouvernement a néanmoins voulu s'assurer de la compatibilité de la démarche ainsi entreprise avec les exigences liées au respect des droits et libertés des personnes physiques. Aussi s'est-il attaché à tirer pleinement les conséquences de la recommandation émise par la Commission nationale de l'informatique et des libertés, à laquelle fait référence l'honorable parlementaire. Conformément aux termes de cette recommandation, il a décidé qu'il irait au-delà du respect des dispositions spéciales qui font obligation de ne pas mentionner le nom des parties à certaines instances et qu'il s'abstiendrait, plus généralement, de faire apparaître l'identité et l'adresse des parties et des témoins, pour l'ensemble des arrêts et jugements des juridictions administrative et judiciaire mis en ligne. Ainsi, depuis le 15 septembre 2002, date d'ouverture du nouveau service de diffusion, aucune décision de justice n'est plus intégrée dans les bases répertoriant les arrêts du Conseil d'État et de la Cour de cassation sans avoir fait l'objet de ce traitement préalable. Quant aux décisions déjà présentes dans les bases de données, elles feront l'objet du même traitement, qui devra être achevé dans un délai maximum de deux ans. Les dispositions ainsi rappelées figurent dans l'arrêté du 9 octobre 2002 relatif au site internet Légifrance (*JO* du 11 octobre 2002), qui a reçu l'avis favorable de la Commission nationale de l'informatique et des libertés, dans les conditions prévues par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Sénat

Question n° : 525 de M. **Masson Jean-Louis**, ministère interrogé : Intérieur, ministère attributaire : Premier ministre
Réponse publiée au *JO* le 16 janvier 2003 (page 189)

Utilisation des actes d'état civil par certains maires

Question : M. Jean-Louis Masson attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur le fait que certains maires utilisent les actes d'état civil pour adresser des courriers personnalisés aux administrés lors d'événements familiaux (naissances, décès...). Il souhaiterait qu'il lui indique si un tel procédé est légal.

Réponse : l'utilisation par les maires des registres d'état civil de leurs communes pour l'envoi de courriers personnalisés à l'occasion d'une naissance, d'un décès ou d'un mariage, participe d'une action de communication municipale. Toutefois, dans sa délibération n° 99-24 du 8 avril 1999 portant sur un projet d'arrêté concernant l'envoi de courriers personnalisés aux administrés lors d'événements tels que les décès, naissances et mariages, la CNIL a considéré que le *« respect du principe de finalité des traitements s'oppose, de manière générale, à ce que des informations enregistrées dans un fichier soient utilisées à des fins étrangères à celles qui ont justifié leur collecte et leur traitement »*. De plus, la Commission estime *« de doctrine constante, que ce principe de finalité constitue une garantie essentielle au respect de la vie privée et de la tranquillité des personnes tout particulièrement lorsque des fichiers publics sont en cause »*, ce d'autant que les personnes concernées ne disposent pas de la faculté de s'opposer à y figurer. Dès lors, les données recueillies à l'occasion de cette mission de service public, confiée par la loi aux officiers d'état civil, ne sauraient être utilisées à d'autres fins par quiconque, et par conséquent, à des actions de communication municipale. Cet avis a fait l'objet d'une circulaire n° NORINTB9900130C du ministère de l'Intérieur en date du 2 juin 1999, invitant les préfets à appeler l'attention des élus communaux sur les conditions d'utilisation des fichiers concernant les administrés, et à porter à leur connaissance la teneur de l'avis de la CNIL. Par ailleurs, il doit être souligné que l'utilisation par les officiers d'état civil à des fins de communication personnalisée des informations portées sur les registres dont ils sont responsables n'a pas été prévue par le décret modifié n° 62-921 du 3 août 1962, dont les dispositions restrictives, prévoyant un accès limité au registre et des règles strictes de publicité des actes de l'état civil, ont été édictées dans le souci de respecter la confidentialité de la vie privée. Ces éléments conduisent à considérer que, si légitime fût-il par ailleurs, le souci de proximité des maires avec leurs administrés ne constitue pas un motif suffisant pour qu'il soit envisagé d'introduire dans les textes une dérogation aux principes fondamentaux de protection des personnes, même en la limitant aux communications qui n'ont pas un caractère de propagande politique ou qui n'auraient pas lieu en période préélectorale.

Sénat

Question n° : 02956 de M^me^ **Borvo Nicole**, ministère interrogé : Justice
Réponse publiée au *JO* le 6 février 2003 (page 478)

Listes des données circulant sur Internet à enregistrer par les opérateurs techniques

Question : M^me^ Nicole Borvo attire l'attention de M. le garde des Sceaux, ministre de la Justice, sur la question de la surveillance des données de communication publique et privée circulant sur l'internet, et de la définition des données devant donner lieu à l'enregistrement par les opérateurs techniques. La loi n° 2001-1062 du 15 novembre 2001, relative à la sécurité quotidienne introduit en effet, par son article 29, la nécessité pour les opérateurs de conserver un ensemble de données techniques, susceptibles d'être extraites à des fins d'enquêtes judiciaires. La nature exacte de ces données n'est certes pas encore connue, un décret en Conseil d'État devant compléter le texte de loi. Il n'en reste pas moins que les préconisations du G8 et d'Europol en la matière sont de nature à inquiéter tant les prestataires techniques concernés que l'ensemble des citoyens français, tant elles vont à l'encontre du respect des libertés individuelles et des préceptes énoncés dans la Déclaration universelle des droits de l'homme et du citoyen. En effet, que ce soit par son article 12, qui affirme le droit de chacun à la protection de sa vie privée et au secret de sa correspondance, ou son article 18, qui fonde le droit de tout individu à l'expression publique ou privée de ses opinions, cette déclaration est là pour nous rappeler combien il serait dommageable pour une démocratie de chercher à contrôler ou à restreindre par des mesures de surveillance systématique la libre circulation de l'information sur les réseaux de communication. Les mesures de vigilance que les citoyens français sont en droit d'attendre de l'État en matière de lutte contre le terrorisme ne sauraient en retour les faire considérer tous comme suspects par défaut et entraîner la mise en œuvre de dispositifs d'écoute généraliste de l'ensemble du pays. La réflexion concernant les données que la justice peut légitimement demander aux opérateurs de conserver ne saurait être engagée sans consultation préalable de ceux que ces nouvelles mesures législatives vont concerner. Le législateur ne saurait faire l'impasse sur l'avis en la matière des opérateurs internet, mais pas plus sur celui des représentants de la société civile informatique, et plus largement de tous les utilisateurs des réseaux électroniques et de communication. Le droit imprescriptible à l'anonymat et à la vie privée ne saurait être diminué par de nouvelles lois d'exception prenant prétexte de nouveaux médias. Il existe déjà en France des dispositifs réglementaires sur la protection de la correspondance postale, sur l'informatique et les libertés, la protection des personnes et de leur vie privée, sur les propos racistes et antisémites. Reste à dégager pour la justice et ses auxiliaires, les moyens, y compris sur internet, de la mise en œuvre de ces différentes lois. Elle lui demande donc quelles sont les intentions du Gouvernement quant à la procédure d'établissement de la liste des données qui seront incluses dans le décret précisant la loi relative à la sécurité quotidienne. Elle lui demande également de surseoir à la rédaction de ce décret, pour permettre la mise en place d'une commission de travail compétente sur l'opportunité de conservation de chaque type de données, associant tous les acteurs concernés et aboutissant à la production d'un document qui ne soit pas que l'expression d'une angoisse exacerbée par la violence extrême d'actes isolés.

Réponse : le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire qu'il ne partage pas les craintes que celle-ci exprime quant à un caractère attentatoire aux libertés fondamentales du dispositif prévu par l'article 29 de la loi du 15 novembre 2001 relative à la sécurité quotidienne, lequel permet

au Gouvernement de prendre par voie réglementaire des mesures conduisant les opérateurs de télécommunications à conserver pendant une durée maximale d'un an certaines données techniques relatives aux communications, dites parfois « données de connexion ». En effet, ces mesures, dont le but exclusif est de permettre en tant que de besoin la mise à disposition de l'autorité judiciaire de telles ou telles de ces données, ne sauraient en aucun cas être assimilées, ainsi qu'il est suggéré par l'auteur de la question, à une surveillance systématique de l'information circulant sur les réseaux de communication, ou à un dispositif d'écoute généralisé de l'ensemble des citoyens français. Sur ce point, il est en effet clairement énoncé par la loi susvisée que les données ainsi conservées, si elles rendent possible l'identification de l'utilisateur d'un service de télécommunications, ne peuvent en revanche d'aucune manière porter, comme le ferait une interception de correspondance émise par la voie des télécommunications, sur le contenu des correspondances échangées ou des informations consultées. Ces raisons expliquent que la conservation temporaire des données dites de connexion ne constitue pas à proprement parler une ingérence dans la liberté d'expression et de communication. Il doit du reste être observé que les dispositions suscitant les inquiétudes de l'honorable parlementaire sont en stricte conformité avec les possibilités expressément ménagées aux États dans un but de prévention, de recherche, de détection et de poursuite d'infractions pénales, par l'article 15 de la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Par ailleurs, ces dispositions ne sont aucunement contraires aux principes énoncés dans la Déclaration universelle des droits de l'homme proclamée par l'assemblée générale des Nations unies le 10 décembre 1948. En effet, l'exercice des droits prévus aux articles 12 et 18 de celle-ci, lesquels prohibent les immixtions arbitraires dans la vie privée ou la correspondance et proclament le droit de toute personne à la liberté de pensée de conscience et de religion, ne peut se concevoir concrètement sans un certain nombre de limitations. L'édiction de celles-ci par la loi est expressément envisagée par l'article 29 de la Déclaration, et elle peut être autorisée notamment pour assurer la reconnaissance et le respect des droits et libertés d'autrui et la prise en considération des exigences de l'ordre public dans une société démocratique. À cet égard, dans un contexte marqué par les menaces terroristes que doivent affronter les sociétés démocratiques contemporaines, le Gouvernement ne peut faire sienne l'opinion selon laquelle les libertés dont il convient d'assurer le respect sur les réseaux électroniques de communication se traduisent par « un droit imprescriptible à l'anonymat ». Une telle analyse conduirait en effet à paralyser la lutte contre de multiples activités terroristes et de nombreuses formes de délinquance organisée qui s'exercent par le biais des réseaux de communication électronique. S'agissant enfin des aspects de la présente question qui concernent les modalités d'élaboration du décret d'application de l'article 29 de la loi susvisée du 15 novembre 2001, il importe de préciser que la procédure qui devra être suivie à cet égard de par un choix du législateur, prévoit un haut niveau de garanties, puisque ce texte réglementaire requiert la double consultation de la Commission nationale de l'informatique et des libertés et du Conseil d'État. Il convient par ailleurs de rappeler que les dispositions qui figurent à l'article 29 de la loi sur la sécurité quotidienne ont d'ores et déjà fait l'objet d'une consultation publique dans le cadre de l'élaboration du projet de loi sur la société de l'information, où elles figuraient initialement. En outre, sous la présente législature, elles ont été soumises aux opérateurs de télécommunication. Dans ces conditions, il n'apparaît pas que de nouvelles mesures de concertation de la nature de celles proposées par l'honorable parlementaire soient nécessaires.

Assemblée nationale

Question n° : 8558 de M. **Deflesselles Bernard**, ministère interrogé : Justice
Réponse publiée au *JO* le 2 juin 2003 (page 4306)

Ventes et échanges — Ventes par téléphone. Démarchage. Usage abusif

Question : M. Bernard Deflesselles attire l'attention de M. le garde des Sceaux, ministre de la Justice, sur la multiplication inquiétante de pratiques téléphoniques commerciales susceptibles de constituer des ingérences dans la vie privée des particuliers. En effet, de plus en plus d'entreprises pratiquent des démarchages téléphoniques en utilisant des questionnaires particulièrement indiscrets et qui représentent autant d'atteintes potentielles au droit du respect de la vie privée. De plus certaines de ces méthodes commerciales sont à la limite du harcèlement moral étant pratiquées à toute heure de la journée et en tout lieu sans aucune considération au trouble porté à la tranquillité des destinataires. C'est pourquoi il lui demande de bien vouloir préciser les mesures qu'il entend prendre afin de mettre un terme à ces pratiques intempestives et qui utilisent, en outre, des numéros de téléphones privés à des fins commerciales sans accord préalable.

Réponse : le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que le législateur, soucieux d'assurer la protection des particuliers, a élaboré un régime spécifique au démarchage commercial par téléphone. Notamment, l'article L. 121-27 du Code de la consommation impose au professionnel d'adresser une confirmation écrite de l'offre qu'il a faite téléphoniquement au consommateur. Le destinataire est donc en mesure d'opérer, le cas échéant, un choix commercial dans des conditions éclairées, mais il peut également demander au professionnel de cesser toute sollicitation. Plus généralement, les abonnés peuvent, en vertu des articles R. 10-1 et R. 10-2 du Code des postes et des télécommunications pris en application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, demander à ne pas figurer sur les listes extraites des annuaires commercialisés par France Télécom en se faisant inscrire gratuitement dans un fichier public dénommé « liste Orange », ce qui impose aux entreprises de ne plus user de leurs coordonnées téléphoniques. Ainsi, une personne privée dispose toujours de la faculté de s'abstraire du circuit commercial. Si pour ce faire elle doit, certes, effectuer une démarche, elle peut ainsi éviter les nuisances de méthodes par trop intrusives. Sur ce point, les principes fondamentaux du droit trouvent à s'appliquer, et, en particulier, l'article 9 du Code civil aux termes duquel chacun a droit au respect de sa vie privée et peut demander au juge, appréciant souverainement la réalité de l'atteinte à ce droit fondamental, de faire cesser tout abus.

Assemblée nationale

Question n° : 15696 de M. **Abelin Jean-Pierre**, ministère interrogé : Justice
Réponse publiée au *JO* le 2 juin 2003 (page 4316)

Droits de l'homme et libertés publiques — Fichiers informatisés. Directive européenne. Transposition

Question : pendant longtemps, la France n'a pas respecté le délai de transposition de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le délai de transposition venait à échéance le 24 octobre 1998. Après une procédure de

mise en demeure et d'avis motivé de la Commission en application de l'article 226 du traité, la Commission s'est désistée le 29 octobre 2001 et l'affaire a été radiée. M. Jean-Pierre Abelin demande à M. le garde des Sceaux, ministre de la Justice, de bien vouloir lui indiquer les raisons avancées par la France pour justifier la satisfaction des exigences de la directive par la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Réponse : le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que la France a obtenu, le 29 novembre 2001, le désistement de la Commission européenne de son action en manquement en faisant valoir que les dispositions de la directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données étaient d'ores et déjà mises en œuvre en droit français par la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. En effet, la Commission s'est très largement inspirée de cette législation pionnière pour élaborer la proposition de texte qui allait conduire à l'adoption de cette directive. La Commission a accueilli l'argument selon lequel la France s'était abstenue de notifier cette législation parce qu'elle avait entrepris, peu après l'entrée en vigueur de la directive 95/46, une vaste révision de sa loi dont l'adoption avait pris du retard. Ce projet de loi exprime la volonté du Gouvernement d'adapter le dispositif d'ensemble de la protection des données à l'ère nouvelle inaugurée par la très large diffusion de l'outil informatique et de l'internet et ne se limite pas à un souci de transposition de la directive 95/46. Le projet de loi sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel a été adopté en première lecture par l'Assemblée nationale, puis par le Sénat le 2 avril dernier et il devrait être examiné prochainement par le Parlement en seconde lecture.

Assemblée nationale

Question nº : 12300 de M. **Bourg-Broc Bruno**, ministère interrogé : Santé
Réponse publiée au *JO* le 9 juin 2003 (page 4612)

Santé — Sida. Fichiers informatisés. Secret médical. Respect

Question : M. Bruno Bourg-Broc appelle l'attention de M. le ministre de la Santé, de la Famille et des Personnes handicapées sur l'intérêt et l'importance qui s'attachent à une amélioration des fichiers relatifs aux malades du sida. Avec la nécessité du maintien du secret médical, il apparaît, aux yeux des spécialistes, qu'il convient d'adapter les fichiers des personnes concernées, en liaison avec les propositions de la CNIL. Il lui demande les perspectives de son action ministérielle s'inspirant de ces considérations puisque, de l'avis général, la France a pris quatre années de retard, avec notamment l'Autriche et l'Irlande.

Réponse : afin d'améliorer la prise en charge médicale et sociale des personnes atteintes du sida et d'adapter les actions de prévention, les pouvoirs publics ont souhaité organiser un dispositif permettant de recueillir des informations concernant les personnes atteintes. Depuis 1986, ces données sont recueillies auprès des malades au moyen d'une fiche de déclaration, le sida faisant partie des maladies dites « à déclaration obligatoire ». En 1999, suite à l'introduction des trithérapies qui ont modifié l'évolution de l'infection vers la maladie, il est apparu nécessaire, afin d'avoir une vision dynamique de l'épidémie, de rendre aussi obligatoire la déclaration de l'infection au VIH. À la suite des craintes exprimées par les associations de défense des malades atteints du sida d'un fichage nominatif des personnes séropositives, la direction générale de la santé a, dans un souci de concertation, constitué un

groupe de travail comprenant notamment les associations de patients et la CNIL. La Commission, sur la base des travaux de ce comité, a préconisé la mise en place d'un certain nombre de mesures propres à garantir l'anonymat des personnes et à assurer le respect du secret médical : anonymisation à la source des déclarations à l'aide d'un codage informatique des initiales des nom et prénom et de la date de naissance. Identification du lieu de domicile de la personne limitée au seul code du département et de la profession sous la seule forme de la catégorie socioprofessionnelle. Le dispositif de notification anonymisé des maladies à déclaration obligatoire dont le VIH/sida, a donc été repensé afin de garantir la protection de l'anonymat des malades. Près de quatre années de travaux communs entre les différents acteurs (associations de malades, défenseurs des droits de l'homme, CNIL, INVS et services de l'État) ont été nécessaires pour que soient réunies les conditions de mise en œuvre de ce dispositif. L'ensemble du nouveau dispositif qui sera prochainement mis en œuvre par l'INVS respecte donc les recommandations de la CNIL et a d'ailleurs reçu un avis favorable de la Commission qui a considéré que le secret médical ainsi que l'anonymat des personnes atteintes du sida ou d'une infection au VIH sont respectés. Il est à noter que pendant la période de mise en place de ce dispositif le recueil des informations issues de la déclaration obligatoire des cas de sida a eu lieu selon les procédures antérieurement mises en place.

Assemblée nationale

Question n° : 11685 de M. **Tiberi Jean**, ministère interrogé : Intérieur
Réponse publiée au *JO* le 16 juin 2003 (page 4806)

Sécurité publique — Délinquance. Lutte et prévention. Système informatique. Perspectives

Question : M. Jean Tiberi demande à M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales le sentiment du Gouvernement sur les premiers résultats de l'expérience du système informatique Géoprévention visant à renforcer la prévention locale et conduite dans la ville de Roubaix. Ce système s'inspire des expériences menées depuis plusieurs années dans plusieurs grandes villes américaines ou canadiennes, afin de diminuer quantitativement les délits et incivilités commis sur la voie publique. Le Gouvernement pourrait en encourager l'utilisation.

Réponse : un procédé de localisation et de cartographie des phénomènes de délinquance est actuellement expérimenté à Roubaix. La Commission nationale de l'informatique et des libertés a émis un avis favorable à sa mise en œuvre pour une durée d'un an. La version initiale du logiciel, en l'occurrence le système Géoprévention, a nécessité des ajustements techniques qui ont retardé la phase des essais pratiques. Aussi est-il encore prématuré de dresser un bilan et de statuer sur l'opportunité et les modalités de son éventuelle extension. Sur ce point, il doit être précisé que son alimentation provient, pour une large part, d'informations issues du système de traitement des infractions constatées (STIC), application gérée par la police nationale, dont l'exploitation et la transmission des données sont régies par le décret n° 2001-583 du 5 juillet 2001. Le STIC étant une banque de données orientée à des fins de recherches criminelles, son exploitation et sa consultation sont placées sous l'autorité du procureur de la République, afin de concilier les impératifs opérationnels et le respect des libertés individuelles, notamment en ce qui concerne la transmission d'informations à caractère nominatif ou indirectement nominatif. Son utilisation comme instrument d'aide au pilotage des politiques locales partenariales de prévention et de sécurité, auxquelles les élus sont aujourd'hui étroitement associés, n'a pas été prévue. Le développement de tels dispositifs nécessite la résolution préalable des

questions de sécurité informatique et l'élaboration d'une procédure type, propre à concilier l'information des élus locaux par les services de l'État et le respect de la vie privée et de la liberté individuelle. Tel est le sens des travaux actuellement menés au sein du ministère de l'Intérieur, de la Sécurité intérieure et des Libertés locales.

Sénat

Question n° : 03500 de M^me^ **Beaudeau Marie-Claude**, ministère interrogé : Intérieur
Réponse publiée au *JO* le 19 juin 2003 (page 2017)

Recensement des personnes « mobiles »

Question : M^me^ Marie-Claude Beaudeau attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur la nouvelle organisation par l'INSEE du recensement général de la population dans le cadre du « recensement rénové » et notamment sur celui des personnes classées « mobiles », à savoir les personnes n'ayant pas de domicile fixe et en particulier les gens du voyage. En effet, contrairement à ses engagements initiaux, la direction de l'INSEE a décidé unilatéralement de déléguer aux communes le dénombrement des personnes « mobiles » au même titre que celui des personnes résidant dans des logements « ordinaires ». Elle lui fait pourtant remarquer que les relations entre les autorités communales et les personnes « mobiles » sont souvent difficiles et conflictuelles. Il lui paraît difficile d'ignorer que nombre de communes sont réticentes à accueillir les gens du voyage quand elles n'exercent pas ouvertement des pressions à leur égard visant à les dissuader de rester sur leur territoire, par exemple par des arrêtés municipaux d'expulsion des caravanes. Elle lui rappelle également l'absence d'aires de stationnement ou de terrains d'accueil dans la plupart des communes de moins de 5 000 habitants, et les multiples retards d'application de la loi Besson n° 2000-614 du 5 juillet 2000 qui stipule pourtant leur création obligatoire dans les communes de plus de 5 000 habitants. Aussi, il lui semble contradictoire avec l'esprit de confiance qui doit présider à la collecte des informations destinées au recensement qu'elle soit confiée, dans le cas des personnes mobiles, à des agents placés sous la responsabilité des communes, éventuellement même leurs forces de police municipale, dont on ne peut pas exclure qu'ils les utilisent à des fins répressives. C'est pourquoi, elle lui demande pour préserver l'efficacité, l'objectivité, la neutralité et la confidentialité du recensement, action administrative qui doit n'avoir pour but que le recueil de données à des fins statistiques et rester débarrassée de toute intention de contrôle et de jugement sur l'opportunité d'une présence, de lui faire connaître les mesures qu'il envisage de prendre pour continuer à faire recenser les personnes « mobiles » par les délégués de l'INSEE. Elle lui demande plus précisément quelles dispositions il compte retenir dans ce sens dans les six décrets d'application de la loi n° 2002-276 du 27 février 2002 sur la démocratie de proximité qui institue le « recensement rénové ».

Réponse : dans le recensement traditionnel, les personnes vivant habituellement dans des habitations mobiles et les personnes sans abri étaient recensées par les agents recenseurs recrutés par les soins des maires. La loi du 27 février 2002, qui confie aux communes la responsabilité de préparer et de réaliser les enquêtes de recensement sous le contrôle de l'INSEE, et le projet de décret d'application de celle-ci ne changent rien à cet égard. En effet, une condition nécessaire pour assurer un bon dénombrement est d'avoir pu recenser effectivement les personnes dont il s'agit. Chacune des 36 500 communes de France est en situation de connaître à tout moment la présence d'habitations mobiles sur son territoire. Tel n'est pas le cas de l'INSEE. Face

aux interrogations sur l'éventualité d'une utilisation des informations tirées du recensement à d'autres fins que statistiques, il convient de rappeler que la collecte des informations individuelles est encadrée par la loi du 7 juin 1951 sur le secret statistique et, sous le contrôle de la Commission nationale de l'informatique et des libertés (CNIL), par la loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés. Les questionnaires du recensement sont destinés à une utilisation statistique et ne peuvent connaître d'autre utilisation. Les détourner de cette finalité exposerait à de lourdes sanctions pénales. Tout au long de la collecte, l'INSEE aura sur le terrain des responsables chargés de conseiller les communes sur la bonne exécution des enquêtes de recensement et de contrôler la mise en œuvre des dispositions législatives et réglementaires qui encadrent le recensement de la population. Ces dispositions s'appliquent à toutes les personnes recensées, sans aucune exception.

Assemblée nationale

Question nº : 17333 de M. **Wœrth Éric**, ministère interrogé : Intérieur
Réponse publiée au *JO* le 14 juillet 2003 (page 5664)

Élections et référendums — Opérations de vote. Vote électronique. Perspectives

Question : M. Éric Wœrth appelle l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur le projet de généralisation des machines à voter dans les communes. En effet, ce processus semble bien enclenché, puisque les machines à voter doivent au préalable avoir reçu l'agrément du ministère et que pour ce faire le ministère a, à cet effet, conclu en juin 2002, après appel d'offres, un marché avec une société de conseil en vue de l'élaboration d'un cahier des charges techniques. « L'objectif est de permettre aux communes de s'équiper dès 2004. » Or, le prix moyen d'une machine à voter s'élève à 3 500 euros. Ainsi, pour une commune de 10 000 électeurs avec dix bureaux de vote, le budget d'investissement serait de 140 000 euros plus environ 20 % de frais d'exploitation annuels (formation, stockage, etc.) et 5 % de frais de maintenance soit environ 245 000 euros. Le budget pour une commune comme Paris s'élèverait à 11,5 millions d'euros. À l'heure où l'expérimentation du vote par internet (coût d'investissement matériel nul) apparaît possible, puisque les techniques mises au point offrent des garanties suffisantes pour assurer le secret du vote ; le Parlement a d'ailleurs adopté la proposition de loi tendant à autoriser le vote par correspondance électronique des Français établis hors de France pour les élections du Conseil supérieur des Français de l'étranger qui va dans ce sens. À un moment où la maîtrise des dépenses publiques devient une priorité, il lui demande de préciser s'il entend poursuivre ce processus de généralisation fort coûteux pour les communes et semble-t-il très prochainement obsolète.

Réponse : il n'est pas possible, pour les élections politiques, de comparer les avantages et inconvénients respectifs des machines à voter et du vote par internet. En effet, le vote par internet n'a pas vocation à s'appliquer aux élections politiques. Le fait que le vote s'effectue hors du bureau de vote, sans isoloir, ne permet pas de protéger l'électeur des pressions extérieures au moment du vote. Le caractère personnel et secret du vote, principe à valeur constitutionnelle pour les élections politiques, ne serait donc plus garanti. Ces inconvénients sont d'ailleurs les mêmes que ceux présentés par le vote par correspondance, interdit en 1975 pour les élections politiques. Dans ces conditions, le vote par internet ne peut être mis en œuvre qu'à l'occasion d'élections pour lesquelles le vote par correspondance est autorisé, comme celles au Conseil supérieur des Français de l'étranger. L'acquisition de machines à voter

demeure donc pertinente. Les communes pourront d'ailleurs choisir de s'équiper de machines allant au-delà de la simple urne électronique et permettant de transmettre les résultats électoraux par voie informatique. Les machines pourront en outre être utilisées pour les élections prud'homales et consulaires. Au demeurant, et conformément à l'article L. 57-1 du Code électoral, le Gouvernement n'entend pas généraliser l'emploi des machines à voter mais permettre aux communes qui le souhaitent de s'équiper en agréant des modèles de machine. Le montant de la participation de l'État à l'acquisition de cet équipement sera fixé dans le cadre de la loi de finances pour 2004.

Assemblée nationale

Question nº : 15610 de M. **Lamy François,** ministère interrogé : Santé
Réponse publiée au *JO* le 21 juillet 2003 (page 5879)

Droits de l'homme et libertés publiques — Dossier médical. Discriminations fondées sur l'état de santé. Interdiction

Question : M. François Lamy appelle l'attention de M. le ministre de la Santé, de la Famille et des Personnes handicapées sur la loi et sur les droits des malades. Cette dernière laisse entrevoir des effets pervers, un an après son entrée en vigueur. Selon les premiers éléments d'une enquête de l'observatoire éthique de l'Assistance publique des hôpitaux de Paris, un de ses volets, concernant le droit d'accès au dossier médical, donnerait lieu à des dérives. *« Nous n'en sommes qu'au stade de la préenquête, note le professeur Roger Mislavski, mais nous avons pu voir, sur la région parisienne, que de plus en plus de patients demandent leurs dossiers. Or, outre le coût que cela entraîne, ces dossiers semblent être utilisés par des compagnies d'assurances parce que les gens acceptent de donner leur dossier sans réfléchir à la gravité du geste. Nous avons eu le sentiment que certains patients étaient presque contraints à fournir le leur »*. Une pression que certains organismes de prêts bancaires feraient parfois également subir à leurs clients. Si les compagnies d'assurance ne peuvent se baser sur les résultats de tests génétiques pour modifier leurs contrats, rien ne leur interdit de le faire en cas de suspicion de maladie, par exemple. Il lui demande donc de bien vouloir lui signifier quels ajustements entend-t-il apporter pour pallier ces effets pervers.

Réponse : le Code de la santé publique dispose que toute personne a droit au respect de sa vie privée et au secret sur les informations concernant sa santé. Pour autant, le secret médical doit être concilié en matière d'assurance avec l'obligation pour l'assuré de fournir les indications nécessaires à l'appréciation du risque assuré. L'assuré ne peut contourner cette obligation, pas même en invoquant le secret médical, lorsque l'état de santé constitue un élément devant être nécessairement pris en compte pour le risque assuré. Toutefois, dans ce cas, l'appréciation du risque ou la preuve de l'obligation d'exécuter le contrat ne devrait pas conduire à ce que les demandes de renseignements excèdent le strict nécessaire ; la loyauté s'impose à chacun des contractants. Cependant, le principe de l'accès direct de toute personne à ses informations de santé, institué par la loi du 4 mars 2002 dans le respect de l'autonomie de la personne malade, comporte par nature le risque de mésusage par la personne concernée des informations obtenues directement. La personne sollicitée abusivement pour fournir des informations confidentielles n'est pas tenue de les communiquer ; elle pourra aussi trouver conseil auprès du professionnel de santé qui détient le dossier, en particulier pour apprécier l'étendue de la demande et les documents pertinents à fournir. La question du recueil et de la collecte des informa-

tions de santé par les assureurs est suivie par la direction générale de la santé. Elle a demandé que la commission de suivi de la convention du 19 septembre 2001, visant à améliorer l'accès à l'assurance des personnes présentant un risque de santé aggravé, examine la question au titre du « code de bonne conduite » concernant le recueil et la collecte des données personnelles de santé, annexé à la convention et qui est de portée générale.

Sénat

Question n° : 04494 de M. **Hamel Emmanuel**, ministère interrogé : Économie
Réponse publiée au *JO* le 21 août 2003 (page 2619)

Création d'un « fichier positif » pour les ménages surendettés

Question : M. Emmanuel Hamel attire l'attention de M. le ministre de l'Économie, des Finances et de l'Industrie sur l'information parue à la page V du *Figaro-Économie* du 19 juin 2002 selon laquelle le directeur du Trésor a évoqué devant l'assemblée générale de l'Association française des sociétés financières « l'éventualité de la création en France d'un fichier positif des particuliers endettés ».

Réponse : la création d'un fichier central nominatif recensant l'ensemble des crédits contractés par les ménages, fichier dit « positif », avait été évoquée dès 1989 au moment de l'élaboration de la loi Neiertz, mais avait été écartée au profit d'un fichier dit « négatif », le Fichier national des incidents de paiement des crédits aux particuliers (FICP). La question de la création d'un fichier « positif » revient depuis très régulièrement. Elle a été de nouveau soulevée par le projet de directive sur le crédit à la consommation en cours de négociation à Bruxelles, qui en fait mention. Au sein du comité consultatif, la création d'un fichier « positif » a été de nouveau débattue à l'occasion du nouvel avis sur le surendettement rendu en décembre 2002. Elle n'a pas réuni de consensus. Aussi, malgré l'intérêt manifesté par certaines organisations de consommateurs qui considèrent qu'un tel fichier, bien encadré, serait un moyen de renforcer la prévention du surendettement, le comité consultatif a rejeté l'idée de préconiser sa création. Techniquement, l'efficacité d'un tel fichier en tant qu'outil de prévention du surendettement fait débat. Les représentants des consommateurs et des établissements de crédit constatent en effet qu'un fichier « positif » serait inopérant au regard de la principale cause de surendettement (64 % des cas selon l'enquête typologique réalisée par la Banque de France) que sont les accidents de la vie (chômage, rupture de la vie commune, maladie et décès). Il devrait notamment faire l'objet d'une mise à jour en temps réel pour prévenir des situations dans lesquelles, placées devant une brusque baisse de leurs revenus, les personnes confrontées à un « accident de la vie » se mettent à tirer rapidement sur des lignes de crédit jusqu'alors peu utilisées. Le seul recensement des crédits aux particuliers ne pourrait, par ailleurs, procurer qu'une vision partielle de l'endettement réel des ménages, les dettes fiscales et les loyers, par exemple, étant exclus. Il ne serait pas un indicateur suffisant en l'absence d'informations précises sur la situation financière des particuliers, notamment leurs revenus et leur situation de famille. Or, la création d'un fichier de l'endettement recensant toutes ces informations soulève d'importantes questions en termes de protection de la vie privée. La Commission nationale de l'informatique et des libertés, sans avoir émis un avis formel, est traditionnellement réservée vis-à-vis de la mise en œuvre d'une telle centralisation. L'utilisation d'un tel fichier par les établissements de crédit pourrait conduire à l'officialisation d'une norme d'endettement qui serait préjudiciable aux ménages les plus modestes et constituer alors un facteur d'exclusion de l'accès au crédit. Enfin, un tel fichier conduirait

à recenser un ménage sur deux, soit près de 12 à 15 millions d'emprunteurs (contre 1,8 million de personnes au FICP) et serait donc très lourd et très coûteux à gérer, alors même que le dispositif préventif mis en place depuis 1998 autour d'un fichier « négatif » a concouru efficacement à la diminution des situations de surendettement liées à l'excès de crédit. Au demeurant, les exemples étrangers n'ont pas prouvé leur efficacité. On ne constate pas dans les pays dotés de fichiers « positifs » de diminution du nombre de personnes en situation de surendettement. Pour l'ensemble de ces raisons, le Gouvernement n'a pas retenu cette proposition dans le cadre de la réforme du dispositif de lutte contre le surendettement présenté dans le projet de loi de rénovation urbaine.

Assemblée nationale

Question nº : 23557 de M. **Warsmann Jean-Luc**, ministère interrogé : Intérieur, ministère attributaire : Culture et Communication
Réponse publiée au *JO* le 29 septembre 2003 (page 7501)

Élections et référendums — Listes électorales. Inscription. Réglementation

Question : M. Jean-Luc Warsmann attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur l'importance du nombre de Français non inscrits sur les listes électorales. Il semblerait en effet qu'il y ait près de 2 millions et demi de personnes qui soient dans ce cas. Il lui demande si des mesures précises sont envisagées afin de réduire ce nombre de manière significative.

Réponse : pour être inscrit sur la liste électorale d'une commune, deux conditions sont nécessaires. Il faut tout d'abord avoir la qualité d'électeur : sont électeurs tous les nationaux français, majeurs, des deux sexes, jouissant de leurs droits civils et politiques. Il faut ensuite avoir une attache avec la commune caractérisée par l'existence d'un domicile, d'une résidence d'au moins six mois ou de l'inscription personnelle au rôle d'une des contributions directes communales depuis au moins cinq ans (article L. 11 du Code électoral). L'inscription d'office sur les listes électorales de tous les électeurs exige donc de disposer de fichiers nationaux spécifiques à chacun des critères précités et de pouvoir les croiser. Or, de tels fichiers n'existent pas. Ainsi, le fichier des cartes nationales d'identité n'est pas « un fichier des citoyens », la carte nationale d'identité n'étant pas obligatoire et aucun fichier ne recense les adresses exactes des Français, faute d'obligation légale de déclaration d'adresse. Le Gouvernement étudie donc d'autres voies de progrès qui respectent strictement les libertés individuelles. Sans attendre l'issue de cette réflexion, le Gouvernement souhaite engager des actions ponctuelles. Parmi les propositions avancées, peuvent être citées la généralisation de la demande d'inscription par correspondance et l'utilisation du fichier de changement d'adresse de La Poste pour rappeler personnellement à chaque électeur qui a changé de lieu de résidence qu'il doit s'inscrire sur les listes électorales. Enfin, des campagnes d'information et de communication sont régulièrement organisées à l'approche d'élections générales.

Sénat

Question n° : 07670 de M. **Trégouët René,** ministère interrogé : Intérieur
Réponse publiée au *JO* le 2 octobre 2003 (page 2978)

Caméras numériques dans les voitures de police

Question : M. René Trégouët attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur les termes d'une dépêche (Reuters) datée du 16 mai 2003 consultable à l'adresse suivante : http://www.yahoo.fr dans la rubrique « actualités — multimédia » intitulé : « Des caméras numériques dans des voitures de police américaines. » On y lit que la police d'une des villes de l'État de Washington a décidé d'équiper ses voitures de caméras numériques pouvant enregistrer et garder en mémoire les images des contrevenants susceptibles d'être déférés à la justice. Il s'agirait pour la police de fournir des preuves au moment des arrestations mais aussi de se protéger d'éventuelles poursuites judiciaires à son encontre (par exemple contre l'accusation récurrente de préjugé raciste avancée par certains contrevenants). Une telle mesure est-elle envisageable en France ? Le Gouvernement a-t-il des intentions à cet égard ? Pour quelles raisons ?

Réponse : l'honorable parlementaire appelle l'attention du ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur un procédé technique qui serait utilisé par une police de l'État de Washington consistant à équiper les véhicules de police de caméras numériques pouvant enregistrer et garder en mémoire les images des contrevenants susceptibles d'être déférés à la justice. Il lui demande s'il serait envisageable en France d'utiliser de tels dispositifs. Afin d'utiliser des techniques d'enregistrement d'images, plusieurs mesures récentes ont été prises. Ainsi la loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, dans la deuxième partie de l'annexe 1, prévoit, parmi les mesures tendant au renforcement de l'efficacité des investigations policières que : *« Afin de faciliter la recherche de preuves en matière de violences urbaines, des dotations de caméras vidéo seront prévues dans les zones sensibles. »* En outre, la loi dispose que *« les textes nécessaires seront adoptés dans le but d'autoriser sous le contrôle judiciaire* [...] *la mise en place de dispositifs de surveillance élaborés rendus nécessaires en raison du recours de plus en plus systématique des délinquants aux possibilités de brouillage de leurs échanges ou aux camouflages de leurs rencontres »*. L'article 26 de la loi du 18 mars 2003 pour la sécurité intérieure prévoit quant à lui l'installation en tous points appropriés du territoire de dispositifs fixes et permanents de contrôle automatisé des données signalétiques des véhicules permettant la vérification au fichier des véhicules volés. Il convient en outre de souligner que la conservation des images des particuliers constitue une information indirectement nominative au sens de l'article 4 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui dispose : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent »*. Dès lors, ce sont toutes les dispositions législatives afférentes à la protection de la vie privée des personnes qui doivent être appliquées aux enregistrements vidéo et notamment celles relatives à la durée de conservation des informations et au droit d'accès. Au surplus, les images qui peuvent être prises concernent non seulement l'auteur de l'infraction mais également d'autres personnes simplement présentes au moment des faits, ce qui peut être de nature à porter atteinte à la vie privée de ces dernières. L'utilisation de ce procédé technique suppose donc de s'entourer de précautions particulières, le tout sous le contrôle de la Commission nationale de l'informatique et des libertés. Il est à noter

qu'en matière d'infractions routières le Gouvernement a choisi de recourir à la présomption de responsabilité du titulaire du certificat d'immatriculation. Cette disposition juridique qui a été introduite par la loi du 18 juin 1999 portant diverses mesures relatives à la sécurité routière, après avoir été validée par le Conseil constitutionnel, permet de sanctionner pécuniairement le titulaire du certificat d'immatriculation sans qu'il soit nécessaire d'apporter la preuve de sa culpabilité personnelle. La responsabilité pécuniaire, depuis la loi du 12 juin 2003 renforçant la lutte contre la violence routière, porte désormais sur l'ensemble des infractions qui peuvent être constatées par des appareils de contrôle automatisé, à savoir les excès de vitesse, le non-respect des signalisations imposant l'arrêt absolu, le non-respect des distances de sécurité et l'usage de voies et chaussées réservées à certaines catégories de véhicules. Ainsi il existe en droit français des dispositions juridiques qui permettent de recourir, dans certaines conditions et quand cela est nécessaire, à des enregistrements vidéo, tout en garantissant le respect de la vie privée des citoyens.

Assemblée nationale

Question n° : 22345 de M. **Bardet Jean**, ministère interrogé : PME, Commerce, Artisanat, Professions libérales et Consommation
Réponse publiée au *JO* le 6 octobre 2003 (page 7690)

Télécommunications — Téléphones portables. Numéros. Confidentialité

Question : M. Jean Bardet appelle l'attention de M. le secrétaire d'État aux Petites et Moyennes entreprises, au Commerce, à l'Artisanat, aux Professions libérales et à la Consommation sur le respect de la confidentialité des numéros de téléphone portable inscrits sur liste rouge par l'opérateur même. Le prestataire de service a, de par le contrat commercial, les coordonnées de tous ses abonnés. De ce fait, il peut profiter de cette situation pour appeler ses clients à des fins publicitaires et commerciales. Il a donc la capacité de ne pas respecter lui-même le service qu'il propose. Il lui demande donc de bien vouloir lui préciser si de tels actes sont permis par la loi.

Réponse : le numéro d'un téléphone portable constitue une donnée à caractère personnel dont la collecte, le traitement et l'utilisation sont régis, d'une part, par les textes de portée générale que sont la loi n° 78-17 du 6 janvier 1978 relative à l'informatique et aux libertés et la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et, d'autre part, par des dispositions sectorielles que sont les articles L. 33-4 et R. 10 et suivants du Code des postes et télécommunications (CPT) relatifs aux annuaires universels et les articles L. 33-4-1 du CPT et L. 121-20-5 du Code de la consommation relatifs aux communications non sollicitées. Ces deux derniers articles vont être prochainement modifiés et complétés par le projet de loi pour la confiance dans l'économie numérique, examiné en première lecture par le Parlement et transposant, notamment, les dispositions de la directive 2002/58/CE relative à la vie privée et aux communications électroniques. L'inscription d'un numéro de téléphone en liste dite « rouge » correspond au droit des personnes à s'opposer à la publication de leurs coordonnées dans les annuaires d'abonnés, imprimés ou électroniques, accessibles au public ou consultables par l'intermédiaire de services de renseignements ou des services d'annuaires inversés et à leur revente à des services marketing. S'agissant de la faculté d'utilisation des coordonnées à des fins de prospection, celle-ci est strictement encadrée, qu'il s'agisse d'une prospection téléphonique classique avec intervention humaine ou d'une prospection par automate d'appel ou par SMS *(Short Message Service)*. Le. projet de loi pour la confiance dans l'économie numérique

pose le principe de l'interdiction de prospection sans le consentement préalable de l'abonné. Ce texte étend au SMS ce régime dit *d'Opt In* déjà en vigueur pour les automates d'appel. Il prévoit cependant, à titre dérogatoire, que les entreprises ayant, ou ayant eu, une relation contractuelle avec un client (ce qui est le cas de l'opérateur fournissant le service téléphonique) peuvent utiliser les coordonnées de ce dernier aux fins de prospection, si l'abonné a été informé de l'éventualité d'une telle utilisation et s'il se voit expressément offrir la possibilité de s'opposer, sans frais et de manière simple, à cette utilisation de ses coordonnées. L'article R. 10-4 du Code des postes et télécommunications, modifié par le décret 2003-752 du 1er août 2003, rappelle également cette dérogation. En conclusion, un opérateur mobile peut prospecter ses abonnés par appel téléphonique classique et par SMS sous réserve, notamment, du respect des principes d'information et de droit d'opposition de la personne concernée. La prospection par automate d'appel n'est quant à elle autorisée qu'avec le consentement préalable de l'abonné.

Assemblée nationale

Question n° : 24194 de M. **Asensi François**, ministère interrogé : Affaires étrangères
Réponse publiée au *JO* le 27 octobre 2003 (page 8171)

États-Unis — Transports aériens. Terrorisme. Droits de l'homme et libertés publiques

Question : M. François Asensi souhaite interroger M. le ministre des Affaires étrangères sur la coopération avec les États-Unis en matière de prévention contre le terrorisme dans le transport aérien. D'ores et déjà, des informations personnelles concernant tous ceux qui désirent se rendre aux États-Unis sont fournies aux autorités américaines. Des informations sur les passagers telles que leur carte de crédit, leur état de santé, leurs préférences alimentaires, leurs voyages précédents peuvent être ainsi livrées à un dispositif de filtrage baptisé CAPPS *(Computer Assisted Passenger Pre-screening)* avant même qu'ils ne montent dans l'avion. En croisant ces informations avec celles détenues par les services de police, le département d'État, le ministère de la Justice et les banques, ce système prétend détecter d'éventuels suspects. Les médias se sont fait l'écho de l'exaspération du public et notamment des pilotes de ligne face à la multiplication des contrôles tatillons de sécurité. Un pilote a même été arrêté et libéré sous caution pour un propos jugé déplacé. Aujourd'hui, un grand mensuel annonce sous le nom de *Total Information Awarness* (TIA), un projet de fichage de la population mondiale. Un hyper-ordinateur ne traiterait pas moins de quarante pages d'informations sur chacun des 6 milliards d'habitants de la planète. Il souhaite savoir de quelle nature sont les accords passés avec l'administration américaine depuis les attentats du 11 septembre 2001 sur la livraison des informations relevant de la vie privée. Il lui demande quelle serait la position de la France face aux demandes répétées de cette administration de disposer de toujours plus d'informations personnelles sur les voyageurs à destination des États-Unis.

Réponse : à la suite des attentats du 11 septembre 2001, les États-Unis ont adopté deux lois, *« l'Aviation and Transportation Security Act »* (novembre 2001) et le *« Enhanced Border Security and Visa Entry Reform Act »* (mai 2002). Pratiquement, les vols à destination du territoire américain sont soumis à l'obligation de transmission préalable des données relatives à l'équipage et aux passagers. Ont été visées dans un premier temps les informations figurant sur le passeport tels le nom, l'adresse, ainsi que l'adresse de séjour aux États-Unis, puis, à partir du 25 juin 2002, les données du système de réservation électronique des compagnies (PNR). Ces don-

nées peuvent comporter des informations personnelles, portant en particulier sur « l'historique » des voyageurs et incluant le cas échéant des éléments sur leur pratique religieuse (régime alimentaire) ou leur santé, nécessaires au bon déroulement du vol. En France et en Europe, ces données sont protégées par la loi. C'est ainsi que la Commission européenne s'est saisie de ce dossier dès 2001, conformément à l'article 25 de la directive 95/46/CE sur la protection des données personnelles. La discussion n'a pu vraiment s'engager avec les États-Unis qu'en décembre 2002. Comme il se doit, les négociations sont conduites sous le contrôle du Conseil. Une phase transitoire, à compter du 5 mars 2003, prévoit l'accès des douanes au « PNR » sous certaines conditions restrictives : limitation aux vols au départ et à destination des États-Unis, utilisation de données uniquement dans le cadre de la lutte contre le terrorisme, conservation des données dans un délai limité, conditions limitatives de partage ou de communication des informations pertinentes avec les autres agences gouvernementales compétentes. La Commission se fonde en l'espèce sur la directive 95/46/CE qui prévoit, à titre de dérogation, le transfert de données personnelles sous conditions. La Commission, par lettre du 6 mai 2003, a également précisé aux compagnies aériennes qu'il leur incombait d'informer les passagers préalablement à la communication des données et également de demander leur consentement. Cependant, les négociations entre l'Union européenne et les États-Unis se poursuivent afin d'aboutir à un accord sur le niveau de protection adéquat des données. Les autorités françaises sont très attachées à la conclusion d'un accord définitif conforme à la directive européenne sur la protection des données et à notre propre législation. L'Union européenne insiste pour que soient garantis les droits d'accès, de rectification et de recours effectif, et encadrés le transfert et l'exploitation des données pour parvenir à un accord définitif. Un tel accord entre les États-Unis et l'Union, qui concilierait la sûreté et les droits de la personne, serait un exemple qui pourrait être étendu à l'ensemble des destinations du trafic aérien.

Sénat

Question n° : 07820 de M. **Trégouët René**, ministère interrogé : Justice
Réponse publiée au *JO* le 30 octobre 2003 (page 3222)

Informatique et libertés

Question : M. René Trégouët attire l'attention de M. le garde des Sceaux, ministre de la Justice, sur l'importance toujours plus grande du traitement automatisé des données dans la vie courante, et particulièrement le phénomène de croisement des fichiers nominatifs à usages multiples. La loi n° 78-17 du 6 janvier 1978, relative à l'informatique et aux libertés, prévoit l'exercice du droit d'accès et de rectification pour chaque citoyen. Elle prévoit également l'engagement de la responsabilité des personnes morales s'étant rendues coupables d'une utilisation illégale de fichiers nominatifs. Les abus existent cependant, qui ne sont pas toujours sanctionnés malgré le rôle joué par la Commission nationale de l'informatique et des libertés. Il lui demande de bien vouloir lui rappeler le nombre d'incidents enregistrés ainsi que le type des infractions les plus couramment relevées, et également de lui préciser si des projets d'amélioration du contrôle de l'utilisation de ces fichiers existent.

Réponse : le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que, dans le contexte de la société de l'information, il ne peut que partager les préoccupations de celui-ci à propos des risques d'abus auxquels peut donner lieu le croisement de fichiers, en particulier s'agissant de l'interconnexion de fichiers à finalité privée. Pour la période allant de 1984 à 2001, seule

période pour laquelle des statistiques sont susceptibles d'être extraites à ce jour du Casier judiciaire national, les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, actuellement sanctionnées par les articles 226-16 à 226-23 du Code pénal, ont donné lieu à la condamnation d'environ soixante-dix personnes, plusieurs infractions à la loi informatique et libertés ayant été en général retenues lors de chacune de ces condamnations. Par ailleurs, la moitié des condamnations prononcées concerne des infractions formelles tenant au non-respect des formalités préalables à la mise en œuvre des traitements. Pour ce qui est des infractions substantielles relatives au non-respect des droits des personnes fichées, les infractions les plus couramment relevées ont trait à la collecte de données nominatives par un moyen frauduleux, déloyal ou illicite, au détournement d'un traitement de sa finalité d'origine, ainsi qu'aux divulgations d'informations portant atteinte à l'intimité de la vie privée de l'intéressé ou à sa considération. Si le nombre total des atteintes pénalement sanctionnées peut paraître faible, il importe de souligner que, s'agissant d'atteintes moins graves mais nombreuses, la Commission nationale de l'informatique et des libertés (CNIL) a joué au cours de la période de référence un rôle de premier plan, en permettant, par ses interventions et ses signalements, de faire cesser ou de prévenir les abus. Il n'en demeure pas moins que les pouvoirs de la CNIL en matière de contrôle *a posteriori* des traitements sont notoirement insuffisants. C'est pourquoi il est prévu de les accroître substantiellement dans le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel en cours d'examen par le Parlement. La CNIL se verra confier par ce texte des prérogatives nouvelles, lui ménageant la possibilité d'investigations approfondies, celle du prononcé de sanctions pécuniaires, si le responsable du traitement ne se conforme pas à une mise en demeure préalable, et de décisions d'interruption provisoire de certains traitements en cas d'urgence, et lui permettant de saisir par la voie du référé le juge compétent en cas d'atteinte grave et immédiate aux droits et libertés.

Sénat

Question n° : 8517 de M. **Lagauche Serge**, ministère interrogé : Intérieur
Réponse publiée au *JO* le 6 novembre 2003 (page 3281)

Mise en œuvre par la police et la gendarmerie d'applications automatisées d'informations nominatives

Question : M. Serge Lagauche attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur la question de la mise en œuvre, par les services de la police et de la gendarmerie nationale, des applications automatisées d'informations nominatives recueillies lors d'enquêtes préliminaires, de flagrance ou exécutées sur commission rogatoire. Plusieurs dispositions de la loi n° 2003-239 du 18 mars 2003 relative à la sécurité intérieure, qui consacre l'existence légale des fichiers de police judiciaire STIC et JUDEX notamment, semblent en effet constituer une atteinte manifeste au principe fondamental de la présomption d'innocence. Ce principe figurant dans la Déclaration des droits de l'homme et du citoyen, et ainsi pourvu d'une valeur constitutionnelle supralégislative, garantit que *« toute personne suspectée ou poursuivie est présumée innocente tant que sa culpabilité n'a pas été établie »* (article préliminaire du Code de procédure pénale). Or, il ressort des termes de la loi que sont susceptibles d'être inscrites sur ces fichiers de police judiciaire, parallèles au casier judiciaire, toutes les personnes, sans limitation d'âge, qui ont été mises en cause lors d'une procédure judiciaire sans qu'il existe impérati-

vement à leur encontre des indices graves ou concordants rendant vraisemblables qu'elles aient pu participer, comme auteurs ou complices, aux infractions en cause. Le champ d'application de la loi relative à la sécurité intérieure est donc si large que celle-ci peut constituer dans son application une atteinte manifeste non seulement au principe de la présomption d'innocence mais également à celui de la protection de la vie privée. En effet, cette loi permet, dans de très nombreuses hypothèses, aux services administratifs de l'État de diligenter des enquêtes administratives donnant lieu à la consultation des fichiers de police judiciaire. Ainsi la Commission nationale de l'informatique et des libertés (CNIL) cite-t-elle dans son dernier rapport d'activité plusieurs exemples où des particuliers l'avaient saisie, parce que leur candidature à des emplois ou à des stages avait été refusée, après que les services chargés de l'enquête administrative aient constaté l'inscription, à tort, sur les fichiers de police judiciaire, de données les concernant. Pour toutes ces raisons, il lui demande de bien vouloir lui faire connaître de quelles manières le Gouvernement compte mettre un terme aux inscriptions et aux consultations abusives de données personnelles figurant dans les fichiers de police judiciaire. Il lui demande également dans quels délais le Gouvernement envisage d'adopter les décrets d'application de la loi relative à la sécurité intérieure, décret devant préciser les modalités pratiques de l'inscription des données personnelles et les conditions de leur accès, dans le respect intégral de la présomption d'innocence, de la vie privée et des libertés individuelles de tous.

Réponse : la loi du 18 mars 2003 pour la sécurité intérieure (LSI) confère une base légale à la mise en œuvre, par les services de police et de gendarmerie, d'applications automatisées d'informations nominatives recueillies au cours des enquêtes de police. Le législateur répond ainsi à l'exigence de sécurité des citoyens en dotant les services chargés de missions de sécurité intérieure des outils nécessaires à l'exercice de ces missions, tout en assurant le respect des libertés individuelles grâce aux garanties fixées pour le fonctionnement de ces fichiers. Parmi les catégories de personnes susceptibles d'être enregistrées, la mis en cause est expressément défini par l'article 21 de la LSI comme la personne à l'encontre de laquelle existent des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer comme auteur ou complice à la commission d'une infraction. Le système de traitement des infractions constatées (STIC) est placé sous le contrôle du procureur de la République, lequel peut demander que les informations nominatives enregistrées soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. En cas de décision de relaxe ou d'acquittement, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas cette décision fait l'objet d'une mention. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite, font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. L'utilisation des fichiers de procédure aux fins d'enquêtes administratives ne constitue pas une nouveauté de la loi précitée pour la sécurité intérieure. Cette disposition est issue en effet de la loi du 15 novembre 2001 relative à la sécurité quotidienne (LSQ) modifiant l'article 17-1 de la loi du 21 janvier 1995, qui en a autorisé le principe. Le décret du 28 mars 2002, pris pour l'application de la LSQ, liste de façon limitative les enquêtes administratives donnant lieu à la consultation des fichiers, dans laquelle ne figurent pas l'attribution de logement, l'embauche ou le suivi de carrière. Ce décret est en effet limité aux enquêtes d'habilitation défense, d'affectation dans les emplois publics et privés liés à la sécurité ou à la défense, d'accès dans les sites sensibles et d'agrément pour l'utilisation de produits et matériels dangereux (armes, munitions, explosifs, matériaux nucléaires etc. La LSI, a en revanche pérennisé

dans le temps les dispositions de la LSQ et n'en a élargi le champ d'application qu'aux enquêtes relatives à la naturalisation et à l'attribution des titres de séjour, aux agréments relevant du domaine des jeux, paris et courses et à la nomination dans les ordres nationaux. En outre, le STIC sera doté, au cours du second semestre 2003, d'une fonction spécifique dédiée aux consultations de police administrative, laquelle permet de restreindre la visibilité de certaines informations : les données nominatives relatives aux victimes ou aux personnes mises en cause ayant bénéficié d'une suite judiciaire favorable (classement sans suite ou non-lieu) seront occultées pour les services de sécurité intérieure. En ce qui concerne les personnels de l'État (autres que policiers et gendarmes) investis de missions de police administrative, la fonction fera l'objet d'adaptations supplémentaires afin de ne restituer qu'une réponse de type « connu inconnu », l'enquête ne pouvant être poursuivie que par un service de police ou de gendarmerie en cas de réponse positive. De façon générale, l'utilisation du STIC est entourée de différentes garanties concernant tant son alimentation que les durées de conservation des données inscrites, la mise à jour de celles-ci, ainsi que le double contrôle exercé sur le traitement par la Commission nationale de l'informatique et des libertés (CNIL) et le procureur de la République. Intégré par ailleurs dans l'architecture informatique du ministère de l'Intérieur, le STIC bénéficie des sécurités techniques qui y sont associées (mot de passe personnel et confidentiel associé au matricule). Seuls les personnels spécialement habilités y ont accès (à ce jour, 75 017 policiers habilités dans 1 288 services, toutes directions d'emploi confondues). Cette habilitation personnelle et individuelle est délivrée par le chef de service qui détermine pour chaque fonctionnaire relevant de son autorité son profil utilisateur (consultation, alimentation, statistique...) correspondant à l'exercice de sa mission (police judiciaire, police administrative, gestionnaire). Les outils d'administration fonctionnelle permettent de mémoriser la trace nominative de toutes les consultations et mises à jour effectuées sur le système. Le détournement d'usage ou l'utilisation illicite est passible de sanctions pénales (articles 226-17 et 226-20 à 226-23 du Code pénal) et disciplinaires (Code de déontologie de la police nationale). Les décrets d'application concernant aussi bien les conditions de mise en œuvre de ces traitements que les modalités d'accès aux informations nominatives dans le cadre d'enquêtes administratives limitativement énumérées sont en cours d'élaboration et devraient en tout état de cause être adoptés d'ici à la fin de l'année. La décision du Conseil constitutionnel le 13 mars 2003 dont le statut garantit l'indépendance et dont les décisions s'imposent aux pouvoirs publics et aux autorités administratives et juridictionnelles a jugé que la loi pour la sécurité intérieure offre suffisamment de garanties pour assurer un juste équilibre entre le respect de la vie privée et la sauvegarde de l'ordre public. En conséquence, l'article 21 de la loi n'est pas contraire à la Constitution, et il n'est nullement dans l'intention du Gouvernement — pas plus que cela ne l'a été de la part de la majorité parlementaire — d'écarter la loi du 6 janvier 1978 de l'application des traitements automatisés d'informations personnelles.

Assemblée nationale

Question n° : 24272 de M. **Raoult Éric**, ministère interrogé : Culture et Communication
Réponse publiée au *JO* le 1er décembre 2003 (page 9182)

Publicité — Internet. Usage abusif

Question : M. Éric Raoult attire l'attention de M. le ministre de la Culture et de la Communication sur la nécessité de réglementer les Spam (ou publicités forcées

par e-mail courriers électroniques). Cette nouvelle forme de diffusion publicitaire encombre la communication électronique par son caractère massif et insidieux. Cette propagation publicitaire est devenue tellement problématique dans un pays comme les États-Unis, que le législateur a déjà commencé à la réglementer et s'apprête à renforcer encore plus la législation américaine en ce domaine. Ce phénomène commençant à se répandre également en France, au détriment de la qualité des échanges électroniques librement menés, il conviendrait donc d'anticiper sur ce phénomène de nuisance d'un genre nouveau. Il lui demande donc ce qu'il compte entreprendre pour réglementer et donc limiter le développement des Spam dans notre pays.

Réponse : l'honorable parlementaire a souhaité attirer l'attention du ministre de la Culture et de la Communication sur la nécessité de réglementer les Spam (ou publicités forcées par e-mails, courriers électroniques). Le Gouvernement a très tôt pris conscience des nuisances susceptibles d'être provoquées par l'envoi massif aux usagers de l'internet de courriers électroniques non sollicités. Du point de vue législatif, il a donc souscrit sans réserve à l'approche européenne, formalisée par la directive 2002/581 CE du 12 juillet 2002 relative au traitement des données à caractère personnel, qui instaure le régime de l'accord préalable *(Opt In)* des consommateurs à l'utilisation de leur adresse mél pour l'envoi de communications électroniques à caractère commercial, transposée en droit national par le projet de loi pour la confiance dans l'économie numérique adopté en première lecture à l'Assemblée nationale le 26 février 2003 et au Sénat le 25 juin 2003. C'est notamment l'article 12 du projet de loi qui renforce la protection des utilisateurs vis-à-vis de la prospection directe effectuée par courrier électronique, tout particulièrement en subordonnant l'envoi de courriers électroniques à des fins commerciales à l'accord préalable du destinataire, et en permettant à la Commission nationale informatique et libertés (CNIL) de recueillir les plaintes relatives au non-respect des dispositions de l'article. Ce régime du consentement préalable de l'utilisateur est un élément essentiel de la protection des utilisateurs français de l'internet contre les courriers électroniques non sollicités. En effet, l'expérience des États-Unis, qui ont privilégié le régime de l'accord a posteriori *(opt out)*, prouve très largement les nuisances susceptibles de découler d'une réglementation trop laxiste de l'usage commercial du courrier électronique. En s'inscrivant dans un dispositif européen cohérent et unifié, le projet de loi pour la confiance dans l'économie numérique clarifiera les règles d'utilisation en France du courrier électronique publicitaire. Il contribuera ainsi à limiter le développement de l'envoi de Spam français. La mise en place d'un cadre législatif adapté est nécessaire, mais n'est pas suffisante aujourd'hui pour protéger les utilisateurs contre les courriers publicitaires massifs provenant d'autres pays que la France et l'Union européenne, et n'y étant pas, par voie de conséquence, soumis. C'est pourquoi, à l'occasion du dernier comité interministériel pour la société de l'information du 10 juillet 2003, le ministre de la Culture et de la Communication a annoncé la création d'un groupe de contact sur le Spam, organisé et animé par la direction du développement des médias. Ce groupe a pour objectifs de susciter le dialogue entre les nombreux acteurs de la lutte contre le Spam en France de contribuer à l'analyse statistique et technique du phénomène en France, et, en partenariat avec le ministère de l'Économie, des Finances et de l'Industrie (mission pour l'économie numérique), de contribuer à l'élaboration des textes réglementaires nécessaires à l'application des dispositions protectrices de la loi pour la confiance dans l'économie numérique, et notamment pour l'organisation des registres d'opposition, les modalités du recueil du consentement, les habilitations nécessaires pour permettre la constatation et la répression du Spam. La direction du développement des médias a déjà engagé des entretiens préliminaires à la constitution du groupe, dont la première réunion devrait

intervenir avant fin janvier 2004. Enfin, la lutte contre le Spam représente un défi d'envergure pour la coopération internationale. Le ministre de la Culture et de la Communication a pris connaissance avec beaucoup d'attention des récentes déclarations sur ce sujet de M. Erkki Likkanen, commissaire européen en charge des entreprises et de la société de l'information, qui invite les pays membres de l'Union européenne et la communauté internationale à s'unir sur ce sujet. Il a également suivi avec intérêt l'évolution des législations nationales des pays qui, comme la France, s'engagent résolument dans la lutte contre le Spam, au nombre desquels la Belgique, l'Allemagne, l'Italie, l'Australie et les États-Unis, qui semblent être, du fait de leur réglementation précitée, les premiers responsables du Spam à l'échelle mondiale. Il est donc convaincu que la lutte contre le Spam, et ce qu'elle représente en termes de protection des libertés individuelles des utilisateurs, doit s'organiser à l'échelle internationale et il va chercher à mobiliser les partenaires de la France autour de l'élaboration d'une initiative internationale commune.

Participation de la CNIL à divers organismes

Organismes européens et internationaux

- Autorité de contrôle commune Europol
- Autorité de contrôle commune Schengen
- Autorité de contrôle commune du système d'information des douanes (SID)
- Comité des recours Europol
- Conférence européenne des commissaires à la protection des données
- Conférence internationale des commissaires à la protection des données
- Formation *ad hoc* du comité assistance mutuelle de l'art 43-5 du règlement du 13 mars 1997 compétente pour tout problème lié au SID
- Groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel, dit « Groupe de l'article 29 » (nombreux sous-groupes de travail)
- Groupe européen de travail sur les plaintes
- Groupe européen de travail sur le Spam
- Groupe de travail international sur la protection des données personnelles dans le secteur des télécommunications, dit « Groupe de Berlin »

Organismes nationaux

- AFNOR

Commission AFNOR Z 43 C « Archivage des données électroniques ». Comité de la marque NF service — « conseil en recrutement »

- Agence pour le développement de l'administration électronique (ADAE) : groupes de travail
- Club de la sécurité des systèmes d'information français (CLUSIF). Groupe de travail sur la sécurité des systèmes d'information de santé
- Commission locale informatique et libertés (Lycée Charles-de-Gaulle de Muret)
- Comité consultatif pour l'agrément des applications du réseau santé-social
- Comité national des registres
- Comité de pilotage de l'accord-cadre ministère de l'Éducation nationale-CNIL
- Conseil consultatif de l'internet
- Conseil national de l'information statistique — comité du label
- Conseil national du sida
- Groupe de travail relatif à la conservation des données de santé à caractère personnel

- Groupe de travail « Principes généraux relatifs à la conservation des documents électroniques » du Forum des droits sur l'internet
- Groupe de travail « Fichiers planétaires et liberté individuelle » (créé par l'association PRESAJE)
- Groupes animés par la direction du développement des médias (DDM)
- Groupe de contact des acteurs de la lutte contre le Spam
- Groupe pour la protection des droits d'auteur

Annexe 8

Le panorama des législations

Le panorama des législations adoptées dans le monde est présenté ci-après en fonction du niveau des garanties qu'elles présentent au regard de la législation européenne :

— les législations des pays de l'Union européenne incluant les pays de l'Europe centrale et orientale, membres de l'Union européenne depuis le 1er mai 2004, qui offrent tous un niveau de protection équivalent, du fait, notamment, de la mise en œuvre de la directive 95/46/CE ;

— les législations des pays de l'Espace économique européen qui, ayant transposé dans leur droit interne la directive 95/46/CE, doivent également être considérés comme accordant un niveau de protection équivalent à celui accordé par les pays membres de l'Union européenne [1] ;

— les pays dits « tiers », c'est-à-dire non-membres de l'Union européenne, ayant fait l'objet d'une décision de la Commission européenne reconnaissant le caractère adéquat de la protection des données dans ces pays. En 2003, l'Argentine et Guernesey ont fait l'objet de telles décisions prises après avis favorable des autorités indépendantes de protection des données (groupe dit « de l'article 29 ») et du comité des États membres (comité « de l'article 31 »). La décision relative à l'Ile de Man est attendue prochainement après avis favorable du G29 ;

— les pays tiers ne rentrant dans aucune des catégories précédemment énoncées mais qui disposent toutefois de législations de protection des données personnelles générales ou sectorielles. Il convient de préciser que des procédures ont été engagées avec la Nouvelle-Zélande et l'Australie mais les lois de protection des données de ce dernier État n'assurent pas, en l'état, la protection des étrangers.

Enfin, ce panorama est complété de la liste des organisations internationales et des instruments internationaux qui régissent la matière.

1 L'Espace économique européen, ou « EEE » (en anglais, *European Economic Area*, abrégé en « EEA ») a été créé en 1992 par accord entre l'Union européenne et l'AELE (Association européenne de libre échange, en anglais, *European Free Trade Association*, ou « EFTA »). Cet accord ne concerne que trois sur quatre des pays de l'AELE, à savoir l'Islande, la Norvège et le Liechtenstein, à l'exception de la Suisse, qui a rejeté l'EEE par référendum en 1992. Les pays de l'EEE se sont engagés à transposer dans leurs législations nationales environ 1 400 textes communautaires. A ce titre, l'Islande, la Norvège et le Liechtenstein ont transposé la directive 95/46/CE dans leur droit interne.

1 — L'Union européenne

Pays	Législation	Autorité de contrôle
Allemagne	◆ Loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement de données, modifiée par la loi fédérale de protection des données du 20 décembre 1990 et amendée par la loi du 14 septembre 1994 ◆ Législations dans les *Länder* ◆ Loi fédérale de protection des données — 2001 (*Bundesdatenschutzgesetz* (BDSG)). Disponible en allemand, anglais et français sur le site web	Der Bundesbeauftragte für den Datenschutz (autorité fédérale) Friedrich Ebert Strasse 1 53173 Bonn Allemagne Site web : www.datenschutz.de
Autriche	◆ Loi fédérale sur la protection des données du 18 octobre 1978, amendée en 1986 ◆ Loi de protection des données — 2000 (*Datenschutzgesetz* 2000 (DSG 2000) Disponible en allemand et en anglais sur le site web	Direktor Buro der Datenschutzkommission und des Datenschutzrater Bundeskanzlerant Ballhausplatz 1 1014 Vienne Autriche Site web : www.bka.gv.at/datenschutz
Belgique	◆ Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992 ◆ Version coordonnée de la loi relative à la protection des données à caractère personnel du 8 décembre 1992 (11 décembre 1998) ◆ Arrêté royal du 13 mars 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection des données personnelles ◆ Loi du 24 février 2003 sur le statut de l'autorité de protection des données	Commission de la protection de la vie privée Ministère de la Justice Boulevard de Waterloo 115 1000 Bruxelles Site web : http://www.privacy.fgov.be/
Chypre	◆ Loi n° 138 (I) 2001 sur le traitement des données personnelles (protection des individus) — 2001	Commission for Personal Data Protection 40 Th Dervis Street 1066 Nicosia Cyprus Site Web : www.dataprotection.gov.cy
Danemark	◆ Loi n° 293 du 8 juin 1978 sur les registres privés et loi n° 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées en 1988 et en 1991 ◆ Loi n° 429, relative au traitement des données personnelles — 2000 (Lov nr. 429 af 31. maj 2000 som ændret ved lov nr. 280 af 25. ap) Disponible en anglais sur le site	Datatilsynet Christians Brygge 28 4 sal 1559 Copenhague Danemark Site web : www.datatilsynet.dk
Espagne	◆ Loi du 29 octobre 1992 réglementant le traitement automatisé de données personnelles ◆ Loi organique de protection des données à caractère personnel — 1999 (Ley Organica 15/99 de Protección de Datos de Carácter Personal) Disponible en anglais sur le site web	Agencia de Protection de Datos C/Sagasta, 22 Madrid 28004 Espagne Site web : www.agpd.es
Estonie	◆ Loi sur la protection des données personnelles — 1997	Estonian Data Protection Inspectorate Väike-Ameerika 19 10129 Tallinn Estonia

Finlande	◆ Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police ◆ Loi de protection des données personnelles — 1999 (Personuppgiftslag 22.4 1999/523) Disponible en anglais sur le site web	Office of the Data Protection Ombudsman Albertinkatu 25 PO Box 315 00181 Helsinki Finlande Site web : www.tietosuoja.fi/index.htm
France	◆ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ◆ Transposition directive 95/46/CE : projet de loi adopté en première lecture par l'Assemblée nationale le 30 janvier 2002 et au Sénat le 1er avril 2003 — deuxième lecture à l'Assemblée nationale en avril 2004	Commission nationale de l'informatique et des libertés 21, rue Saint-Guillaume 75340 Paris cedex 07 Site web : www.cnil.fr
Grèce	◆ Loi n° 2472 sur la protection des personnes à l'égard du traitement des données à caractère personnel — 1997	Hellenic Data Protection Authority Kifisias Avenue 1-3 PC 115 23 Ampelokipi Athènes Grèce Site web : www.dpa.gr
Hongrie	◆ Loi sur la protection des données personnelles et la communication de données publiques — 1992	Parliamentary commissioner for data protection and freedom of information Nádor u. 22. 1051 Budapest Hungary Site web : www.obh.hu
Irlande	◆ Loi sur la protection des données du 13 juillet 1988 ◆ Loi adoptée le 18 février 2002 (European Communities Data Protection Regulations, 2001) (Entrée en vigueur en avril 2002)	Data protection commissioner Block 4, Irish Life Centre Talbot Street — Dublin 1 Irlande Site web : www.dataprivacy.ie
Italie	◆ Loi n° 675 sur la protection des données personnelles — 1996 (modifiée par plusieurs décrets législatifs de 1997, 1998 et 1999) (Legge n. 675 del 31 dicembre 1996 — Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) Disponible en anglais sur le site web	Garante per la protezione dei dati personali Piazza di Monte Citorio n.121 00186 Rome Italie Site web : www.garanteprivacy.it/
Lettonie	◆ Loi sur la protection des données — avril 2000	Data State Inspection Kr. Barona Street 5-4 1050 Riga Latvia Site web : www.dvi.gov.lv/
Lituanie	◆ Loi sur la protection des données personnelles — 1996 amendée en 2000	State Data Protection Inspectorate Gedimino ave.27/2 LT -2600 Vilnius Lithuania Site web : www.is.lt/dsinsp
Luxembourg	◆ Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, amendée en 1992 ◆ Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, disponible en allemand et en anglais sur le site web	Commission nationale pour la protection des données 68, rue de Luxembourg 4221 Esch-sur-Alzette Luxembourg Site web : http://www.cnpd.lu/

Malte	◆ Loi de protection des données personnelles — 2002	Office of the Commissioner for Data Protection Commissioner for Data Protection 280, Republic Street Valletta GPO 01 Malta Site web : www.dataprotection.gov.mt
Pays-Bas	◆ Loi du 28 décembre 1988 sur la protection des données, complétée par une loi du 21 juin 1990 sur les fichiers de police ◆ Loi de protection des données — 2001 (Wet bescherming persoonsgegevens (WBP) 2001). Disponible en anglais sur le site web	Data Protection Authority Prins Clauslaan 20 Postbus 93374 -2509 AJ. S'Gravenhage Pays-Bas Site web : www.cbpweb.nl
Pologne	◆ Loi sur la protection des données personnelles — 1997	Biuro Geneeralnego Inspektora ul. Stawki 2 0193 Warsaw Poland Site web : www.giodo.gov.pl
Portugal	◆ Loi n° 10/91 du 29 avril 1991 sur la protection des données à caractère personnel face à l'informatique, amendée par une loi du 29 août 1994 ◆ Loi n° 67/98 relative à la protection des données à caractère personnel -1998 (Lei da protecçao de dados pessoais n° 67/98) Disponible en français et anglais sur le site web	Comissào Nacional de Potecçào de Dados Informatizados 148, rue de Sao Bento 1200 Lisbonne Portugal Site web : www.cnpd.pt
République tchèque	◆ Loi relative à la protection des données personnelles des systèmes informatisés — 1992 ◆ Loi n° 101/2000 sur la protection des données personnelles — 1er juin 2000	Office for Personal Data Protection Pplk. Sochora 27 170 00 Prague 7 Czech Republic Site web : www.uoou.cz
Royaume-Uni	◆ Loi sur la protection des données du 12 juillet 1988 ◆ Loi de protection des données — 1998 (Data Protection Act 1998) Disponible en anglais sur le site web	The office of information Commissioner Wycliffe House-Water Lane Wilmslow-Cheshire SK9 5AF Royaume-Uni Site web : www.dataprotection.gov.uk
Slovaquie	◆ Loi relative à la protection des données personnelles des systèmes informatisés — 1998 ◆ Loi n° 428 relative à la protection des données — juillet 2002	Office for the Protection of Personal Data Odborárske nám. 3 817 60, Bratislava Slovak Republic Site web : www.dataprotection.gov.sk
Slovénie	◆ Loi n° 210-01/89-3 sur la protection des données — 1999	Namestnik varuha clovekovih pravic Urad varuha clovekovih pravic Dunajska 56 1000 Ljubljana Slovenia
Suède	◆ Loi du 11 mai 1973 sur la protection des données ◆ Loi n° 98/204 sur la protection des données — 1998 (Personuppgiftslagen 1998 : 204) Disponible en anglais sur le site web	Datainspektionen Box 8114 104 20 Stockholm Suède Site web : www.datainspektionen.se

2 — Les pays de l'EEE (Espace économique européen)

Pays	Législation	Autorité de contrôle
Islande	◆ Loi n° 63-1981 relative l'enregistrement de données personnelles — 1981 (Amendée en 1989) ◆ Loi n° 77 du 23 mai 2000	Personuvernd Rauôararstig 10 105 Reykjavik Iceland Site web : www.personuvernd.is
Liechtenstein	◆ Loi sur la protection des données (Datenschutzgesetz) du 14 mars 2002	Data Protection Commissioner of the Principality of Liechtenstein Herrengasse 6 9490 Vaduz — Liechtenstein Site web : www.sds.llv.li
Norvège	◆ Loi sur les registres de données personnelles — 1978 ◆ Loi du 14 avril 2000	Datatilsynet Postboks 8177 Dep 0034 Oslo 1 Norvège Site web : www.datatilsynet.no

3 — Les autres pays tiers dont le niveau de protection est adéquat (article 25 de la directive 95/46/CE)

Pays	Législation et autres textes	Décision d'adéquation de la Commission européenne	Autorité de contrôle / Contacts
Argentine	◆ Loi n 25 326 sur la protection des données personnelles — 2 novembre 2000	Décision n° 2003/1731/CE constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi argentine sur la protection des données à caractère personnel	Direccion Nacional de Datos Personales Sarmiento 329 Piso 5° 1041 Buenos Aires Argentina Site web : www.protecciondedatos.com.ar/
Canada (niveau fédéral)	◆ Loi fédérale sur la protection des renseignements personnels — 1982 ◆ Loi fédérale sur la protection des renseignements personnels et les documents électroniques — 2000	Décision n° 2002/2/CE du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques	Federal privacy commission Tower B, 3rd Floor, 112 Kent Street — Otawa, Ontario K1A 1H3 Canada Site web : www.privcom.gc.ca
États-Unis *(Safe Harbor* uniquement)	◆ Principes internationaux de protection des données au sein du *Safe Harbor*	Décision n° 2000/520/CE du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil, relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique	Federal Trade Commission FTC 600 Pennsylvania Avenue NW DC 25080 Washington USA

Guernesey	◆ Loi sur la protection des données — 1986 ◆ Loi sur la protection des données — 2001 (entrée en vigueur le 1er août 2002)	Décision n° 2003/821/CE du 21 novembre 2003 constatant le niveau de protection adéquat des données à caractère personnel à Guernesey	Data Protection Office Frances House Sir William Place Saint. Peter Port Guernsey GY1 1GX web : www.dpcommission.gov.gg
Suisse	◆ Loi fédérale sur la protection des données — 1992	Décision n° 2000/518/CE du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse	Commissaire à la protection des données Feldeggweg 1 3003 Berne SUISSE Site web : www.edsb.ch

4 — Les autres pays tiers ayant adopté une législation

Pays	Législation	Autorité de contrôle/contacts
Afrique du Sud	◆ Loi de promotion de l'accès à l'information — 2000	
Albanie	◆ Loi n 8517 sur la protection des données personnelles — 1999	
Australie	◆ Loi fédérale sur la vie privée — 1988 (secteur public), amendement visant à étendre la protection des données dans le secteur privé — 6 décembre 2000	Federal Privacy Commission GPO Box 5218 — Sydney NSW 1024 Australia Site web : www.privacy.gov.au
Brésil	◆ Loi réglementaire de l'Habeas Data n° 9507 — 1997	
Bulgarie	◆ Loi de protection des données personnelles — 2002	Bulgarian Commission for Personal Data Protection 1 Dondukov bul. 1000 Sofia Bulgaria
Burkina Faso	◆ Projet de loi portant protection des données à caractère personnel — 2003	
Chili	◆ Loi sur la protection de la vie privée — août 1999	
Corée (sud)	◆ Loi sur la protection des données personnelles — 1994	Korea Information Security Agency 78, Karak dong, Songpa-Gu Seoul 138-160 South Korea
États-Unis	◆ Loi sur la protection des libertés individuelles dans les administrations fédérales — 1974 ◆ Diverses lois sectorielles fédérales relatives à la protection des données Ex : The Fair Credit Reporting Act (FCRA) — 1970 The video privacy protection Act — 1988 Electronic Freedom of Information Act — 1996 Children's Online Privacy Protection Act — 1998 Health Insurance Portability and Accountability Act (HIPAA) — 1996 Financial Services Modernization Act (Gramm-Leach-Bliley) (1999)	Federal Trade Commission FTC 600 Pennsylvania Avenue NW DC 25080 Washington USA

Hong-Kong	◆ Loi sur la protection des données — 1990 ◆ Ordonnance sur la protection des données — 1995	Privacy commission for personal data Unit 2001, 20/F — OfficeTower Convention Plaza -1 Harbour Road Wan Chai — Hong-Kong Site web : www.pco.org.hk
Ile de Man	◆ Loi de protection des données à caractère personnel — 2002 ◆ Avis du Groupe de l'article 29 n° 6/2003 du 21 novembre 2003 relatif au niveau de protection des données à caractère personnel dans l'Ile de Man	Office of Data Protection Supervisor P.O. Box 69 Douglas Isle of Man IM99 1EQ Site web : www.gov.im/odps/
Inde	◆ Loi sur la technologie de l'information — 9 juin 2000	
Israël	◆ Loi n° 5741 sur la protection de la vie privée — 1981 (Amendée en 1985 et 1996) ◆ Loi n 5746 sur la protection des données dans l'administration 1986	Registrar of data bases Hashlocha 2 Yad Eliahu POB 9288 Tel Aviv Israel
Japon	◆ Loi sur la protection des données personnelles informatisées dans le secteur public — 1988 ◆ Projet de lois pour le secteur privé et projet de loi modifiant la loi pour le secteur public — mai 2001 ◆ Loi de protection des informations personnelles — mai 2003	Personal Data Protection Task Force 1-6-1 Nagata Cho Chiyoda-ku 1008914 Tokyo Japon
Jersey	◆ Loi sur la protection des données — 1987	Data protection registry Morier House Halckett Place Saint-Helier Jersey JE1 1DD Site web : www.dataprotection.gov.je/
Monaco	◆ Loi n° 1165 relative aux traitements d'informations nominatives — 1993	Commission de contrôle des informations nominatives Gildor Pastor Center, 7, rue du Gablan Bloc B — Bureau 409 98000 Monaco
Nouvelle-Zélande	◆ Loi sur l'information du secteur public — 17 décembre 1982 ◆ Loi sur la vie privée — 1993	Privacy commission PO Box 466 Auckland Nouvelle-Zélande Site web : www.privacy.org.nz
Paraguay	◆ Loi sur la protection des données — 28 décembre 2000	
République de Macédoine	◆ Loi sur la protection des données personnelles — 1994	
Roumanie	◆ Loi relative à la protection des données à caractère personnel : n° 677/2001 JO n° 790 du 12 décembre 2001	Le Médiateur des Droits de l'homme Str. Eugen Carada, nr. 3 Sector 3 Bucuresti Romania Site web : www.avp.ro/
République de Saint-Marin	◆ Loi relative à la protection des données personnelles — 1983 (Amendée en 1995)	
Russie	◆ Loi fédérale sur l'information, l'informatisation et la protection des informations — 1995	

Taiwan	◆ Loi sur la protection des données — 1995	The ministry of justice 130, Sec 1, Chung Ching South Road Taipei 100 — Taiwan
Thaïlande	◆ Loi sur la protection des données dans le secteur public — 1998	Authority for the protection of Personal Data Information Commission Government House Bangkok 10300 Thailand

5 — Instruments internationaux

Union européenne		
Communauté européenne	◆ Directive européenne n° 95/46/CE relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données — 24 octobre 1995	Commission européenne DG marché intérieur — Unité A4 200 rue de la Loi — Bruxelles B — 1049 Belgique Site web : http://europa.eu.int/comm/internal_market/fr/index.htm
Contrôleur européen à la protection des données	◆ Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données	European Data Protection Supervisor Rue Wiertz 60 B — 1047 Bruxelles
Autorités de contrôle communes : Europol Schengen SID	◆ Convention sur la base de l'article K. 3 du traité sur l'Union européenne portant création d'un office européen de police (convention Europol) Convention d'application de l'accord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes, en date du 19 juin 1990. ◆ Convention du 26 juillet 1995 sur l'emploi de l'informatique dans le domaine des douanes et règlement communautaire n° 515/97 du 13 mars 1997	Secrétariat commun des autorités de contrôle communes 175, rue de la Loi B — 1048 Bruxelles
	◆ Règlement (CE) n° 515/97 du Conseil du 13 mars 1997 relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole (titre V)	Système d'information douanier 175, rue de la Loi B — 1048 Bruxelles
Conseil de l'Europe	◆ Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel — 28 janvier 1981	Conseil de l'Europe Direction des affaires juridiques Section protection des données Avenue de l'Europe 67075 Strasbourg — France Site web : www.legal.coe.int/dataprotection
OCDE	◆ Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel — 23 septembre 1980	OCDE 2, rue André Pascal 75775 Paris cedex 16 Site web : www.oecd.org/index-fr.htm
ONU	◆ Lignes directives pour la réglementation des fichiers informatisés de données à caractère personnel — 1989	Site web : www.unhchr/french/html/intlinst_fr.htm

Les travaux du groupe « article 29 »

En 2003, le groupe dit « de l'article 29 » a adopté et publié les documents suivants, classés selon les missions du groupe (http://europa.eu.int/comm/internal_market/privacy/workingroup_fr.htm) :

• Programme de travail 2003 du groupe article 29 sur la protection des données (10 mars 2003)

• Sixième rapport annuel sur l'état de la protection des personnes à l'égard du traitement des données à caractère personnel et de la vie privée dans l'Union européenne et les pays tiers portant sur l'année 2001 (16 décembre 2003)

Transfert de données à caractère personnel hors de l'Union européenne :

• Avis 2/2004 sur la protection adéquate des données personnelles contenues dans les dossiers des passagers aériens transférés au bureau des douanes et de la protection des frontières des États-Unis (US CBP) (29 janvier 2004) [1] . . . . p. 457

• Avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers (13 juin 2003)[1] . . . . . p. 468

• Avis 5/2003 sur le niveau de protection adéquat des données personnelles en Guernesey (13 juin 2003)

• Avis 6/2003 relatif au niveau de protection des données à caractère personnel dans l'Île de Man (21 novembre 2003)

• Document de travail : transferts de données personnelles vers des pays tiers : application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données (3 juin 2003)

• Avis 8/2003 relatif au projet de clauses contractuelles types présenté par un groupe d'associations commerciales (17 décembre 2003)

Initiatives des institutions européennes :

• Avis 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE (27 février 2004)[1]. . . . . p. 476

• Avis 7/2003 sur la réutilisation des informations émanant du secteur public et protection des données à caractère personnel (12 décembre 2003)

Codes de conduite :

• Avis 3/2003 sur le Code de déontologie européen en matière d'utilisation de données à caractère personnel dans le marketing direct (FEDMA) (13 juin 2003)

Documents d'initiatives du groupe :

• Document de travail sur l'administration électronique (8 mai 2003)

• Document de travail sur la biométrie (1er août 2003)[1]. . . . . p. 484

1 Document complet ci-après.

• Avis 1/2003 sur le stockage des données relatives au trafic à des fins de facturation (29 janvier 2003)

• Document de travail sur la protection des données sur les systèmes d'authentification en ligne (29 janvier 2003)

• Avis 2/2003 sur l'application des principes de protection des données aux répertoires internet « Whois » (13 juin 2003)

AVIS 2/2004 SUR LE NIVEAU DE PROTECTION ADÉQUAT DES DONNÉES À CARACTÈRE PERSONNEL CONTENUES DANS LES DOSSIERS DES PASSAGERS AÉRIENS (PNR) TRANSFÉRÉS AU BUREAU DES DOUANES ET DE LA PROTECTION DES FRONTIÈRES DES ÉTATS-UNIS (US CBP)

Adopté le 29 janvier 2004

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel, institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 [1] ;

Vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3, de ladite directive ;

Vu ses règles de procédure, et notamment leurs articles 12 et 14 ;

A adopté le présent avis :

Introduction

Dans la foulée des événements du 11 septembre 2001, les États-Unis ont adopté un ensemble de lois et de règlements imposant aux compagnies aériennes opérant des vols à destination de leur territoire de transférer aux autorités américaines des données personnelles sur les passagers et les membres d'équipage des vols à destination ou en provenance de ce pays. En particulier, les autorités ont imposé aux compagnies aériennes l'obligation de fournir au bureau américain des douanes et de la protection des frontières (CPB) un accès électronique aux données des passagers figurant dans les fichiers « PNR » pour les vols à destination, en provenance et via les États-Unis. Les compagnies aériennes qui rejettent ces demandes sont susceptibles d'être sanctionnées par de lourdes amendes et même par la perte de leurs droits d'atterrissage, et leurs passagers subiraient des retards à leur arrivée aux États-Unis.

Le groupe de travail a émis un premier avis en octobre 2002 et un deuxième le 13 juin 2003. Ce dernier prenait en considération la déclaration d'engagement des États-Unis du 22 mai 2003 (*Undertakings of the United States Bureau of Customs and Border Protection et the United States Transportation Security Administration*) reflétant le dernier stade du dialogue relatif aux engagements de la partie américaine sur les conditions de traitement des données passagers PNR.

Dans son avis du 13 juin, le groupe de travail a attiré l'attention sur plusieurs questions de protection des données résultant du transfert des données passagers PNR aux autorités américaines. Les principaux points en suspens concernent la finalité des transferts, le principe de proportionnalité en ce qui concerne les données personnelles à transférer ainsi que le moment des transferts et la durée de conservation

1 *Journal officiel* n° L 281 du 23 novembre 1995, p. 31, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

des données, le traitement des données sensibles, l'importance d'adopter une méthode de transfert *Push*, le contrôle strict des transferts ultérieurs vers d'autres administrations ou autorités étrangères, les garanties et les droits des personnes concernées, le mécanisme d'application et de règlement des litiges ainsi que le niveau des engagements.

Plus récemment, le groupe de travail a reçu la communication de la Commission au Conseil et au Parlement intitulée « Transfert des données des dossiers passagers (*Passenger Name Record* — PNR) : une démarche globale de l'Union européenne » [1] et une version actualisée de la déclaration d'engagement américaine datée du 12 janvier 2004 (annexe I).

Conformément à son avis 4/2003, le groupe de travail estime qu'il convient d'émettre un nouvel avis à la lumière des derniers développements concernant le transfert de données passagers PNR, en tenant compte en particulier des résultats des négociations entre la Commission européenne et les autorités américaines.

1. Action contre le terrorisme et protection des libertés et des droits fondamentaux

Comme cela est déjà indiqué dans les avis 6/2002 et 4/2003, les transferts de données à des autorités américaines suscitent des préoccupations publiques, ont des répercussions profondes et sensibles au plan politique et institutionnel et revêtent une dimension internationale.

La lutte contre le terrorisme est un élément à la fois utile et nécessaire dans les sociétés démocratiques. Dans ce combat contre le terrorisme, il convient de protéger les libertés individuelles et des droits fondamentaux, y compris le respect de la vie privée et la protection des données.

Ces droits sont notamment protégés par la directive 95/46/CE ainsi que par l'article 8 de la Convention européenne des droits de l'homme et sont ancrés dans les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. La protection des données est en outre reconnue et renforcée par le projet de constitution européenne discuté par la Convention sur l'avenir de l'Europe.

Aussi les libertés et les droits fondamentaux relatifs aux principes régissant la protection des données à caractère personnel dans l'Union européenne ne doivent-ils être restreints que dans les cas où cela est nécessaire au sein d'une société démocratique ou pour les besoins de la protection des intérêts publics tels qu'ils sont définis exhaustivement dans les instruments susmentionnés.

Compte tenu du volume et de la sensibilité des données concernées ainsi que du nombre d'individus touchés (10 à 11 millions de passagers par an), la demande de communication à une autorité publique de données personnelles collectées à des fins commerciales et figurant dans les bases de données des compagnies aériennes proposant des vols à destination des États-Unis ou transitant par les États-Unis, ainsi que dans les systèmes de réservation connexes, en lui fournissant un accès à ces systèmes, est sans précédent dans l'histoire des relations entre les États-Unis et l'Europe et constitue une exception au principe fondamental de spécification de la finalité en matière de protection des données. Il y a donc lieu de faire preuve de prudence tout en tenant compte également des possibilités d'extraction de données auxquelles cette évolution ouvre la voie, en particulier pour les résidents européens, ainsi que du

1 COM (2003) 826 final.

risque qui en découle en matière de surveillance généralisée et de contrôle par un pays tiers.

De plus, des flux similaires de données des compagnies aériennes ont déjà été demandés et/ou proposés par plusieurs autres pays tiers, ce qui soulève la question de l'égalité de traitement des pays tiers et met en évidence la nécessité d'adopter une approche globale pour l'utilisation des données des transports aériens à des fins de sécurité dans un contexte multilatéral.

Il n'est pas certain que la lutte contre le terrorisme et le maintien de la sécurité intérieure seront plus efficaces en mettant partiellement entre parenthèses les principes de proportionnalité et de minimisation des données, alors que le respect de ces principes constitue une garantie essentielle pour la protection des droits des citoyens et convient davantage aux besoins du développement commercial.

À cet égard, le groupe de travail note que la question du transfert de données passagers PNR se pose également à d'autres pays, ce qui exige une approche globale et uniforme à l'échelle mondiale, c'est-à-dire une harmonisation des solutions envisagées pour différents pays.

Le groupe de travail observe par ailleurs que l'expérience récente acquise par certains pays, et notamment l'Australie, montre que l'on peut apporter une réponse proportionnelle et raisonnable aux exigences légitimes de la sécurité intérieure et de la lutte contre le terrorisme en utilisant des systèmes qui sont compatibles avec les principes fondamentaux du respect de la vie privée et de la protection des données à caractère personnel.

2. Actes législatifs à adopter

Le groupe de travail déduit de la communication que la Commission considère que la définition d'une base juridique de qualité pour le transfert de données « PNR » aux autorités américaines doit passer par une décision de la Commission basée sur l'article 25, paragraphe 6, de la directive 95/46/CE en liaison avec un accord international autorisant les compagnies aériennes à traiter les exigences américaines comme des exigences juridiques au sein de l'UE et enjoignant les États-Unis à la réciprocité et au respect des droits des résidents de l'UE *(Due Process)*. Pour ce faire, la Commission envisage de passer un « accord bilatéral allégé » avec les États-Unis.

Compte tenu de l'absence de documents pertinents et des compétences des États membres en ce qui concerne la mise en œuvre des articles 6 et 7 de la directive 95/46/CE, le groupe de travail n'est pas en mesure d'adopter un avis sur le contenu ainsi que sur la base et la valeur juridiques éventuelles d'un tel accord.

Le groupe de travail souhaiterait souligner, toutefois, que les décisions de la Commission, prises sur la base de l'article 25, paragraphe 6, de la directive, font référence, de par leur nature, à la protection appropriée des données personnelles une fois que celles-ci ont été transférées à un pays tiers, et que, jusqu'à présent, elles ont visé les transferts à des organismes du secteur privé situés dans des pays tiers. Il s'agit là de la première fois qu'un transfert est opéré en raison d'une obligation légale issue d'un pays tiers qui requiert que des sous-traitants opérant à partir de l'Union européenne transfèrent des données à une autorité publique de ce pays tiers, en non-conformité avec les provisions de la directive.

Afin de garantir une base légale certaine à ces transferts, une formule composée d'une décision sur le caractère adéquat de la protection et d'un accord international est envisagée ; celle-ci devra avoir un certain nombre d'effets juridiques. Le groupe de travail considère que, dans la mesure où l'accord international permet de

légitimer une limitation au droit à la vie privée ou une restriction au principe de limitation de la finalité prévu à l'article 6 de la directive, ledit accord devra en tout état de cause respecter les limites posées par l'article 8 de la Convention européenne des droits de l'homme et l'article 13 de la directive.

3. Champ d'application du principe de protection adéquate et d'un éventuel accord : le système CAPPS II et la TSA

Le groupe de travail a expressément exclu le programme CAPPS II et tout autre système capable de réaliser des opérations de traitement de données à grande échelle du champ d'application de son avis 4/2003.

En fait, ces systèmes présentent des différences qualitatives par rapport au simple transfert de données passagers PNR et soulèvent des questions graves qui doivent être clarifiées et de traitées spécifiquement par le groupe de travail, compte tenu des effets généralisés qu'ils auraient sur les droits fondamentaux des personnes concernées.

Le système CAPPS II soulève notamment un certain nombre de questions spécifiques qui appellent non seulement l'attention particulière du groupe de travail, mais aussi des clauses de sauvegarde plus importantes. Toute décision future sur le système CAPPS II devra être spécifiquement étudiée par le groupe de travail et ne devra pas découler d'une extension automatique du champ d'application de la première décision de la Commission sur le niveau de protection adéquat des transferts de données passagers PNR vers les États-Unis.

Par conséquent, étant donné que le groupe de travail n'a été ni informé ni consulté à propos du cadre juridique définitif du système CAPPS II, tout usage de données à caractère personnel par la TSA dans le cadre du système CAPPS II tel qu'il est proposé et tout essai y afférent doit être exclu au présent comme l'avenir du champ d'application de la décision de la Commission. En d'autres termes, les réflexions émises dans le présent avis reposent sur la supposition selon laquelle la décision de la Commission ne sera pas étendue à l'avenir au système CAPPS II, ni directement, ni indirectement par référence à la législation interne des États-Unis. Dans le cas contraire, il y aurait lieu d'émettre dès à présent des observations beaucoup plus critiques.

De ce fait, le groupe de travail recommande à la Commission de préciser, par une clause spécifique de la décision, que les autorités américaines doivent s'abstenir d'utiliser les données passagers PNR transmises par l'UE non seulement pour mettre en œuvre le système CAPPS II, mais aussi pour l'essayer.

Le groupe de travail est d'avis qu'une telle clause devra également s'appliquer à tout autre usage des données sur les passagers européens transmises par les compagnies aériennes dans le cadre d'autres programmes tels que les dispositifs *Terrorism Information Awareness* et *US Visit* ou les programmes de traitement de données biométriques.

4. Niveau des engagements

Le groupe de travail rappelle que toute décision de la Commission ne devra pas reposer sur de simples « engagements » de la part d'autorités administratives, mais sur des engagements qui sont officiellement publiés au niveau du registre fédéral au moins et ayant force exécutoire aux États-Unis. Plus particulièrement, il ne devra pas y avoir de doute quant à l'effet créateur de droits au profit de tierces personnes.

Sur ce point, il est clair que les engagements pris par les États-Unis n'auront pas de force exécutoire du côté des États-Unis. En outre, le nouveau paragraphe 47 ajouté à la fin des engagements clarifie de manière explicite la force exécutoire des

engagements pris par les États-Unis, en disposant qu'ils *« ne sont pas créateurs de droits ou d'avantages au bénéfice de personnes ou de parties, quelles soient privées ou publiques »*.

Le groupe de travail souligne ainsi que le niveau des engagements du côté des États-Unis ne peut pas être considéré comme conforme aux exigences posées dans son avis 4/2003 et considère que cette question est une condition essentielle et devra être adressée avant qu'un accord puisse être formalisé.

5. Aspects spécifiques

Compte tenu du contexte global décrit ci-dessus, les demandes américaines telles qu'elles ressortent de la déclaration d'engagement (version mise à jour du 12 janvier 2004) doivent être évaluées à la lumière des avis émis dans ce domaine par le groupe de travail, en particulier l'avis 4/2003 du 13 juin 2003.

A) Nature transitoire du niveau de protection adéquat

Une durée de trois ans et demi a été suggérée pour l'ensemble des mesures, y compris la déclaration d'engagement, le constat de protection adéquate et l'accord international correspondant.

Le groupe de travail accueille favorablement l'introduction d'une clause de caducité dans l'accord et espère que les trois ans et demi proposés dans son avis 4/2003 seront pris en considération.

B) Limitation de finalité

Le DHS (ministère américain de la Sécurité intérieure) utilisera les données passagers PNR pour les besoins de la CBP, le but étant de prévenir et de combattre :
1) le terrorisme et les crimes liés au terrorisme ;
2) d'autres crimes graves, y compris les crimes organisés qui, par nature, revêtent un caractère transnational ;
3) la fuite d'individus faisant l'objet d'un mandat d'arrêt ou placé en détention pour l'un des crimes visés ci-dessus.

Le groupe de travail note que l'on a donné une description plus ciblée et plus précise de la finalité de l'usage des données « PNR ». Toutefois, la catégorie 2 demeure vague, notamment en ce qui concerne le champ d'application des « autres crimes graves » visés dans la déclaration américaine. De plus, la finalité des mesures reste beaucoup plus vaste que la lutte contre les actes de terrorisme sur laquelle le groupe de travail juge qu'il faut mettre l'accent (avis 4/2003).

C) Liste des données à transférer

Le CPB propose désormais que les transferts de données passagers PNR incluent une liste de trente-quatre éléments informatifs, ce que la Commission a approuvé. Cette liste résulte de l'exclusion de quatre champs de données, (identification des billets gratuits, nombre de bagages, nombre de bagages pour chaque segment, surclassements volontaires/involontaires) de la liste des trente-huit éléments « PNR » figurant à l'annexe B de la déclaration d'engagements du 22 mai 2003 [1].

1 Même si l'annexe B de la déclaration d'engagement du 22 mai 2003 énumère trente-neuf éléments, seuls trente-huit peuvent réellement figurer dans un PNR, puisque l'ancien domaine OSI *(Other Service Information)* ne devrait être utilisé que si un code SSR *(Special Service Request)* n'est pas disponible, conformément au service de réservation IATA — manuel, 20e édition, effectif le 1er juin 2003-31 mai 2003, point 10.3, p. 127.

Le groupe de travail observe que les progrès réalisés en ce qui concerne la liste des données à transmettre sont très minces. En effet, la liste américaine révisée contient toujours les vingt éléments dont le groupe de travail juge le transfert disproportionné et problématique dans son avis 4/2003.

Il convient en outre de noter que les autorités américaines n'ont fait passer le nombre d'éléments à transmettre de trente-huit à trente-quatre qu'en supprimant quatre éléments qui avaient été acceptés par le groupe de travail dans son avis du 13 juin. Pour ce qui est des vingt éléments qui continuent d'être demandés par les autorités américaines même s'ils n'ont pas été acceptés par le groupe de travail, aucune indication ou explication n'a été fournie pour justifier la nécessité de leur traitement ou leur caractère proportionnel et non excessif dans la lutte d'une société démocratique contre le terrorisme.

Le groupe de travail rappelle la liste des dix-neuf éléments acceptés dans son avis du 13 juin 2003, tout ajout à cette liste étant soumis à une vérification stricte des principes de proportionnalité et de minimisation de données.

D) Données sensibles

Le dialogue a notamment permis de faire en sorte que certaines données « PNR » ne seront pas utilisées, mais supprimées par les autorités américaines, sachant à cet égard que l'article 8, paragraphe 1, de la directive renvoie aux « *données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle* ».

La liste des codes et des champs de données à supprimer n'est pas encore disponible. Le groupe de travail tient néanmoins à souligner que si certains codes doivent clairement être supprimés (par exemple ceux qui ont trait aux préférences alimentaires, à l'état de santé ou aux convictions religieuses, tels que « tarif pèlerin », « missionnaire » ou « clergé »), d'autres codes nécessitent un examen approfondi, en particulier les champs « libres » de type « remarques générales » qui sont susceptibles de contenir des données sensibles. Dans leur déclaration d'engagement (version du 12 janvier), les autorités américaines font savoir que ces éléments seraient supprimés par l'utilisation d'une liste de mots « déclencheurs ». Une telle approche ne garantit pas la suppression de l'ensemble des données sensibles figurant dans ces champs. Aussi, la seule solution sûre consisterait à exclure ces champs du transfert, conformément à l'avis 4/2003.

À cet égard, le groupe de travail rappelle son avis du 13 juin 2003 selon lequel le transfert de données sensibles doit être exclu. Il n'est donc pas envisageable de ne procéder à des suppressions qu'après avoir transmis des données sensibles aux autorités américaines. Le groupe de travail invite la Commission à trouver les solutions techniques appropriées (tels que des filtres) afin d'éviter toute transmission de données sensibles aux autorités américaines.

E) Utilisation des données tirées des dossiers passagers PNR

Dans une formule ajoutée à la déclaration, les autorités américaines décrivent les limitations qui existent en ce qui concerne leur accès aux données « tirées » de fichiers « PNR » lesquelles sont susceptibles de révéler certains aspects de la vie d'un passager et risquent d'interférer gravement avec le droit de la personne concernée à une vie privée et familiale, conformément à l'article 8 de la Convention européenne des droits de l'homme. La nouvelle formulation est la suivante : « *Les informations personnelles supplémentaires qui seront recherchées par suite directe de l'examen de données passagers PNR seront obtenues auprès de sources non gou-*

vernementales, uniquement par des voies légales et pour des impératifs légitimes de lutte contre le terrorisme ou d'application de la loi. Par exemple, si un numéro de carte de crédit figure dans un PNR, des informations sur les opérations liées (subpœna) *émis par un grand jury, une ordonnance de tribunal ou tout autre moyen légal. En outre, l'accès aux fichiers liés à des adresses électroniques mentionnées dans un PNR obéira aux exigences de la loi des États-Unis en matière de* subpœnas, *d'ordonnances des tribunaux, de mandats et d'autres procédures légales, en fonction du type d'information recherché ».*

Ces éclaircissements sont les bienvenus. Toutefois, ils ne répondent pas entièrement aux préoccupations du groupe de travail. En particulier, les finalités pour lesquelles les données passagers PNR peuvent être utilisées ne doivent pas inclure d'autres « *impératifs* [...] *d'application de la loi* » non spécifiés. De plus, l'accès aux messageries électroniques et à d'autres informations personnelles tirées d'un fichier « PNR » ne doit s'inscrire que dans le cadre des exigences de procédure visées dans les instruments internationaux de coopération judiciaire et policière. En outre, il doit être clair qu'en cas d'abus, un individu peut intenter un recours devant une autorité indépendante.

F) Période de conservation des données

Le CBP conservera les données passagers PNR aux fins convenues par le CBP pendant trois ans et demi. Les données qui sont consultées manuellement pendant cette période seront conservées dans un fichier de données effacées pendant huit années supplémentaires.

Le groupe de travail note qu'il s'agit là d'une amélioration par rapport aux sept ans initialement proposés dans la déclaration du 22 mai. Une durée de trois ans et demi, reste cependant beaucoup plus longue que la période de « quelques semaines voire quelques mois » telle que la préconise le groupe de travail dans son avis 4/2003. Le groupe de travail doute que le stockage généralisé de l'ensemble des données « PNR » sur des périodes aussi longues puisse être jugé « *proportionnel et nécessaire dans une société démocratique* ».

De plus, la conservation supplémentaire des données pendant huit ans, prévue au simple cas où celles-ci seraient consultées, est disproportionnée dans la mesure où il n'y a pas de lien avec une enquête concrète ou un mandat concernant la personne dont les données sont consultées et qu'il est ainsi possible de dépasser *de facto* la limite de trois ans et demi.

On notera à cet égard qu'il est possible d'envisager des solutions qui sont plus respectueuses des principes de protection des données, mais qui restent efficaces dans la lutte contre la criminalité. L'Australie par exemple a élaboré un système dans le cadre duquel les douanes de ce pays ne conservent ou ne stockent de données sur un passager que si ce dernier a commis un acte illégal ou si les données sont nécessaires pour les besoins d'une enquête concernant un délit présumé.

G) Méthode de transfert

En ce qui concerne la méthode de transfert, le groupe de travail rappelle son avis 4/2003 dans lequel in considère que le seul mécanisme de transfert dont la mise en œuvre ne crée pas de problèmes majeurs est celui du *Push* (par lequel les données sont sélectionnées et transférées par les compagnies aériennes aux administrations américaines) plutôt que celui du *Pull* (par lequel les autorités américaines ont un accès en ligne direct aux bases de données des compagnies aériennes et des systèmes de réservation).

Même si les autorités américaines n'émettent plus d'objection depuis quelques mois sur le système *Push*, le groupe de travail est particulièrement inquiet par le fait que les mécanismes techniques permettant d'appliquer un tel système géré directement par les compagnies aériennes européennes n'aient pas encore été mis en place. Le groupe de travail considère que des mesures concrètes devraient être adoptées d'ici avril 2004 au plus tard et encourage vivement la Commission à prendre sans attendre les mesures nécessaires pour atteindre cet objectif. En outre, le groupe de travail souligne que le niveau de protection assuré par les États-Unis ne pourra pas être considéré comme adéquat sans l'instauration d'un système *push*.

H) Moment du transfert

Dans son avis 4/2003, le groupe de travail estime que les services de l'US CBP devraient recevoir les données relatives à un vol spécifique au plus tôt 48 heures avant le décollage. Après cela, les données ne devraient être mises à jour qu'une seule fois.

Sur ce point, la dernière version de la déclaration est strictement fidèle à la version précédente, qui prévoit un transfert des données 72 heures avant le décollage et un maximum de trois mises à jour.

Le groupe de travail déplore qu'aucune amélioration n'ait été obtenue sur ce point pendant les négociations.

I) Transfert de données passagers PNR vers d'autres autorités administratives ou étrangères

Dans son avis 4/2003, le groupe de travail demande que les autres organes publics habilités à recevoir les données soient identifiés avec précision, ajoutant que tout transfert ultérieur direct ou indirect devra être subordonné à l'acceptation d'engagements spécifiques au moins aussi favorables que ceux qui sont fournis à la Commission par les autorités américaines en ce qui concerne la protection des données transférées. En outre, le nombre d'autorités susceptibles de recevoir des données devra être restreint.

Le groupe de travail note qu'aucune liste globale des autorités auxquelles les données sont susceptibles d'être transférées n'a encore été établie. En outre, le groupe de travail reste préoccupé par les dispositions permettant au CBP de divulguer des données conformément aux *« autres exigences prévues par la loi »*, en particulier si ces dispositions sont envisagées à la lumière des lois et des protocoles d'accord obligeant les États-Unis à partager leurs données avec d'autres pays.

En particulier, le mécanisme visé aux points 29 et 35 de la déclaration diffère sensiblement du principe de limitation de la finalité tel qu'affirmé par le groupe de travail (à savoir la lutte contre le terrorisme et les crimes liés au terrorisme) et même des finalités plus larges telles que définies aux points 1 et 3 de la déclaration.

J) Garanties — droits des personnes concernées

a) Informations claires sur les personnes concernées

Aux termes de l'avis 4/2003, et conformément à l'article 10 de la directive, une information claire et précise devra être fournie aux personnes concernées sur l'identité du responsable du traitement, la finalité du traitement et toute autre information, telle que l'existence d'un droit d'accès et de rectification et les voies de recours effectives qui leur sont ouvertes.

Le groupe de travail note que le CBP fournira des informations aux voyageurs. À cet égard, le groupe de travail observe qu'il sera possible de finaliser rapidement une note d'information type une fois que le cadre juridique aura été fixé de manière plus précise, compte tenu également du projet soumis au groupe de travail.

Il y a toutefois lieu de considérer qu'une note d'information globale peut servir de complément, mais en aucun cas de substitut aux exigences juridiques qui doivent être remplies pour que les transferts de données passagers PNR vers les États-Unis soient légaux.

b) Accès

Dans son avis 4/2003, le groupe de travail souligne la nécessité de garanties réellement applicables, pour ce qui est des règles générales relatives à la liberté d'information (FOIA) afin d'assurer que ces dernières ne seront pas utilisées par des tiers pour accéder à des données passagers PNR détenues pas l'administration américaine. Dans ces circonstances, il est important d'empêcher une possible discrimination entre citoyens et d'assurer que le droit d'accès des personnes concernées est mis en œuvre de manière générale et non ambiguë.

En ce qui concerne l'accès des tierces parties, le groupe de travail accueille favorablement les éclaircissements fournis par le CBP dans le document *Exemptions under the Freedom of Information Act (FOIA) Applicable to Passenger Name Record (PNR) Data*.

Néanmoins, pour ce qui est de l'accès des passagers à leurs propres données, le groupe de travail continue d'avoir des craintes quant à la façon dont certaines exemptions pourraient être utilisées pour faire opposition aux droits d'une personne concernée, permettant ainsi à l'administration de lui refuser l'accès à ses données.

En outre, le groupe de travail souligne que le droit d'accès des personnes concernées n'a pas été explicitement étendu, alors que cela est préconisé dans l'avis 4/2003, aux nouvelles données susceptibles d'être générée par le traitement des données transmises depuis l'Europe (profil de risque, listes d'exclusion, etc.).

c) Rectification

Dans son avis 4/2003, le groupe de travail insiste sur l'importance de fournir aux personnes concernées un mécanisme efficace pour obtenir la rectification de leurs données. Le groupe de travail note que le champ d'application de la loi américaine sur la vie privée *(US Privacy Act)* est limité aux résidents américains. Aussi la question de la non-discrimination des résidents européens par rapport aux citoyens américains n'est-elle toujours pas résolue et il convient de déterminer si le mécanisme de rectification exposé dans la déclaration peut être considéré comme un outil efficace et juridiquement contraignant en ce qui concerne le droit de rectification que le FOIA accorde aux citoyens américains et aux résidents étrangers.

d) Recours

Le *DHS Privacy Office* est convenu d'examiner rapidement les plaintes qui lui seront adressées par les autorités chargées de la protection des données dans les États membres pour le compte d'un résident de l'UE estimant que le DHS, y compris son *Privacy Office*, n'a pas traité sa plainte à sa satisfaction.

Le groupe de travail accueille favorablement cette évolution. Il est important qu'une personne puisse obtenir une aide qualifiée dans certains cas ; toutefois, la question relative à l'indépendance réelle du *Chief Privacy Officer*, telle qu'elle est soulevée dans l'avis 4/2003 du groupe, n'a pas encore été résolue. Les membres du groupe de travail considèrent que les dispositions internes qu'ils ont prises en ce qui concerne les fonctions de « panel » visés dans la FAQ 5 de l'accord sur la sphère de sécurité peuvent être utiles dans ce contexte. Ils étudieront les corrections qu'il conviendra éventuellement d'y apporter en vue d'une application dans le contexte des « PNR ».

Le groupe de travail déplore en revanche que les passagers n'aient pas la garantie de pouvoir s'adresser dans tous les cas à un mécanisme de recours véritablement indépendant en cas de litige avec le DHS. En outre, il apparaît maintenant que la déclaration ne se traduira peut-être pas par des effets juridiques contraignants ou des obligations dont la mise en œuvre peut être exigée devant un tribunal (*cf.* point I ci-dessus). Cette lacune reste importante en comparaison des droits dont jouit tout individu dont les données sont traitées dans l'UE, indépendamment de sa nationalité.

K) Audits

La nouvelle formulation suivante a été incluse dans la déclaration d'engagement (paragraphe 43) : *« Le CBP, conjointement avec le ministère de la Sécurité intérieure, s'engage à participer une fois par an, ou plus souvent si cela est convenu entre les parties, à une révision conjointe avec la Commission assistée au besoin d'experts des États membres de l'UE* [1] *concernant la mise en* œuvre des présents engagements afin de contribuer au bon fonctionnement des modalités détaillées dans la présente déclaration. Cette révision commune peut porter sur les résultats du rapport annuel adressé au Congrès par le haut responsable de la vie privée auprès du ministère de la Sécurité intérieure (conformément au paragraphe 42 de la présente déclaration) et, dans la mesure autorisée par ce haut responsable, sur toute enquête réalisée au cours de la période sous-revue ou sur tout constat concernant, en particulier, la sécurité des données, le partage des PNR avec les autorités désignées et l'accès du personnel au PNR dans les bases de données concernées, ainsi que le traitement des plaintes. Dans la mesure où le haut responsable l'autorise, la révision commune peut porter aussi sur la mise en œuvre des présents engagements, de même que sur tout aspect susceptible d'améliorer les modalités d'utilisation des données passagers PNR aux fins visées au paragraphe 3 de la présente déclaration d'engagement ».

Il s'agit là d'une autre évolution favorable et le groupe de travail attend de ces révisions qu'elles soient menées avec l'ouverture et la transparence nécessaires pour en assurer l'efficacité. En tout état de cause, les membres du groupe de travail s'engagent à participer le cas échéant à toute révision de ce type et à observer les règles de confidentialité convenues par les deux parties. Le groupe de travail se réserve évidemment le droit de réétudier cette question, s'il le juge nécessaire, quel que soit le calendrier des révisions.

L) Croisement de fichiers

Les événements récents montrent qu'un nouvel élément doit être pris en considération en plus de ceux qui ont été mentionnés ci-dessus. Les données passagers PNR collectées par le CBP sont comparées aux États-Unis à des listes de personnes recherchées. Ces opérations de croisement de fichiers sont à l'origine de l'annulation à la dernière minute de plusieurs vols en provenance de l'UE. Les informations fournies ultérieurement au public montrent que ces annulations étaient dues à des erreurs

1 Chaque partie devra, au préalable, informer l'autre de la composition de sa délégation, qui pourra regrouper des responsables des autorités compétentes en matière de protection des données ou de la vie privée, des autorités douanières et d'autres autorités policières ou en charge de la sécurité des frontières et des transports aériens. Les autorités participantes seront tenues au secret des délibérations et recevront les autorisations nécessaires. Cette exigence de confidentialité ne fera cependant pas obstacle à ce que chaque partie rende compte comme il se doit des résultats de la révision commune aux autorités nationales compétentes, y compris le Congrès des États-Unis et le Parlement européen. Les deux parties arrêteront d'un commun accord les modalités détaillées de la révision.

ou à des cas de confusion d'identité ou d'homonymie avec des personnes suspectées de terrorisme.

Ces circonstances s'inscrivent dans le cadre de la qualité des données et du principe de protection des données. Le groupe de travail considère que d'autres initiatives doivent être prises pour éviter d'exposer les passagers, les membres d'équipage et les compagnies aériennes à ce type de problèmes.

Conclusion

Le groupe de travail rappelle que l'objectif global, conformément à ce qu'il indique dans son avis 4/2003, est l'établissement d'un cadre légal clair pour que tout transfert de données des compagnies aériennes vers les États-Unis soit compatible avec les principes de protection des données personnelles. Le groupe de travail a pris bonne note des progrès réalisés dans le dialogue États-Unis/Union européenne en ce qui concerne les données passagers PNR, notamment la dernière déclaration du 12 janvier 2004 récemment présentée par l'administration américaine et se réjouit des améliorations qu'elle comporte par rapport à la version précédente.

De l'avis du groupe de travail toutefois, les progrès limités qui ont été enregistrés ne permettent pas de juger qu'un niveau adéquat de protection des données est atteint. Le groupe de travail estime que toute solution devra respecter au moins les principes suivants de protection des données :

- **Qualité des données :**

— le transfert de données doit uniquement avoir pour finalité la lutte contre les actes de terrorisme et certains crimes en rapport avec le terrorisme (à définir) ;
— la liste des données à transférer doit être proportionnelle et ne pas être excessive ;
— les croisements de données par rapport à celles d'individus suspects doivent respecter des normes de qualité élevée assurant une certitude de résultat ;
— les périodes de conservation des données doivent être courtes et proportionnelles ;
— les données des passagers ne doivent pas être utilisées pour mettre en œuvre et/ou tester le système CAPPS II ou des systèmes similaires.

- Les **données sensibles** ne doivent pas être transmises.

- **Droits des personnes concernées :**

— il convient de transmettre des informations claires, actuelles et compréhensibles aux passagers ;
— un droit d'accès et de rectification doit être accordé sans discrimination ;
— il y a lieu de prévoir des dispositions satisfaisantes garantissant aux passagers le droit de s'adresser à un organe de recours véritablement indépendant.

- **Niveau d'engagement des autorités américaines :**

— les engagements pris par la partie américaine doivent avoir un caractère juridique pleinement contraignant pour les États-Unis ;
— il y a lieu de clarifier le champ d'application, la base juridique et la valeur d'un éventuel « accord international allégé ».

- Les **transferts ultérieurs** de données passagers PNR à d'autres gouvernements ou organes étrangers doivent être strictement limités.

- **Méthode de transfert** : il convient de mettre en place une méthode de transfert *Push*, par laquelle les données sont sélectionnées et transférées par les compagnies aériennes aux administrations américaines.

AVIS 4/2003 SUR LE NIVEAU DE PROTECTION ASSURÉ AUX ÉTATS-UNIS POUR LA TRANSMISSION DES DONNÉES PASSAGERS

Adopté le 13 juin 2003

[Traduction non certifiée]

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel, établi par la directive 95/46/ECCE du Parlement européen et du Conseil du 24 octobre 1995 [1] ;

Vu l'article 29 et l'article 30, paragraphes 1 (a) et 3 de ladite directive ;

Vu son règlement intérieur, notamment les articles 12 et 14 ;

A adopté le présent avis :

Introduction

Dans la foulée des événements du 11 septembre 2001, les États-Unis ont adopté plusieurs lois et règlements imposant aux compagnies aériennes opérant des vols à destination de leur territoire de transférer à l'administration américaine les données personnelles relatives aux passagers et membres d'équipage des vols à partir ou à destination de ce pays.

Dans un précédent avis publié en octobre 2002 [2], le groupe de travail a considéré que le respect par les compagnies aériennes des exigences américaines posait problème au regard de la directive 95/46/CE sur la protection des données personnelles [3] et a appelé à la recherche d'une approche commune au niveau de l'Union européenne. Une recommandation spécifique a été adressée à la Commission européenne pour qu'elle ouvre des négociations avec les USA afin de résoudre ce problème.

Le groupe de travail a été tenu au courant par la Commission des progrès relatifs aux discussions qu'elle a menées en vue d'établir les conditions qui lui permettraient d'adopter une décision reconnaissant la « protection adéquate » sur la base de l'article 25 (6) de la directive 95/46/CE et a également obtenu des informations en ayant l'opportunité de discuter des exigences américaines avec des hauts fonctionnaires du département de la sécurité nationale *(Departement of Homeland Security)* lors d'une réunion le 5 mai.

En particulier, le groupe de travail a reçu de la Commission européenne un document, daté du 22 mai 2003, contenant des engagements *(Undertakings)* émis par le bureau américain des douanes et de la protection des frontières et l'administration américaine pour la sécurité des transports *(United States Customs and Border Protection Bureau* et *United States Transportation Security Administration)* [4]. Il reconnaît que ces *Undertakings* sont le résultat actuel des négociations qui ont lieu entre l'administration américaine et la Commission et que la Commission demande encore aux États-Unis de faire des progrès sur certains points.

1 *Journal officiel* n° L 281 du 23 novembre 1995, p. 31, disponible sur le site : http://europa.eu.int/comm/internal_market/fr/dataprot/index.htm

2 Avis 6/2002 du groupe de travail sur la « transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis ».

3 Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

4 Ci-après dénommés les *Undertakings* dans cet avis.

Le présent avis concerne le niveau de protection assuré par les États-Unis d'Amérique après transmission par les compagnies aériennes des données personnelles relatives à leurs passagers et membres d'équipage sur la base de leur législation et de leurs engagements internationaux, tels que décrits dans les *Undertakings* et établis par la législation pertinente. Le groupe de travail s'est basé sur les critères généraux, relatifs à l'évaluation du caractère adéquat de la protection contenus dans des documents antérieurs [1] et dans un précédent avis sur le sujet des données APIS/PNR exigées par les États-Unis [2].

Cet avis est adopté dans un contexte où les États-Unis requièrent de l'Union européenne ou directement des États membres de nombreux transferts de données personnelles (visa…).

En outre, le groupe de travail est parfaitement conscient que des transferts similaires en provenance des compagnies aériennes ont déjà été exigés et/ou proposés par d'autres pays tiers. Cela soulève le problème de la non-discrimination entre États tiers et le besoin d'une évaluation globale, qui pourrait servir de solution type pour les autres pays susceptibles de faire l'objet d'exigences similaires. Le groupe de travail souligne la nécessité de fournir un cadre à la circulation dans le monde d'informations personnelles pour des finalités liées à la sécurité en relation avec les transports aériens.

1. Lutte contre le terrorisme et protection des droits et libertés fondamentaux

Le problème en question relatif à la transmission de données par les compagnies aériennes aux autorités américaines soulève des inquiétudes publiques et a des conséquences larges et sensibles en termes politiques et institutionnels, en plus d'une dimension internationale.

La lutte contre le terrorisme est une composante à la fois nécessaire et précieuse des sociétés démocratiques. Dans ce combat contre le terrorisme, le respect des droits fondamentaux et des libertés individuelles, y compris le droit à la vie privée et la protection des données personnelles, doit être assuré [3].

Ces droits sont notamment protégés par la directive 95/46/CE, l'article 8 de la Convention européenne des droits de l'homme [4] et sont inclus dans les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne [5]. La protection des données est de plus reconnue et développée dans le projet de Constitution européenne discutée au sein de la Convention sur le futur de l'Europe.

Les exigences légitimes de sécurité intérieure aux États-Unis ne doivent pas interférer avec ces principes fondamentaux. Les restrictions aux droits et libertés fondamentaux relatifs aux traitements des données personnelles dans l'Union européenne ne devraient être prises que si elles sont nécessaires dans une société

1 Document de travail du groupe sur les « transferts de données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données » publié le 24 juillet 1998 (WP 12).

2 Avis 6/2002 du groupe de travail sur la « transmission aux États-Unis d'informations relatives aux passagers et autres données de lignes aériennes » publié le 24 octobre 2002 (WP 66).

3 Voir l'opinion 10/2001 « sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme et la criminalité ».

4 Voir aussi jurisprudence pertinente de la Cour européenne des droits de l'homme.

5 La Commission européenne s'est engagée à respecter la chartre. Voir la communication de la Commission sur la nature de la charte des droits fondamentaux de l'Union européenne (COM (2000) 559 final).

démocratique et pour la protection d'intérêts publics énumérés de manière exhaustive dans ces instruments [1].

2. Remarques générales

La portée du présent avis se rapporte à la protection des droits et libertés fondamentaux relatifs aux traitements de données personnelles.

Cet avis est délivré par le groupe de travail dans le but d'évaluer l'adéquation de la protection fournie par les États-Unis en rapport avec les futures décisions de la Commission ou les autres instruments légaux relatifs à cette question. Le groupe de travail se réserve le droit de formuler un nouvel avis, si le présent avis n'était pas correctement pris en compte ou si des changements substantiels apparaissaient lors de négociations futures, justifiant un examen spécifique.

Le groupe de travail observe que les circonstances mentionnées dans les *Undertakings* requièrent une analyse précise en vue de déterminer l'adéquation de la protection qu'elles garantissent aux données personnelles.

Le choix entre différents mécanismes de transfert des données (accès direct des autorités américaines aux bases de données des compagnies aériennes versus la communication pro-active des données par les compagnies aériennes) ne soulève pas seulement des problèmes techniques mais aussi, de manière plus significative, des questions de proportionnalité.

Cela signifie également que les demandes formulées par les autorités américaines excèdent les pouvoirs conférés actuellement aux autorités policières et judiciaires européennes et/ou aux autorités en charge des questions liées à l'immigration ou même des services de renseignement et de sécurité lorsqu'elles entreprennent des activités similaires au sein du territoire de l'Union européenne.

Les problèmes en question affectent également la coopération judiciaire et policière et devraient donc être considérés à la lumière des garanties établies dans les récentes versions provisoires des accords entre l'Union européenne et les États-Unis relatifs à la coopération, à l'assistance mutuelle et à l'extradition.

La collecte des données enregistrées dans les bases de données des compagnies aériennes et requises par les États-Unis couvre un grand nombre de passagers (estimé au moins à 10/11 millions par année), ce qui souligne la nécessité d'une approche prudente, en ayant à l'esprit les possibilités que cela ouvre pour l'exploitation de données affectant, en particulier, les citoyens européens et entraînant le risque d'une surveillance et d'un contrôle généralisés de la part d'un État tiers. Par conséquent, les demandes provenant des administrations américaines doivent faire l'objet de la plus grande attention.

3. Nature transitoire d'une décision d'adéquation

La portée des transferts de données est liée aux graves circonstances internationales récentes. Le groupe de travail recommande que des réévaluations soient faites périodiquement et à court terme pour déterminer si la nécessité de tels transferts perdure. Si ces circonstances internationales venaient à changer, il serait nécessaire de revoir la situation. Le groupe de travail recommande à la Commission d'inclure dans sa décision des clauses prévoyant une « limitation automatique d'effectivité »

1 Voir les intérêts énumérés dans l'article 13 de la directive 95/46/CE.

(Sunset Limitation) et, dans tous les cas, réévaluer la situation à l'issue d'un délai de trois ans.

En outre, si les garanties fournies par l'administration américaine ne sont pas correctement mises en œuvre, une réévaluation de la situation sera nécessaire. Pour cette raison, il est essentiel qu'un rapport sur l'utilisation exacte des données aux États-Unis soit régulièrement soumis par la Commission dans le cadre de la mise en œuvre de la protection aux États-Unis. Cela devrait permettre la vérification des conditions de traitement aux États-Unis, afin de vérifier que les hypothèses qui ont sous-tendu la décision de la Commission restent valables.

4. Le cadre réglementaire américain

Le groupe de travail considère que toute décision de la Commission reconnaissant la protection fournie comme adéquate, ainsi que tout autre instrument établissant un cadre légal pour les transferts de données, doit être basée sur une image claire et précise du droit américain primaire et dérivé gouvernant les finalités, mécanismes et raisons de l'utilisation des données aux États-Unis et les entités autorisées à accéder à ces données.

Une image complète du cadre réglementaire américain applicable et pertinent devrait être incluse en annexe à toute décision de la Commission afin de remplir les exigences d'ouverture et de transparence envers les citoyens européens. De plus, un mécanisme assurant que toute innovation législative pertinente sera communiquée à la Commission devrait être prévu. Il est nécessaire d'éviter que d'autres législations, y compris celles antérieures à la décision de la Commission (les *Undertakings* créent un très large mandat pour l'utilisation et la divulgation des données « lorsque cela est requis par la loi »), ou celles contredisant l'interprétation ou l'application des instruments adoptés par les États-Unis, particulièrement en ce qui concerne CAPPS II et la collecte de données biométriques [1], aboutissent à un changement unilatéral et substantiel des conditions américaines constituant la base d'une décision d'adéquation.

En outre, il est essentiel que la décision ne repose pas sur de simples engagements des agences administratives destinés à supporter certaines interprétations au niveau national (*cf.* le point 11).

Une évaluation de l'adéquation de la protection ne peut pas être faite en ce qui concerne les secteurs de l'administration américaine dont le cadre réglementaire relatif au traitement des données PNR ne peut être considéré comme stable ou suffisamment clair quant aux règles d'accès aux données et au droit de traiter celles-ci. Le groupe de travail fait référence en particulier aux points des *Undertakings* relatifs à l'administration pour la sécurité des transports (*Transportation Security Administration*, TSA) et son programme CAPPS II. L'évaluation de l'adéquation du niveau de protection ne devrait pas non plus couvrir ces systèmes capables de procéder à des opérations de traitement de masse des données, et dont le fonctionnement et les caractéristiques actuels soulèvent de vastes questions devant encore être clarifiées, en particulier l'initiative *Terrorism Information Awareness*.

Dans ces circonstances, le groupe de travail met en avant le besoin d'éviter une situation où TSA ou d'autres agences opérant des systèmes de traitement de masse de données recevraient indirectement les données. Dans le cas où des don-

1 Par conséquent, les questions relatives à la collecte de données biométriques envisagée à partir d'octobre 2004 pour la délivrance des visas devront être considérées à un stade ultérieur.

nées seraient transmises à de tels systèmes, une évaluation additionnelle et spécifique du niveau de protection serait exigée.

5. Méthode de transfert et problèmes légaux

En ce qui concerne la base légale, point particulièrement mis en avant par la résolution du Parlement européen du 13 mars 2003, le groupe de travail est d'avis qu'étant donné la complexité des problèmes juridiques entourant la légalité de la communication des données à des tiers et leur transfert dans des pays tiers, il pourrait être nécessaire — prenant en compte la directive 95/46/CE dans son ensemble — qu'un avis favorable de la Commission en application de l'article 25 (6) de la directive soit accompagné d'un engagement formel pris par les États-Unis à la fin des négociations.

Le groupe de travail fait référence à la base légale en supposant que, eu égard aux éventuelles différences techniques, le seul mécanisme de transfert de données dont la mise en œuvre ne crée pas de problèmes majeurs est celui du *Push* — par lequel les données sont sélectionnées et transférées par les compagnies aériennes aux administrations américaines — plutôt que celui du *Pull* — par lequel les autorités américaines ont un accès en ligne direct aux bases de données des compagnies aériennes et des systèmes de réservation.

En plus d'être plus respectueux du principe selon lequel les données personnelles doivent être pertinentes et non excessives (article 6 de la directive), de comporter moins de problèmes relatifs à la sécurité des données et de rendre superflus certains mécanismes de filtrage de l'accès américain, le système *Push* rendrait inutile l'application aux autorités américaines des mesures nationales prises pour la transposition de la directive — qui seraient par contre nécessaires si un système *Pull* était adopté. En effet, dans ce dernier cas, la directive dans sa totalité, et notamment les articles 4, 6 et 13, pourrait être considérée comme directement et totalement applicable aux administrations américaines. En outre, le système *Push* est la seule solution permettant d'assurer que les règles relatives à la responsabilité établies par la directive 95/46/CE soient correctement appliquées.

Le groupe de travail est donc satisfait de remarquer que les États-Unis ne voient aucune objection à la mise en place d'un système *Push*. Cette solution devrait être substituée dès que possible au mécanisme actuel.

6. Finalités

Les finalités pour lesquelles les données seront utilisées devraient être limitées à la lutte contre les actes terroristes sans être étendues à d'autres graves crimes et délits (*Serious Criminal Offences*) non déterminés. Une liste précise et limitée des graves crimes et délits ayant un lien direct avec le terrorisme devrait être fournie par les États-Unis, sans préjuger de la possibilité de procéder à des échanges de données supplémentaires spécifiques et individualisés dans le cadre de la coopération judiciaire et policière.

Une clarification est aussi nécessaire quant aux autres entités publiques autorisées à recevoir les données, étant donné qu'elles ne sont toujours pas identifiées. L'identification exacte de ces organismes publics et de leurs missions ou, alternativement, pour les autorités précisément identifiables tels que les organismes judiciaires, une description fonctionnelle de ceux-ci devrait être précisée. Il est en tout cas nécessaire de rendre tout à fait clair le fait que les données ne pourront être communiquées à d'autres autorités que lorsque cela est indispensable dans des cas spécifiques de

lutte contre les graves crimes et délits ayant un lien direct avec le terrorisme et que l'utilisation ultérieure de ces données continuera d'être limitée de la même manière.

Des éclaircissements sont également nécessaires quant aux organismes publics et aux procédures desdits organismes opérant les *No Fly List* et *Watch List*, auxquelles sont confrontées les données PNR.

Le groupe de travail doute de la justification de la communication des données sur le fondement de la protection des intérêts vitaux de la personne concernée ou d'autres personnes, car cela augmenterait de manière significative la possibilité de transferts additionnels de données. D'autres voies semblent possibles afin de satisfaire ces demandes.

Pour ce qui est des autorités d'autres pays tiers, sans préjuger de la possibilité de procéder à des échanges de données supplémentaires spécifiques et individualisés dans le cadre de la coopération judiciaire et policière, tout transfert ultérieur direct ou indirect devrait être subordonné à l'acceptation d'engagements spécifiques au moins aussi favorables que ceux fournis à la Commission par les autorités américaines en ce qui concerne la protection des données transférées.

7. Proportionnalité

La proportionnalité devrait être assurée non seulement au regard des finalités et du type d'infraction devant être surveillée, mais aussi en fonction d'autres questions concernant les domaines suivants :

Données personnelles transférables

Le groupe de travail considère que le volume de données devant être transférées [1] va bien au-delà de ce qui pourrait être estimé adéquat, pertinent et non excessif (article 6 (1) (c) de la directive). L'accès à l'ensemble des données PNR est excessif. Les données devraient inclure les informations suivantes : PNR *Record Locator Code*, date de réservation, date (s) prévue (s) du voyage, nom du passager, autres noms présents dans le PNR, l'itinéraire de voyage, identifiants de billets gratuits, billets aller simple, *Ticketing Field Information*, données « ATFQ *(Automatic Ticket Fare Quote)* », numéro de billet, date à laquelle le billet a été délivré, *No Show History*, nombre de bagages, numéros des étiquettes de bagages, *Go Show Information*, nombre de bagages sur chaque segment, changements de classe volontaires ou involontaires, détail des changements effectués sur les données PNR et concernant les éléments mentionnés précédemment.

Le droit primaire américain exigeant que les compagnies aériennes fournissent les données PNR sur demande n'oblige pas les autorités américaines concernées à exiger les données, encore moins à exiger qu'elles soient transférées de manière systématique. En outre, les autorités américaines en question pourraient limiter le nombre de données PNR qu'elles demandent aux compagnies aériennes de leur transmettre. Les autorités américaines interprètent donc leur mandat légal d'une manière excessivement large.

Le groupe de travail estime nécessaire de prendre en compte les différentes sources d'information que les autorités américaines ont à leur disposition ou tentent d'obtenir dans leurs efforts pour acquérir des informations relatives aux étrangers, telles que les données fournies par les formalités d'immigration, les données APIS etc.

1 Voir l 'Annexe B des *Undertakings*.

Les échanges supplémentaires de données dans le cadre de la coopération judiciaire et policière devraient également être pris en compte dans ce contexte.

Le transfert de ce qui peut être regardé, de manière large, comme des données sensibles — protégées par l'article 8 de la directive — devrait être interdit. En outre, le transfert de données SSR — qui sont actuellement traitées de manière optionnelle par certains systèmes de réservation — ne semble pas être proportionnel, en particulier au regard des initiatives entreprises par IATA pour mettre à jour le manuel pertinent, qui en est à sa 20e édition. Ceci est également valable pour les données OSI (informations relatives aux autres services), les champs d'écriture libre ou ouverts (tels que les « remarques générales » où des données d'une nature équivoque peuvent être présentes), et l'information relative aux grands voyageurs *(Frequent Flyers)* et aux « données comportementales » *(Behavioural Data)*.

Une liste claire et exhaustive des données transférées sur la base de la décision de la Commission devrait être attachée en tant qu'annexe avec le tableau auquel il est fait référence au point 4).

Moment du transfert des données

Le groupe de travail est d'avis que le bureau américain des douanes et de la protection des frontières (US CBP) devrait recevoir les données relatives à un vol spécifique au plus tôt 48 heures avant le décollage. Après cela, les données ne devraient être mises à jour qu'une seule fois.

Durée de conservation des données

Le groupe de travail doute de l'efficacité, pour des finalités d'enquêtes, d'une durée excessivement longue de conservation des données concernant des millions d'individus. Les données personnelles ne devraient pas être conservées pour une durée supérieure à ce qui est nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Ainsi, seule la conservation des données transférées conformément à la finalité d'entrée sur le territoire américain dans l'optique de détecter des actes terroristes peut être acceptée. Les données ne devraient être conservées que pour une période courte n'excédant pas quelques semaines voire quelques mois suivant l'entrée sur le territoire américain. Une durée de sept ou huit ans ne peut pas être considérée comme justifiée. Une période courte semblerait plus adaptée à l'acquittement des tâches difficiles dont il est question, tout en étant considérablement moins onéreux. Ceci ne préjuge évidemment pas du possible besoin de continuer le traitement de manière transitoire dans des cas individuels lorsque des motifs spécifiques et bien établis requièrent un examen attentif de certaines personnes, dans le but de prendre des mesures liées à leur participation actuelle et/ou potentielle dans des activités terroristes.

8. Sous contractants

Le groupe de travail souligne la nécessité de prévoir le même niveau de responsabilité pour les sous contractants et leurs employés que pour les fonctionnaires américains, afin d'assurer que les garanties fournies soient maintenues.

9. Garanties — droits des personnes concernées

L'un des principes de base d'un système offrant une protection adéquate des données personnelles est que la personne concernée soit informée et soit à même d'exercer ses droits d'une manière simple, rapide et effective.

Information

Les personnes concernées devraient être informées de manière claire et précise au sujet de leurs droits, en particulier le droit d'accès et de rectification, ainsi que des voies de recours effectives qui leur sont ouvertes.

Accès

Le groupe de travail souligne la nécessité de garanties réellement applicables, pour ce qui est des règles générales relatives à la liberté d'information (FOIA) afin d'assurer que ces dernières ne seront pas utilisées par des tiers pour accéder à des données PNR détenues par l'administration américaine. Dans ces circonstances, il est important d'empêcher une possible discrimination entre citoyens et d'assurer que le droit d'accès des personnes concernées est mis en œuvre de manière générale et non ambiguë.

Les *Undertakings* fournis par les autorités américaines soulèvent des inquiétudes quant à la manière dont des exceptions peuvent être invoquées à l'encontre des personnes concernées afin de permettre à l'administration de leur refuser l'accès aux données.

Le groupe de travail est d'avis que le droit d'accès des personnes concernées devrait être étendu à toutes les données nouvelles générées par les traitements auxquels sont soumises les données d'origine transférées depuis l'Europe (tels que profils de risque, listes d'exclusion...).

Rectification

Étant donné que le champ d'application de la loi américaine sur la vie privée *(US Privacy Act)* est limité aux résidents américains, le groupe de travail souligne l'importance de garantir aux personnes concernées un mécanisme efficace pour obtenir la rectification de leurs données.

10. Mise en œuvre et résolution des litiges

Aide et assistance aux individus en temps approprié/contrôle et recours indépendants

La protection assurée devrait prévoir pour les personnes concernées une aide et une assistance rapides et individualisées relatives à l'exercice de leurs droits ainsi qu'un recours indépendant et approprié en leur faveur.

Le groupe de travail observe l'existence de défauts majeurs concernant la mise en œuvre et le contrôle par des tierces parties indépendantes de l'application des *Undertakings*. Les mécanismes disponibles pour le moment se limitent à des audits et au contrôle interne du *Chief Privacy Officer*. De plus, il existe des incertitudes sur la manière dont les *Undertakings* peuvent produire des effets juridiques contraignants et être source d'obligations pouvant donner lieu à des plaintes devant des tribunaux (*cf.* le point 11 ci-dessous).

En outre, le groupe de travail prend note du besoin d'obtenir plus d'informations sur l'organisme de contrôle indépendant gérant les *No Fly List* et *Watch List* ainsi que sur la logique sous-tendant le mécanisme de surveillance *(Profile Mechanism)*.

Audits

Il devrait exister un moyen d'assurer un niveau satisfaisant de respect des garanties relatives à la protection des données. Dans ces circonstances, le groupe de travail souligne l'importance de la mise à la disposition du public des résultats de certains audits. Les rapports publics devraient mentionner la quantité et le volume des demandes de communication des données PNR effectuées par les autres organismes

publics américains ainsi que la quantité, le volume et les raisons justificatives des demandes de transferts ayant obtenu l'autorisation des destinataires originaux des données.

11. Niveau des engagements

Le groupe de travail souligne la nécessité d'obtenir de la part des États-Unis des engagements qui soient publiés officiellement au moins au niveau du registre fédéral *(Federal Register)* et soient totalement contraignants pour eux. En particulier, il ne devrait y avoir aucune ambiguïté quant à leur capacité de créer des droits en faveur de tiers. Cela soulève le problème de savoir quelle autorité précise engagera la partie américaine. La directive 95/46/CE prévoit en effet qu'une décision reconnaissant comme adéquate la protection assurée par un pays tiers à des données transférées doit être basée sur sa loi interne et/ou sur les engagements internationaux qu'il a souscrits.

Conclusion

Cet avis rend compte des inquiétudes du groupe de travail, du point de vue de la protection des données, lors de l'évaluation de la protection assurée aux États-Unis en perspective d'une éventuelle décision de la Commission. L'objectif global est l'établissement, aussi vite que possible, d'un cadre légal clair pour que tout transfert de données des compagnies aériennes vers les États-Unis soit fait d'une manière conforme aux principes aux principes de protection des données personnelles. Tout en reconnaissant que des décisions politiques seront nécessaires en dernier lieu, le groupe de travail hâte la Commission de prendre pleinement en compte ses opinions durant les négociations qu'elle mène avec les autorités américaines.

Le groupe de travail est conscient qu'une évaluation plus globale des conditions d'utilisation des données relatives au trafic aérien pour des raisons de sécurité pourrait être nécessaire dans un contexte multilatéral.

AVIS 5/2004 PORTANT SUR LES COMMUNICATIONS DE PROSPECTION DIRECTE NON SOLLICITÉES SELON L'ARTICLE 13 DE LA DIRECTIVE 2002/58/CE

Adopté le 27 février 2004

[Traduction non certifiée]

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel, établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 [1] ;

Vu l'article 29 et l'article 30, paragraphes 1 (a) et 3 de ladite directive ;

Vu son règlement intérieur, notamment les articles 12 et 14 ;

A adopté le présent avis :

1 *Journal officiel* n° L 281 du 23 novembre 1995, p. 31, disponible au site : http : //europa.eu.int/comm/internal_market/privacy/law_fr.htm

Introduction

La directive 2002/58/CE portant sur la vie privée et les communications électroniques a harmonisé les conditions dans lesquelles les communications électroniques (par ex. courrier électronique, SMS, télécopieur, téléphone) peuvent être utilisées à des fins de prospection directe [1]. Bien que le présent document attire l'attention sur ces conditions, le groupe de travail observe que d'autres dispositions de la directive nécessiteront une attention particulière à l'avenir.

Se basant sur les règles d'acceptation existantes dans certains États membres, l'article 13 de la directive 2002/58/CE a introduit un régime harmonisé pour les communications à des fins de prospection directe envers les personnes physiques.

Il est évident qu'en dépit de cette harmonisation, certains aspects mentionnés à l'article 13 de la directive 2002/58/CE sur les communications non sollicitées semblent sujets à diverses interprétations.

Conformément à l'article 15 (3) de la directive 2002/58/CE et à l'article 30 de la directive 95/46/CE, le groupe de travail a étudié plus attentivement ces aspects et adopté le présent avis afin de contribuer à une application uniforme des mesures nationales selon la directive 2002/58/CE. Il est à noter que les communications à des fins de prospection directe ont été abordées dans de précédents documents du groupe de travail [2].

Aperçu des questions soulevées dans le présent avis

La règle d'acceptation nécessite le consentement des abonnés avant l'utilisation d'automates d'appel, de courriers électroniques, y compris les SMS, ou de télécopies à des fins de prospection directe.

Il existe une exception pour les communications envoyées aux clients existants, ces communications étant sujettes à certaines conditions (voir ci-dessous). Pour les appels par téléphonie vocale (fixe et mobile) autres que ceux effectués par automates d'appel, les États membres peuvent choisir entre un système d'acceptation et un système d'opposition [3].

En outre, l'expéditeur pour le compte duquel les communications sont réalisées ne doit pas camoufler ni dissimuler son identité. Une adresse valable à laquelle le destinataire peut transmettre une demande visant à obtenir que ces communications cessent doit également être disponible. [4]

Le groupe de travail a décidé d'émettre un avis sur les éléments suivants de ce nouveau régime :

— la notion de courrier électronique ;

1 La Directive doit être transposée d'ici le 31 octobre 2003.

2 Voir par exemple l'avis 7/2000 sur la proposition de la Commission européenne d'une directive du Parlement européen et du Conseil concernant le traitement des données personnelles et la protection de la vie privée dans le domaine des communications électroniques du 12 juillet 2000 ; recommandation 2/2001 portant sur certaines exigences minimums à respecter pour la collecte d'informations personnelles en ligne dans l'Union européenne.

3 Paragraphe 3 de l'article 13 : *« 3. Les États membres prennent les mesures appropriées pour que, sans frais pour l'abonné, les communications non sollicitées par celui-ci et effectuées à des fins de prospection directe, dans les cas autres que ceux visés aux paragraphes 1 et 2 ne soient pas autorisées, soit sans le consentement des abonnés concernés, soit à l'égard des abonnés qui ne souhaitent pas recevoir ces communications, le choix entre ces deux solutions étant régi par la législation nationale ».*

4 Le paragraphe 4 de la directive 2002/58/CE stipule :*« 4. Dans tous les cas, il est interdit d'émettre des messages électroniques à des fins de prospection directe en camouflant ou en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer d'adresse valable à laquelle le destinataire peut transmettre une demande visant à obtenir que ces communications cessent ».*

— la notion de consentement préalable des abonnées ;
— la notion de prospection directe ;
— l'exception à la règle d'acceptation ;
— le régime des communications avec des personnes morales.

Questions soulevées

La notion de courrier électronique

Alors que les notions de télécopieurs (fax) ou de systèmes automatisés d'appels sans intervention humaine (automates d'appel) étaient déjà mentionnées dans la directive 97/66/CE, qui précédait la directive 2002/58/CE, la notion de « courrier électronique » est nouvelle et mérite une attention particulière.

La définition du courrier électronique est la suivante (voir article 2 (h) de la directive 2002/58/CE) : « *Tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère* ».

En résumé, tout message transmis par communication électronique où la participation simultanée de l'expéditeur et du destinataire n'est pas requise est compris dans la notion de courrier électronique.

Cette définition est vaste et volontairement neutre sur le plan technologique. L'objectif était d'adapter la directive précédente de la directive 2002/58/CE [1] à « *l'évolution des marchés et des technologies des services de communications électroniques afin de garantir un niveau égal de protection des données à caractère personnel et de la vie privée aux utilisateurs de services de communications électroniques accessibles au public, indépendamment des technologies utilisées* ». (Considérant 4 de la directive 2002/58/CE).

En guise d'illustration, les services actuellement compris dans la définition du courrier électronique comprennent : le courrier SMTP *(Simple Mail Transport Protocol)*, c'est-à-dire le « courrier électronique » classique ; le service de messages courts ou « SMS » (le considérant 40 de la directive 2002/58/CE indique clairement que le courrier électronique inclut également les SMS) ; le service de messages multimédias ou « MMS » ; les messages laissés sur répondeurs [2] ; les systèmes de messagerie vocale y compris sur les services mobiles ; les communications *Net Send* adressées directement à une adresse IP. Les bulletins d'information envoyés par courrier électronique tombent également dans le champ d'application de cette définition. Cette liste ne peut être considérée comme exhaustive et peut devoir être révisée en considération de développements technologiques et des marchés.

Consentement préalable

La règle d'acceptation est basée sur le consentement préalable comme le précise le paragraphe 1 de l'article 13 de la directive 2002/58/CE : *« 1. L'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable ».*

1 Directive 97/66CE, *JO* L 24, 30 janvier 1998.

2 Il est à noter que certains fournisseurs de services offrent la traduction de SMS en messages vocaux. Si le message résulte d'un appel manuel et n'est pas conservé comme message électronique, l'article 13 (3) s'applique.

Cependant, conformément à l'article 2 (f) et au considérant 17, *« le consentement d'un utilisateur ou d'un abonné, que ce dernier soit une personne physique ou morale, devrait avoir le même sens que le consentement de la personne concernée tel que défini et précisé davantage par la directive 95/46/CE.* [...] *».*

La directive 95/46/CE définit le consentement de la personne concernée comme *« toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».* (Article 2 (h) de la directive 95/46/CE).

Le consentement dans ce contexte n'est pas spécifique aux communications à des fins de prospection directe. On peut faire référence à la recommandation 2/2001 du groupe de travail sur certaines exigences minimums à respecter pour la collecte d'informations personnelles en ligne dans l'Union européenne [1].

Conformément au droit communautaire, le consentement peut être donné de différentes manières. La méthode effective pour obtenir ce consentement n'a pas été spécifiquement prévue dans la directive 2002/58/CE.

Le considérant 17 réaffirme cela : *«* [...] *Le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site internet ».*

Sans préjudice des autres exigences applicables, relatives, par exemple, à l'information sur les finalités de la collecte, les modalités par lesquelles un abonné donne son consentement préalable en s'enregistrant sur un site Internet et à qui l'on demande par la suite de confirmer qu'il était bien la personne s'étant enregistrée et de confirmer son consentement semblent compatibles avec la directive. D'autres modalités peuvent également être compatibles avec les dispositions légales.

Par contraste, la simple demande de consentement pour recevoir des courriers électroniques commerciaux par un courrier électronique général envoyé aux destinataires ne serait pas compatible avec l'article 13 de la directive 2002/58/CE, afin de respecter l'exigence selon laquelle la finalité doit être légitime, explicite, et spécifique.

Un consentement « libre, spécifique et informé » implique également que le consentement donné à l'occasion de l'acceptation des conditions générales gouvernant le contrat principal éventuel, doit respecter les exigences de la directive 95/46/CE, à savoir, être informé, spécifique et libre. Si ces dernières conditions sont remplies, le consentement de la personne concernée peut être donné par exemple, en cochant une case.

Un consentement présumé à recevoir des messages électroniques n'est pas non plus conforme à la définition du consentement de la directive 95/46/CE et en particulier à l'exigence selon laquelle le consentement consiste en l'indication du souhait d'une personne, même si celui-là était prévu « sauf opposition » *Opt Out*. Dans le même ordre d'idées, les cases « pré-cochées », par exemple sur des sites web, ne sont pas davantage compatibles avec la définition de la directive.

La ou les finalité (s) du traitement doivent également être clairement indiquées. Ceci implique que les biens et services, ou les catégories de biens et services, pour lesquels des messages de prospection directe pourraient être envoyés aux fins de prospection directe, doivent être clairement indiqués à l'abonné. Le consentement

1 Document WP 43, adopté le 17 mai 2001. On peut également se référer au premier rapport sur la mise en œuvre de la directive sur la protection des données (95/46/CE (COM (2003) 265 final, p. 18).

à communiquer des données personnelles à des tiers devra également être obtenu le cas échéant. L'information fournie à la personne concernée devra alors inclure les biens et services (ou catégories de biens et services) pour lesquels les tiers procéderaient à l'envoi de courriers électroniques à des fins de prospection.

Le groupe de travail souhaiterait inviter les entreprises (par ex. via les associations professionnelles telles que la Fédération du marketing direct européen (FEDMA)) à insérer dans leurs codes de conduite, et à favoriser, des modalités particulières pour obtenir le consentement conformément au droit communautaire. Le groupe de travail demande aux entreprises de porter particulièrement attention aux systèmes susceptibles d'offrir de meilleures garanties que le consentement a été véritablement et effectivement donné par l'abonné.

De plus, de tels codes devraient inclure une obligation de traiter effectivement les plaintes qui leur sont adressées par les destinataires de messages électroniques. Conformément à l'article 30 de la directive 95/46/CE, le groupe de travail rappelle également qu'il peut émettre un avis sur les codes de conduite établis au niveau européen.

Des éléments pratiques tels que des indications spécifiques, dans les en-tête peuvent également être envisagés dans ces codes de conduite de sorte que les courriers électroniques conformes au code puissent être facilement identifiés par les utilisateurs (et les éventuels filtres) [1].

Listes d'adresses électroniques

Les listes qui n'ont pas été établies moyennant le consentement préalable ne peuvent plus en principe être utilisées sous le régime de l'*opt in*, du moins jusqu'à ce qu'elles soient adaptées aux nouvelles exigences. Vendre de telles listes incompatibles n'est pas davantage légal. Les entreprises souhaitant acheter des listes d'adresses électroniques doivent faire attention à ce que ces listes soient conformes aux exigences applicables, et en particulier à l'exigence de consentement préalable donné en conformité avec ces exigences.

Autres conditions

Alors qu'aucune méthode particulière ne peut être prévue pour donner son consentement — pour accepter — à recevoir des courriers électroniques, les conditions fixées dans le droit communautaire doivent être respectées. Le groupe de travail souhaite rappeler que les conditions de la directive générale 95/46/CE portant sur le traitement des informations personnelles doivent être respectées. Ces conditions impliquent notamment, conformément à l'article 10 de la directive 95/46/CE, la nécessité d'informer au moment de la collecte des informations au moins des éléments suivants :

— l'identité du contrôleur ou de son représentant le cas échéant ;
— les objectifs de la collecte des informations.

Il est également requis de fournir aux personnes physiques des informations sur les destinataires ou catégories de destinataires des données, que les réponses aux questions soient obligatoires ou facultatives, ainsi que sur les conséquences possibles d'une non-réponse, et sur l'existence du droit d'accès et de rectification des données dans la mesure où de telles informations sont nécessaires, en raison des circonstances particulières dans lesquelles les données sont collectées, afin de garantir

1 Sur ce point, on peut faire référence à la disposition de la directive sur le commerce électronique selon laquelle les 'communications commerciales'doivent être clairement identifiables (voir article 6 (a) de la directive 2000/31/CE).

un traitement juste du point de vue de la personne concernée (voir article 10 de la directive 95/46/CE).

Il faut également noter que l'article 13 prévoit aussi l'obligation de donner une possibilité d'opposition sur chaque message envoyé. Cette opposition doit pouvoir être faite en utilisant le même service de communication (par exemple, en envoyant un SMS pour se retirer d'une liste de prospection par SMS).

En outre, le groupe de travail rappelle que la « cueillette de courriers électroniques » (*e-mail harvesting*), à savoir la collecte automatique d'informations personnelles sur les espaces publics sur internet (par ex., le web, les espaces de discussion, etc.) est illégale selon la directive « générale » 95/46/CE. En particulier, celle-ci constitue un traitement de données personnelles déloyales et ne respecte ni le principe de limitation des finalités (finalité) ni l'obligation d'information susmentionnée. Cela s'applique aussi à la collecte automatique des informations par logiciel. Ces points ont fait l'objet de discussions dans le document de travail intitulé *La vie privée sur internet — Une approche intégrée de l'UE sur la protection des données en ligne* [1].

Sous réserve de toute autre exigence supplémentaire émanant d'une législation relative à la commercialisation ou à la vente de produits ou services (spécifiques) (par ex. : produits et services financiers, produits et services de santé, vente à distance).

La notion de prospection directe

Il n'existe aucune définition de la prospection directe ni dans les directives spécifiques de protection des données ni dans les directives générales. On trouve cependant une description des finalités de prospection dans le considérant 30 de la directive 95/46/CE, qui stipule que : « [...] *les États membres peuvent de même préciser les conditions dans lesquelles la communication à des tiers de données à caractère personnel peut être effectuée à des fins de prospection commerciale, ou de prospection faite par une association à but caritatif ou par d'autres associations ou fondations, par exemple à caractère politique, dans le respect de dispositions visant à permettre aux personnes concernées de s'opposer sans devoir indiquer leurs motifs et sans frais au traitement des données les concernant* ».

L'avis du groupe de travail est que l'article 13 de la directive 2002/58/CE englobe par conséquent toute forme de promotion des ventes, y compris la prospection directe réalisée par les associations caritatives et les organisations politiques (par ex. : collecte de fonds, etc.).

Il est à noter qu'une définition large a été utilisée dans le code de bonne pratique de la Fédération du marketing direct européen (FEDMA) pour l'utilisation des informations personnelles dans le marketing direct, qui a été approuvé par le groupe de travail le 13 juin 2003 [2].

1 Document N° WP 37, adopté le 21 novembre 2000.

2 Voir Avis 3/2003 du groupe de travail relatif au code de bonne pratique de la Fédération du marketing direct européen (FEDMA) pour l'utilisation des informations personnelles dans le marketing direct, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77_en.pdf. Le Code FEDMA est disponible à l'adresse suivante :
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77-annex_en.pdf
Ce code définit le marketing direct comme « *La communication par quelque moyen que ce soit (comprenant de manière non limitative le courrier, la télécopie, le téléphone, les services en lignes, etc.) de toute offre de publicité ou marketing, qui est réalisée par le professionnel même ou sous sa responsabilité et qui s'adresse à des particuliers* ».

Communication avec des personnes morales

Le paragraphe 5 de l'article 13 de la directive 2002/58/CE stipule : *« 5. Les paragraphes 1 et 3 s'appliquent aux abonnés qui sont des personnes physiques. Les États membres veillent également, dans le cadre du droit communautaire et des législations nationales applicables, à ce que les intérêts légitimes des abonnés autres que les personnes physiques soient suffisamment protégés en ce qui concerne les communications non sollicitées ».*

En d'autres termes, bien que les États membres doivent toujours garantir que les intérêts légitimes des personnes morales soient suffisamment protégés, ils restent libres de déterminer les protections appropriées pour y parvenir.

En 2002, un certain nombre d'États membres — cinq sur huit — disposant d'un régime d'acceptation pour les courriers électroniques avait choisi d'appliquer le même régime aux personnes morales [1]. Bien que la différence entre les personnes physiques et les personnes morales semble relativement nette, elle n'est pas toujours facile à faire en pratique.

Une situation simple serait celle où des coordonnées électroniques ont été communiquées par un destinataire potentiel, par ex. : sur un site internet ou autre. Il peut alors être assez facile de demander la nature de la personne, par ex. : par une simple question, ou de demander en qualité de quoi la personne a laissé ces informations.

Il s'agit néanmoins d'un élément important dans la mesure où il incombe à l'expéditeur de garantir que les règles soient respectées. En particulier dans ces États membres qui distinguent les communications à des personnes morales et à des personnes physiques, le groupe de travail est d'avis que des règles pratiques doivent être développées.

Bien qu'il devienne nécessaire d'accorder plus d'attention à ce sujet spécifique sur la base de l'exécution par les États membres de l'article 13, le groupe de travail souhaite actuellement soulever les problèmes suivants :
— de telles règles pratiques doivent tenir compte des effets transfrontaliers. Une question soulevée à cet égard concerne la règle à appliquer aux courriers électroniques provenant d'un État membre n'offrant pas de protections pour les personnes morales et reçu dans un État membre offrant le même niveau de protection aux personnes morales et aux personnes physiques ;
— demeure la question de savoir comment l'expéditeur peut déterminer si un destinataire est une personne physique ou morale. En d'autres termes, quels seront les efforts à consentir pour un expéditeur afin de vérifier si le numéro/l'adresse appartient réellement à une personne morale ? Une grande prudence est nécessaire à partir du moment où l'expéditeur n'a pas l'assurance que l'adresse appartient à une personne morale (« secretariat@entreprise.com »). De nombreuses personnes physiques utilisent en effet des pseudonymes ou des termes génériques dans le cadre de leur adresse électronique, sans se trouver pour autant privées de la protection de la directive ;
— un autre problème est lié aux adresses de courrier électronique de personnes qui ne sont pas les abonnés directs du service de communication électronique. Ce peut être le cas par exemple des membres d'une famille ou des employés travaillant pour une entreprise déterminée. Dans le cas où un membre d'une famille ou une société donnerait à d'autres membres de la famille ou à ses employées des adresses de courrier électronique contenant leur nom (par ex. : nom.prénom@entreprise.com), ces

1 Huitième rapport d'exécution de la Commission européenne, décembre 2002.

personnes ne seraient pas en principe des abonnés et ne bénéficieraient pas de la protection de la directive [1]. Certains États membres ont décidé d'appliquer le régime d'*Opt In* à de telles adresses.

Les États membres sont invités à porter attention au fait que des informations personnelles sont incluses dans ce genre d'adresses et doivent être protégées en tant que tel.

De l'avis du groupe de travail, une telle protection implique que l'envoi de courriers électroniques de prospection, liés ou non à des finalités professionnelles, à une adresse de courrier électronique « personnelle » doit être considéré comme de la prospection envers des personnes physiques. En tout état de cause, les dispositions de la directive 95/46/CE relative à la protection de la vie privée devraient être prises en compte.

L'exception des produits et services analogues

Le paragraphe 2 de l'article 13 prévoit une exception harmonisée à la règle d'acceptation qui s'applique aux clients existants, laquelle est soumise à certaines conditions.

« 2. Nonobstant le paragraphe 1, lorsque, dans le respect de la directive 95/46/CE, une personne physique ou morale a, dans le cadre d'une vente d'un produit ou d'un service, obtenu directement de ses clients leurs coordonnées électroniques en vue d'un courrier électronique, ladite personne physique ou morale peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues qu'elle-même fournit pour autant que les lesdits clients se voient donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques lorsqu'elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation ».

Le considérant 41 apporte des éléments utiles à la compréhension de l'article 13 (2) : *« (41) Dans le cadre d'une relation client-fournisseur existante, il est raisonnable d'autoriser l'entreprise qui, conformément à la directive 95/46/CE, a obtenu les coordonnées électroniques auprès du client lui-même, et exclusivement celle-ci, à exploiter ces coordonnées électroniques pour proposer au client des produits ou des services similaires. Il conviendrait, lorsque des coordonnées électroniques sont recueillies, que le client soit informé clairement sur leur utilisation ultérieure à des fins de prospection directe et qu'il lui soit donné la faculté de s'opposer à cet usage. Il convient de continuer d'offrir cette possibilité lors de chaque message de prospection directe ultérieur, et ce, sans frais hormis les coûts liés à la transmission du refus ».*

1 La notion d'abonné est définie dans la directive 2002/21/CE dans un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive-cadre). Il s'agit de la notion à utiliser, sauf stipulation contraire, conformément à l'article 2 de la directive 2002/58/CE.

La notion d'abonné est définie dans la directive-cadre comme « *toute personne physique ou morale partie à un contrat avec un fournisseur de services de communications électroniques accessibles au public, pour la fourniture de tels services* » (voir article 2 (k) de la directive 2002/21/CE).

Le considérant 12 de la directive 2002/58/EC clarifie cette notion, en précisant que : *« (12) Les abonnés à un service de communications électroniques accessible au public peuvent être des personnes physiques ou des personnes morales. En complétant la directive 95/46/CE, la présente directive vise à protéger les droits fondamentaux des personnes physiques et en particulier le droit au respect de leur vie privée, ainsi que les intérêts légitimes des personnes morales. La directive ne comporte aucune obligation pour les États membres d'étendre l'application de la directive 95/46/CE à la protection des intérêts légitimes des personnes morales, qui est déjà garantie dans le cadre de la législation communautaire et nationale en vigueur ».*

Bien que cette description laisse une certaine marge d'interprétation, le groupe de travail souhaite souligner que cette exception est limitée de différentes manières et doit être interprétée de manière restrictive.

Premièrement, cette exception est limitée aux clients en conformité avec la première phrase de l'article 13 (2). De plus, des messages électroniques ne peuvent être envoyés qu'aux clients auprès desquels les coordonnées électroniques pour le courrier électronique ont été obtenues dans le cadre de la vente d'un produit ou d'un service et conformément à la directive 95/46/CE. Cette dernière disposition inclut par exemple les informations sur les raisons de la collecte (voir ci-dessus). Le principe de finalité (utilisation compatible, traitement loyal) doit servir d'aide sur ce point. Dans ce contexte, l'attention doit également être portée sur la période durant laquelle le consentement pourrait être considéré comme valable et des messages électroniques, être envoyés.

Deuxièmement, seule la même personne physique ou morale que celle qui a collecté les données peut envoyer des courriers électroniques à des fins de prospection. Les filiales ou sociétés mères par exemple ne sont pas la même entreprise.

Troisièmement, elle est limitée à la commercialisation de produits et services analogues. L'avis du groupe de travail est que, bien que cette notion de 'produits et services similaires ne soit pas une notion aisément applicable en pratique et nécessite davantage d'attention, la similarité pourrait en particulier être jugée du point de vue objectif du destinataire (attentes raisonnables), plutôt que du point de vue de l'expéditeur.

Le groupe de travail rappelle qu'il existe une obligation, y compris dans le cas de l'exception, de continuer à proposer une possibilité d'opposition dans chaque message de prospection directe.

DOCUMENT DE TRAVAIL SUR LA BIOMÉTRIE

Adopté le 1er août 2003

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel, institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 [1] ;

Vu l'article 29 et l'article 30, paragraphe 1, point a) et paragraphe 3 de ladite directive ;

Vu son règlement intérieur, et notamment les articles 12 et 14 de celui-ci ;

A adopté le présent document de travail :

Introduction

Les progrès rapides des technologies biométriques, ainsi que la généralisation de leur application durant ces dernières années, nécessitent un examen attentif sur le plan de la protection des données [2]. Une utilisation répandue et non contrôlée

1 *Journal officiel* L 281 du 23 novembre 1995, p. 31, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 Depuis le 11 septembre 2001, la biométrie a souvent été présentée comme un moyen valable d'améliorer la sécurité publique. Au niveau de l'UE, l'intégration d'éléments biométriques dans les cartes d'identité, passeports, documents de voyage et visas est à l'étude. Les Etats-Unis exigeront bientôt des identifiants biométriques pour les étrangers entrant sur leur territoire et quittant celui-ci. La convention n° 108 de l'OIT a été modifiée en 2003 par l'introduction du recours obligatoire à la biométrie pour les gens de mer. Des discussions se poursuivent également dans d'autres enceintes internationales, telles que le G8, l'OCDE, etc.

de la biométrie suscite des inquiétudes en ce qui concerne la protection des libertés et des droits fondamentaux des personnes. Les données de ce genre sont d'une nature particulière puisqu'elles ont trait aux caractéristiques comportementales et physiologiques d'une personne, et peuvent permettre de l'identifier sans ambiguïté [1].

Aujourd'hui, il est souvent fait recours au traitement de données biométriques dans des procédures automatisées d'authentification/vérification et d'identification, notamment lors du contrôle de l'entrée dans des zones physiques et virtuelles (c'est-à-dire l'accès à des systèmes ou services électroniques particuliers).

Précédemment, l'utilisation de la biométrie se limitait pour l'essentiel aux domaines de l'ADN et de la vérification d'empreintes digitales. Les empreintes digitales étaient collectées en particulier à des fins de répression (par exemple dans le cadre d'enquêtes judiciaires). Si la société encourage le développement de bases de données d'empreintes digitales ou d'autres bases de données biométriques en vue d'autres applications courantes, elle pourrait accroître les possibilités de réutilisation de ces données par des tiers comme éléments de comparaison et de recherche dans le cadre de leurs propres activités, sans que cet objectif ait été envisagé initialement ; les autorités chargées d'appliquer la loi pourraient figurer parmi les tiers précités.

Une préoccupation spécifique liée aux données biométriques consiste dans le risque d'une désensibilisation du public, en raison d'une utilisation toujours croissante de ces données, aux conséquences que leur traitement peut avoir sur la vie quotidienne. Par exemple, le recours à la biométrie dans les bibliothèques scolaires peut rendre les enfants moins conscients des risques qui sont liés à la protection des données et qui peuvent avoir des conséquences pour eux plus tard dans la vie.

Le présent document a pour but de contribuer à l'application efficace et homogène des dispositions nationales adoptées en vertu de la directive 95/46/CE aux systèmes biométriques. Il porte principalement sur les applications biométriques servant à des fins d'authentification et de vérification. Le groupe de travail entend proposer des orientations uniformes au niveau européen, notamment pour l'industrie des systèmes biométriques et pour les utilisateurs de ces technologies.

Description des systèmes biométriques

Les systèmes biométriques sont des applications de technologies biométriques, qui permettent l'identification et/ou l'authentification/vérification automatiques d'une personne [2]. Des applications d'authentification/vérification sont fréquemment utilisées pour l'exécution de diverses tâches relevant de domaines totalement différents et sous la responsabilité d'un vaste éventail d'entités différentes.

Chaque technique biométrique, qu'elle vise l'authentification/vérification ou l'identification, dépend plus ou moins de l'élément biométrique concerné, qui peut être :

1 Cependant, cette identification certaine dépend de différents facteurs, dont la taille de la base de données et le type d'éléments biométriques utilisés.

2 La différence entre l'authentification (vérification) et l'identification est importante. L'authentification répond à la question : suis-je celui ou celle que je prétends être ? Le système certifie l'identité de l'individu en traitant des données biométriques qui se réfèrent à la personne posant la question et prend une décision oui/non (comparaison 1 : 1). L'identification répond à la question : qui suis-je ? Le système reconnaît l'individu qui pose la question en le distinguant d'autres personnes dont les données biométriques sont également enregistrées. Dans ce cas, le système prend une décision « 1 sur n » et répond que la personne posant la question est X.

— **universel :** l'élément biométrique est présent chez tous les individus [1] ;
— **unique** : l'élément biométrique doit être propre à chaque personne ;
— **permanent :** chaque personne conserve au cours du temps la propriété de l'élément biométrique.

On peut distinguer deux catégories principales de techniques biométriques, selon que des données stables ou des données dynamiques sur le comportement sont utilisées [2].

En premier lieu, il existe des techniques basées sur l'aspect physique et la **physiologie** qui mesurent les caractéristiques physiologiques d'une personne ; elles comprennent la vérification des empreintes digitales, l'analyse de l'image du doigt, la reconnaissance de l'iris, l'analyse de la rétine, la reconnaissance faciale, la géométrie de la main, la reconnaissance de la forme de l'oreille, la détection de l'odeur corporelle, la reconnaissance vocale, l'analyse de la structure de l'ADN [3], l'analyse des pores de la peau, etc.

En second lieu, on dispose de techniques **comportementales** qui mesurent le comportement d'une personne ; elles comprennent la vérification de la signature manuscrite, l'analyse de la frappe sur le clavier, l'analyse de la démarche, etc.

De nombreux systèmes biométriques tiennent compte de l'évolution rapide des technologies et du souci accru de sécurité, et fonctionnent en associant diverses modalités biométriques de l'utilisateur avec d'autres technologies d'identification ou d'authentification. Certains systèmes combinent par exemple la reconnaissance faciale et l'enregistrement de la voix. Pour effectuer une authentification, trois méthodes différentes peuvent être utilisées conjointement : l'identification se fera alors sur la base de quelque chose qu'une personne sait (mot de passe, numéro personnel d'identification, etc.), de quelque chose qu'une personne possède (jeton, clé CAD, carte à puce, etc.) et de quelque chose qu'une personne est (une caractéristique biométrique). Sur un ordinateur, on pourrait, par exemple, introduire une carte à puce, taper un mot de passe et présenter son empreinte digitale.

La collecte d'échantillons biométriques, appelés « données biométriques », telles que l'empreinte digitale, la photographie de l'iris ou de la rétine, l'enregistrement de la voix), est réalisée durant une phase d'« inscription » à l'aide d'un capteur spécifique pour chaque type d'élément biométrique. Le système biométrique extrait de ces données des traits spécifiques à l'utilisateur pour construire un « modèle » biométrique. Celui-ci est une réduction structurée d'une image biométrique, c'est-à-dire la mesure biométrique enregistrée d'un individu. C'est le modèle sous sa forme numérisée qui sera enregistré, et non l'élément biométrique lui-même. En outre, les données biométriques peuvent être traitées comme des données brutes (une image) en fonction du système biométrique qui est utilisé. [4]

La phase d'inscription a une importance primordiale car c'est la seule où les données brutes, les algorithmes d'extraction et de protection (cryptographie,

1 À cet égard, tous les éléments biométriques ne sont pas équivalents, et le taux de différenciation d'une personne par rapport à une autre varie considérablement en fonction des éléments biométriques utilisés. Les éléments biométriques les plus distinctifs semblent être l'ADN, la rétine et l'empreinte digitale.

2 Certaines techniques peuvent reposer à la fois sur la physiologie et sur le comportement.

3 Bien que l'utilisation de l'ADN à des fins d'identification biométrique soulève des questions spécifiques, celles-ci ne seront pas examinées dans le présent document. On peut noter qu'il ne semble pas possible actuellement de générer un profil d'ADN en temps réel en tant que moyen d'authentification.

4 Le présent document se réfère essentiellement aux systèmes biométriques basés sur des « modèles », mais pourrait également s'appliquer à des données brutes. Toutefois, le caractère spécifique de ces dernières pourrait conduire à une adaptation des exigences en matière de protection des données.

hachage, etc.) et les modèles sont présents simultanément. À cet égard, il convient de souligner que, si les données brutes révèlent des informations qui peuvent être considérées comme sensibles au sens de l'article 8 de la directive 95/46/CE, le processus d'inscription de ces données doit se dérouler conformément à cette disposition (*cf.* plus loin « Données sensibles »).

Sur le plan de la protection des données, la forme sous laquelle sont conservés les modèles relatifs aux utilisateurs est également importante. La conservation des modèles dépend du type d'application pour lequel le dispositif biométrique sera utilisé et de la taille des modèles eux-mêmes. Les modèles peuvent être conservés :
a) dans la mémoire d'un dispositif biométrique ;
b) dans une base de données centrale ;
c) sur des cartes plastiques, des cartes optiques ou des cartes à puce. Cette méthode de conservation permet aux utilisateurs de porter sur eux leurs modèles comme moyens d'identification.

En principe, l'enregistrement des données de référence dans une base de données n'est pas nécessaire aux fins de l'authentification/vérification ; un stockage décentralisé des données à caractère personnel est suffisant. En revanche, l'identification n'est réalisable qu'avec un stockage centralisé des données de référence parce que, pour vérifier l'identité de la personne concernée, le système doit comparer le modèle ou les données brutes (image) de cette personne avec ceux de toutes les personnes dont les données sont déjà enregistrées dans une mémoire centrale.

Toujours dans une perspective de protection des données, il est très important de noter que certains systèmes biométriques reposent sur des informations telles que des empreintes digitales ou des échantillons d'ADN, qui peuvent être recueillies à l'insu du sujet concerné car celui-ci peut laisser des traces sans le savoir. Par l'application d'un algorithme biométrique à une empreinte digitale relevée sur un verre, on parviendra peut-être [1] à déterminer si une personne est enregistrée dans une base de données contenant des données biométriques et, le cas échéant, qui est cette personne, en procédant à une comparaison des deux modèles. Cette observation vaut également pour d'autres systèmes biométriques, tels que ceux qui sont basés sur l'analyse de la frappe sur un clavier ou sur la reconnaissance faciale à distance, en raison des caractéristiques spécifiques de la technologie mise en œuvre [2]. Le problème réside dans le fait que, d'une part, cette collecte et ce traitement de données peuvent être réalisés à l'insu de la personne concernée et que, d'autre part, quelle que soit leur fiabilité actuelle, ces technologies biométriques se prêtent à une utilisation généralisée en raison de leur « faible niveau d'intrusion ». Il semble dès lors nécessaire de définir des garanties spécifiques à cet égard.

Application des principes de la directive 95/46/CE

Application de la directive 95/46/CE

Conformément à l'article 2, point a), de la directive 95/46/CE, il faut entendre par « *"données à caractère personnel" toute information concernant une personne physique identifiée ou identifiable* [...] ; *est réputée identifiable une per-*

1 Cela implique cependant que l'on dispose au moins de certains moyens, tels que la possibilité de prélever l'empreinte sur le verre sans l'endommager, l'équipement technique nécessaire pour traiter les données fournies par l'empreinte, ainsi que l'accès à l'algorithme du constructeur et/ou à la base de données des empreintes digitales.

2 Voir point 3 concernant l'application de la directive 95/46/CE, et en particulier le point « Collecte loyale et information de la personne concernée » relatif à l'obligation d'informer la personne concernée.

sonne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique [...] ». Au considérant 26, il est précisé que *« pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement,* ***soit par une autre personne****, pour identifier ladite personne ».*

Selon cette définition, les mesures d'identification biométrique ou leur version numérisée sous forme de modèle sont, dans la plupart des cas, des données à caractère personnel. [1] Il apparaît que des données biométriques peuvent toujours être considérées comme « des informations concernant une personne physique », puisqu'il s'agit de données qui fournissent, par leur nature même, des informations sur une personne précise. Dans le contexte de l'identification biométrique, la personne est généralement identifiable, puisque les données biométriques sont utilisées à des fins d'identification ou d'authentification/vérification au moins dans la mesure où la personne concernée est distinguée de toute autre personne [2].

Conformément à l'article 3, paragraphe 1, de la directive 95/46/CE, les principes de la protection des données s'appliquent au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel faisant partie ou appelées à faire partie d'un fichier. La directive ne s'applique pas aux données qui sont traitées par une personne physique dans le cadre d'une activité purement personnelle ou domestique. De nombreuses applications biométriques dans le cadre domestique relèveront de cette catégorie.

Au-delà de ces exclusions spécifiques, le traitement de données biométriques ne peut être considéré comme licite que si toutes les procédures concernées — à commencer par l'inscription — sont mises en œuvre dans le respect des dispositions de la directive 95/46/CE.

Le présent document ne couvre pas toutes les questions soulevées par l'application de la directive 95/46/CE aux données biométriques, mais uniquement les plus pertinentes. Il ne dresse donc pas un tableau complet des conséquences de l'application de cette directive.

Principes de finalité et de proportionnalité

Selon l'article 6 de la directive 95/46/CE, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. De plus, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (principe de finalité).

Le respect de ce principe implique tout d'abord une définition claire de la finalité pour laquelle les informations biométriques sont collectées et traitées. En outre, une évaluation du respect des principes de proportionnalité et de légitimité est

1 Si des données biométriques, telles qu'un modèle, sont stockées de telle manière qu'aucun moyen raisonnable ne peut être mis en œuvre par le responsable du traitement ou une autre personne pour identifier la personne concernée, ces données ne sont pas à qualifier de données à caractère personnel.

2 L'identifiabilité de la personne dépend également de la disponibilité d'autres données qui — conjointement et séparément — permettent d'identifier la personne en question. La possibilité d'une « identification directe » par référence à « un ou plusieurs éléments spécifiques propres à son identité physique » est expressément mentionnée dans la définition des données à caractère personnel à l'article 2, point a), de la directive 95/46/CE.

nécessaire et doit être effectuée en tenant compte des risques concernant la protection des libertés et des droits fondamentaux de la personne ; il s'agit notamment d'établir si la finalité poursuivie ne pourrait pas être atteinte d'une façon moins intrusive. La proportionnalité a été le critère déterminant dans presque toutes les décisions relatives au traitement de données biométriques, qui ont été prises jusqu'ici par les autorités chargées de la protection des données [1].

Le groupe de travail est d'avis que l'utilisation, à des fins de contrôle d'accès (authentification/vérification), de systèmes biométriques se référant à des caractéristiques physiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les empreintes digitales) ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne. [2] Plusieurs autorités de protection des données se sont ralliées à cette opinion et ont indiqué que les éléments biométriques devraient, de préférence, être conservés non pas dans une base de données, mais plutôt dans un dispositif exclusivement accessible à l'utilisateur, tel qu'une carte à puce, un téléphone portable ou une carte bancaire [3]. En d'autres termes, les applications d'authentification/vérification qui peuvent être mises en œuvre sans enregistrement central de données biométriques ne devraient pas faire appel à des techniques d'identification excessives.

C'est la raison pour laquelle le groupe de travail estime qu'avant de mettre en place d'autres types d'applications (fondées par exemple sur la mise en mémoire de modèles d'empreintes digitales dans des terminaux d'accès ou dans une base de données centrale), il y a lieu de les soumettre à une évaluation minutieuse. Toutefois, si ce type de système est mis en œuvre, par exemple dans le cas d'installations de haute sécurité [4], il peut être considéré comme un traitement de données qui présente des risques au sens de l'article 20 de la directive 95/46/CE, et donc être soumis au contrôle préalable des autorités chargées de la protection des données conformément à la législation nationale (*cf.* « Contrôle préalable — notification »).

La directive 95/46/CE interdit un traitement ultérieur qui serait incompatible avec les finalités pour lesquelles les données ont été collectées. Par exemple, lorsque des données biométriques sont traitées à des fins de contrôle d'accès, leur utilisation en vue d'évaluer l'état émotionnel de la personne concernée ou de surveiller une personne sur son lieu de travail ne serait pas compatible avec la finalité initiale. Toutes les mesures appropriées doivent être prises pour empêcher ce type de réutilisation incompatible [5]. La directive 95/46/CE prévoit, sous certaines conditions, des

1 Par exemple les décisions des autorités néerlandaises, françaises, allemandes, italiennes et grecques.

2 On peut faire une distinction entre le cas où les données biométriques sont traitées de manière centralisée et celui où les données de référence biométriques sont enregistrées sur un dispositif mobile et où le processus de mise en correspondance s'effectue sur la carte, mais non sur le capteur, voire celui où le capteur fait partie du dispositif mobile.

3 Les mécanismes prévus pour remédier aux problèmes découlant de la perte, du vol ou de la détérioration des cartes doivent être pris en compte. Les mécanismes n'entraînant pas le stockage de données biométriques devraient être favorisés. Dans toute la mesure du possible, les données devraient être recueillies à nouveau directement auprès de la personne concernée.

4 Dans l'état actuel de la technologie biométrique, il n'existe pas encore des solutions fiables d'identification pure en temps réel pour une population, quelle qu'en soit la taille, et il est peu probable que des solutions de cette nature soient disponibles dans un avenir proche.

5 Comme indiqué plus haut, cette finalité doit être clairement définie.

dérogations à l'interdiction de soumettre les données à un traitement ultérieur dans un but incompatible avec la finalité initiale.

Il est généralement admis que le risque de réutilisation, pour des finalités incompatibles, de données biométriques obtenues à partir de traces physiques laissées par des personnes à leur insu (empreintes digitales par exemple) est relativement faible lorsque les données sont conservées non pas dans des bases de données centralisées, mais par la personne concernée, et qu'elles sont inaccessibles aux tiers. Le stockage centralisé de données biométriques accroît également le risque que ces données soient utilisées comme une clé pour interconnecter différentes bases de données, ce qui pourrait permettre d'obtenir un profil détaillé des habitudes d'un individu, tant dans la sphère publique que dans la sphère privée. La question de la compatibilité des finalités pose également le problème de l'interopérabilité de différents systèmes reposant sur la biométrie. La standardisation qu'exige l'interopérabilité pourrait entraîner une plus forte interconnexion entre les bases de données.

L'utilisation de la biométrie soulève en outre la question de la proportionnalité de chaque catégorie de données traitées à la lumière de la finalité pour laquelle les données sont exploitées. Des données biométriques ne doivent être utilisées que si leur utilisation est adéquate, pertinente et non excessive, ce qui implique une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées [1]. En France, la CNIL a par exemple refusé que des empreintes digitales soient utilisées pour contrôler l'accès d'enfants à une cantine scolaire [2], mais a accepté pour cette même finalité le recours à la morphologie de la main. Au Portugal, l'autorité chargée de la protection des données vient de prendre une décision défavorable à l'utilisation d'un système biométrique (empreintes digitales) par une université dans le but de contrôler l'assiduité et la ponctualité du personnel non enseignant [3]. L'autorité allemande de protection des données a rendu une décision favorable à l'introduction de caractéristiques biométriques dans les documents d'identité afin d'empêcher la falsification de ceux-ci, à condition que les données soient conservées dans la micropuce de la carte, et non dans une base de données, en vue de la comparaison avec les empreintes digitales du propriétaire.

Une difficulté particulière peut résulter du fait que les données biométriques contiennent souvent davantage d'informations que ne nécessitent les fonctions d'identification ou d'authentification. Cela risque surtout d'être le cas pour l'image originale (données brutes) parce que, du point de vue technique, le modèle peut et doit être construit de manière à exclure le traitement de données qui ne sont pas nécessaires. Les données non nécessaires doivent être détruites dès que possible [4]. En outre, certaines données biométriques peuvent révéler l'origine raciale ou concerner l'état de santé (*cf.* plus loin, « Données sensibles »).

1 En outre, l'anonymat ou l'utilisation de pseudonymes doivent rester possibles dans certaines circonstances. Les mécanismes prévus pour remédier aux problèmes découlant de la perte, du vol ou de la détérioration des cartes doivent être pris en compte dans ce contexte. Les mécanismes n'entraînant pas le stockage de données biométriques doivent être favorisés. Dans toute la mesure du possible, les données devraient être recueillies à nouveau directement auprès de la personne concernée.

2 Il semble cependant qu'au Royaume-Uni, l'autorité de protection des données ait accepté l'utilisation des empreintes digitales dans un cas similaire où des garanties appropriées avaient été mises en place.

3 L'autorité portugaise de protection des données était d'avis que le recours à de tels systèmes était disproportionné et excessif au regard de la finalité du traitement des données. Le système devait stocker ces données dans un dispositif biométrique et le nombre des personnes à contrôler était d'environ 140.

4 Cette suppression est également justifiée par le fait que l'article 6, paragraphe 1, point e), de la directive 95/46/CE dispose que les données à caractère personnel ne sont conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

Enfin, il importe de noter que l'utilisation de systèmes biométriques pourrait être conçue de telle manière qu'on pourrait y voir une technologie améliorant la protection de la vie privée, entre autres en raison d'un moindre recours au traitement d'autres données à caractère personnel, telles que le nom, l'adresse, la résidence, etc.

Collecte loyale et information de la personne concernée

Le traitement de données biométriques, et en particulier leur collecte, doivent se faire de manière loyale. [1] Le responsable du traitement des données doit informer la personne concernée conformément aux articles 10 et 11 de la directive 95/46/CE [2]. Cette information comprend en particulier la définition exacte de la finalité et l'identité du responsable du fichier (qui sera souvent la personne gérant le système biométrique ou appliquant la technique biométrique).

Les systèmes qui collectent des données biométriques à l'insu des personnes concernées doivent être proscrits. Certains systèmes biométriques, tels que la reconnaissance faciale à distance, la collecte d'empreintes digitales ou l'enregistrement de la voix, présentent davantage de risques à cet égard.

Critères de légitimation du traitement de données

Le traitement de données biométriques doit être fondé sur l'un des motifs de légitimité prévus à l'article 7 de la directive 95/46/CE. Le groupe de travail souligne que, si le consentement est utilisé comme motif de légitimité par le responsable du fichier, ce consentement doit respecter les conditions fixées à l'article 2 de la directive 95/46/CE (toute manifestation de volonté, libre, spécifique et informée, par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement).

Contrôle préalable — notification

Comme il a été indiqué plus haut, le groupe de travail est favorable à l'utilisation de systèmes biométriques qui ne mémorisent pas de traces dans des terminaux d'accès ou dans une base de données centrale (*cf.* « Principes de finalité et de proportionnalité »). Mais s'il est prévu d'utiliser de tels systèmes, et compte tenu du risque d'une (ré) utilisation des données pour des finalités différentes, ainsi que des risques spécifiques inhérents à un accès non autorisé, le groupe de travail recommande que les États membres envisagent de les soumettre au contrôle préalable des autorités chargées de la protection des données conformément à l'article 20 de la directive 95/46/CE, car un tel traitement des données présentera probablement des risques particuliers pour les droits et libertés des personnes concernées. Si les États membres ont l'intention d'instaurer un contrôle préalable en relation avec le traitement de données biométriques, il importe que les autorités nationales chargées de la protection des données soient valablement consultées avant la mise en place de mesures de cette nature.

1 Article 6, paragraphe 1, point a), de la directive 95/46/CE.

2 Les exemptions de l'obligation d'informer les personnes concernées, prévue aux articles 10 et 11 de la directive 95/46/CE, devraient être fondées sur des mesures législatives et constituer une mesure nécessaire pour réduire la portée de l'obligation d'information en vue de sauvegarder les intérêts énumérés à l'article 13 de la directive 95/46/CE (sécurité publique, prévention, recherche, détection et poursuite d'infractions pénales, etc.).

Mesures de sécurité

Conformément à l'article 17 de la directive 95/46/CE, le responsable du traitement doit prendre toutes les mesures de sécurité techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite ou la perte accidentelle, la modification, l'accès ou la communication non autorisés, notamment si le traitement des données biométriques implique leur transmission par un réseau. Des mesures de sécurité doivent être prises lorsque des données biométriques font l'objet d'un traitement (conservation, transmission, extraction de certaines caractéristiques et comparaison, etc.), et en particulier lorsqu'elles sont transmises par le responsable via internet. Les mesures de sécurité pourraient inclure le cryptage des modèles et un système de protection des clés de cryptage, venant s'ajouter au contrôle d'accès et à la protection, et rendant pratiquement impossible la reconstitution des données originales à partir de ces modèles.

Dans ce contexte, il y a lieu de tenir compte de certaines technologies nouvelles. La possibilité d'utiliser des données biométriques comme clés de cryptage constitue une évolution intéressante. Une telle solution engendrerait a priori moins de risques pour la personne concernée car le décodage ne pourrait se faire que sur la base d'une nouvelle collecte de données biométriques auprès de l'intéressé lui-même, ce qui éviterait la création de bases de données contenant des modèles de données biométriques susceptibles d'être réutilisés à des fins tout à fait différentes.

Il y a lieu de prendre les mesures de sécurité requises dès le début du traitement des données, en particulier durant la phase d'« inscription » au cours de laquelle les données biométriques sont transformées en modèles ou en images. Il importe de comprendre que, si les bases de données devaient perdre leurs qualités d'intégrité, de confidentialité et de disponibilité, cela pénaliserait manifestement toutes les applications futures basées sur les informations contenues dans ces bases de données et infligerait un préjudice irréversible aux personnes concernées. Si, par exemple, les empreintes digitales d'une personne autorisée étaient associées avec l'identité d'une personne non autorisée, cette dernière pourrait accéder indûment aux services réservés au propriétaire des empreintes. Il en résulterait un vol d'identité qui, détecté ou non, rendrait les empreintes digitales de la personne non fiables pour des applications ultérieures et limiterait ainsi la liberté de cette personne.

Les erreurs qui se produisent à l'intérieur de systèmes biométriques peuvent avoir des conséquences graves pour la personne concernée, en particulier lorsqu'il s'agit du rejet erroné de personnes autorisées et de l'acceptation indue de personnes non autorisées, qui peuvent être à l'origine de problèmes sérieux à plusieurs niveaux différents. *A priori*, l'utilisation de données biométriques devrait réduire le risque de telles erreurs, mais elle pourrait également donner l'illusion que l'identification ou l'authentification/vérification de la personne concernée est toujours correcte. Il peut être difficile, voire impossible pour la personne concernée d'apporter la preuve du contraire. Ainsi, un système pourrait identifier erronément une personne comme quelqu'un qui ne doit pas être autorisé à monter à bord d'un avion ou à entrer dans un pays donné, et cette personne n'aura guère la possibilité de résoudre le problème lorsqu'une telle preuve « incontestable » lui sera opposée. Il convient de souligner à nouveau que, quand des cas pareils se produisent, toute décision produisant des effets juridiques à l'égard d'une personne ne doit être prise qu'après vérification du résultat du traitement automatisé, conformément à l'article 15 de la directive 95/46/CE.

Enfin, il convient de noter que l'utilisation de la biométrie pourrait améliorer les procédures de contrôle dans le cas de l'accès à des données à caractère person-

nel concernant des tiers, par exemple en cas de vol ou d'utilisation abusive (procédures d'autorisation).

Données sensibles

Certaines données biométriques pourraient être considérées comme sensibles au sens de l'article 8 de la directive 95/46/CE, notamment celles qui révèlent l'origine raciale ou ethnique ou encore les données relatives à la santé. Dans les systèmes biométriques reposant sur la reconnaissance faciale, par exemple, il est possible de traiter des données révélant l'origine raciale ou ethnique. Dans ces cas-là, les garanties spéciales prévues à l'article 8 seront applicables en plus des principes généraux de protection énoncés par la directive.

Cela ne signifie pas que tout traitement de données biométriques couvrira nécessairement des données sensibles. Dire si un traitement englobe des données sensibles est une question d'appréciation liée à la caractéristique biométrique spécifique qui est utilisée et à l'application biométrique elle-même. Cela risque davantage d'être le cas lorsque l'on traite des données biométriques sous forme d'images, puisque les données brutes ne peuvent en principe pas être reconstituées à partir du modèle.

Identifiant unique

Les données biométriques sont uniques et la plupart d'entre elles génèrent un modèle (ou une image) unique. Dans le cas d'une large utilisation, en particulier pour une partie importante de la population, elles peuvent être considérées comme un identifiant de portée générale au sens de la directive 95/46/CE. L'article 8, paragraphe 7, de cette directive serait alors applicable et les États membres devraient déterminer les conditions de leur traitement.

Quand des données biométriques doivent être utilisées comme une clé permettant de mettre en relation des bases de données contenant des données à caractère personnel [1], des problèmes particulièrement délicats peuvent se poser si la personne concernée n'a aucune possibilité de s'opposer au traitement de données biométriques, comme cela peut arriver fréquemment dans les rapports entre les citoyens et les autorités publiques.

De ce point de vue, il serait souhaitable que les modèles et leurs représentations numériques soient traités à l'aide de manipulations mathématiques (cryptage, algorithmes ou fonctions de hachage) faisant appel à des paramètres différents pour chaque produit biométrique utilisé, afin d'éviter la combinaison de données à caractère personnel provenant de plusieurs bases de données, grâce à la comparaison de modèles ou de représentations numériques.

Code de conduite et utilisation des technologies renforçant la protection de la vie privée

Le groupe de travail encourage le secteur à développer des systèmes biométriques qui facilitent la mise en œuvre des recommandations contenues dans le présent document de travail et, si des normes européennes ou internationales devaient être élaborées dans ce domaine, elles devraient l'être en coordination avec les autorités chargées de la protection des données, afin que soient favorisés des systèmes biométriques dont la conception respecte la protection des données, qui minimisent les risques sociaux et qui préviennent l'emploi abusif de données biométriques. Le groupe de travail souligne l'importance, dans ce contexte, des technologies renfor-

1 Voir également plus haut, point « Principes de finalité et de proportionnalité » concernant les réutilisations compatibles.

çant la protection de la vie privée (PETS = *Privacy Enhancing Technologies*) afin de réduire la collecte de données et de prévenir le traitement illicite.

En outre, le groupe de travail insiste sur l'importance des codes de conduite qui devraient contribuer, en fonction de la spécificité des divers secteurs, à la bonne application des principes de la protection des données, conformément à l'article 27 de la directive 95/46/CE. Des codes communautaires peuvent être soumis au groupe de travail qui déterminera, entre autres, si les projets qui lui sont présentés sont conformes aux dispositions nationales relatives à la protection des données, adoptées conformément à la directive 95/46/CE.

Conclusions

Le groupe de travail estime que la plupart des systèmes biométriques impliquent le traitement de données à caractère personnel. Il est donc nécessaire de les développer en tenant pleinement compte des principes de protection des données énoncés dans la directive 95/46/CE, et notamment de la capacité de collecter des données biométriques à l'insu de la personne concernée et de la quasi-certitude du lien avec ladite personne.

Le respect du principe de proportionnalité, qui constitue l'élément central de la protection garantie par la directive 95/46/CE, implique, tout particulièrement dans le contexte de l'authentification/vérification, qu'une préférence claire soit accordée aux applications biométriques qui ne traitent pas de données obtenues à partir de traces physiques laissées par des personnes à leur insu, ni des données qui ne sont pas stockées dans un système centralisé. Cela permet aux personnes concernées d'avoir un meilleur contrôle sur le traitement des données à caractère personnel les concernant.

Le groupe de travail a l'intention de revoir le présent document de travail à la lumière de l'expérience des autorités chargées de la protection des données, ainsi que des développements technologiques dans le domaine des applications biométriques. Comme des données biométriques sont utilisées dès à présent en vue d'une large gamme d'utilisations dans divers domaines, d'autres travaux devront être entrepris sans tarder, notamment en ce qui concerne l'emploi, les visas, l'immigration et la sécurité des transports.

Si le secteur doit garder la responsabilité d'élaborer des systèmes biométriques conformes aux principes de protection des données, il serait extrêmement utile, à tout point de vue, qu'un dialogue efficace, reposant en particulier sur un projet de code de conduite, soit instauré entre toutes les parties intéressées, y compris les autorités chargées de la protection des données.

Annexe 10

Décisions des juridictions

TRIBUNAL DE GRANDE INSTANCE DE PARIS ORDONNANCE DE RÉFÉRÉ, RENDUE le 27 JANVIER 2003
(N° RG : 03/50808)

Nous, président ;

Après avoir entendu les parties comparantes ou leur conseil ;

Vu l'assignation en date du 20 janvier 2003 par laquelle Monsieur X. expose qu'une personne se présentant comme M. Y. via une boîte mail Lycos : marco9@lycos.fr a adressé un message e-mail à trois de ses collaborateurs et un client important de la société — dont il est président de directoire — dont le contenu lui paraît diffamatoire ; demande au visa de l'article 145 du Nouveau Code de procédure civile la communication par la Société Lycos France de l'identité de l'utilisateur de l'adresse électronique précitée et de conserver les mails envoyés depuis l'adresse ;

Vu les conclusions déposées à l'audience par la Société Lycos qui fait valoir que le caractère privé de la correspondance incriminée s'oppose à ce qu'il soit fait droit à la demande et se déclare prête toutefois à communiquer l'identité qui lui a été déclarée par l'utilisateur de l'adresse électronique en cause ;

Attendu que les courriers électroniques sont des correspondances privées bénéficiant du secret, que dès lors, l'article 43-9 de la loi du 30 septembre 1986 modifiée n'est pas applicable à la demande de communication de l'identité du titulaire de l'adresse électronique marco9@lycos.fr ; que le même secret s'oppose à ce que la défenderesse puisse intercepter des messages enregistrés sous cette adresse, à supposer qu'ils n'aient pas été détruits, en les transférant sur un autre support en violation de l'article 226-15 du Code pénal ;

Que la demande doit être rejetée ;

Par ces motifs :

Statuant publiquement en premier ressort, par ordonnance contradictoire ;

Rejetons la demande ;

Laissons les dépens à la charge de Monsieur X.

COUR D'APPEL DE VERSAILLES, ARRÊT DU 18 MARS 2003 (N° rôle : 02/00046)

Arrêt contradictoire ;

Infirmation ;

Faits, procédure, demandes et moyens des parties ;

Statuant sur l'appel régulièrement formé par Monsieur X., d'un jugement du conseil de prud'hommes de Nanterre, section encadrement, en date du 17 juillet 2001, dans un litige l'opposant à la société SFR (Société française de radiotéléphone), et qui, sur la demande de Monsieur X. en paiement d'indemnité de licenciement sans cause réelle et sérieuse a :

Débouté Monsieur X. de ses demandes ;

Monsieur X. a été engagé par la Société générale des eaux devenue SFR le 1er septembre 1993 en qualité de chef de ventes. Il a fait l'objet d'une convocation à entretien préalable à licenciement le 17 décembre 1999 pour le 22 décembre 1999 et a été licencié le 3 janvier 2000 au motif d'une utilisation détournée de l'accès **internet** portant sur des sites à caractère pornographique contrairement au règlement intérieur, au risque de propagation de virus, de nature à nuire à l'image de l'entreprise de la part d'un « manager » tenu de donner l'exemple, ayant une grande expérience, comportement contraire aux règles de gestion, de sécurité et aux principes de probité. L'entreprise emploie au moins onze salariés. Il existe des institutions représentatives du personnel ;

Le salaire mensuel est de 39 025 francs, Monsieur X. avait sept ans d'ancienneté et était âgé de 47 ans ;

Monsieur X. par conclusions écrites déposées et visées par le greffier à l'audience, conclut :

À l'infirmation du jugement ;

À la condamnation de la société SFR à lui payer :
— 140 000 euros ; d'indemnité de licenciement sans cause réelle et sérieuse ;
— 1 830 euros ; en application de l'article 700 du Nouveau Code de procédure civile ;

Il expose que l'utilisation internet qui lui est reprochée est survenue à son domicile par l'usage que son fils a fait à son insu de son ordinateur portable ;

La société SFR, par conclusions écrites déposées et visées par le greffier à l'audience conclut :

À la confirmation du jugement ;

Et au paiement de 1 525 euros ; en application de l'article 700 du Nouveau Code de procédure civile ;

Elle expose qu'elle a mis à la disposition de Monsieur X. un ordinateur portable pour son activité professionnelle, il existe un « Guide des bonnes pratiques-sécurité internet » dans l'entreprise et a fait signer un engagement de responsabilité ;

La société a constaté que Monsieur X. s'était branché sur des sites à caractère pornographiques le 8 octobre après 20 heures 58 et le 9 octobre 1999 entre 11 heures et 16 heures 27 allant ce jour également sur des sites comme « nitendo », « lego. com » et « respublica » ;

Le licenciement est justifié ;

Pour un plus ample exposé des moyens et prétentions des parties la cour, conformément à l'article 455 du Nouveau Code de procédure civile, renvoie aux conclusions déposées et soutenues à l'audience ainsi qu'aux prétentions orales telles qu'elles sont rappelées ci-dessus ;

Motifs de la décision :

Les faits reprochés à titre disciplinaire datent de plus de deux mois de l'engagement de la procédure de licenciement ;

La société SFR soutient par l'attestation d'un responsable du contrôle informatique que cette utilisation n'a été découverte que le 23 novembre 1999, aucun élément ne justifie de remettre en cause la sincérité de cette déclaration. La prescription de l'article L. 122-44 du Code du travail n'est pas acquise ;

Les éléments de preuve et de fait portent sur les événements du 8 et 9 octobre 1999 sans qu'il y ait lieu d'examiner d'autres dates de connexion internet ;

Les 8 et 9 octobre 1999 sont des vendredi et samedi, ainsi est établi l'utilisation internet depuis le domicile du salarié hors du temps et lieu du travail, mais durant le temps de sa vie privée et familiale ;

La société ne conteste pas que le salarié soit autorisé à emporter l'ordinateur portable à son domicile en semaine et en fin de semaine ;

Si l'employeur est fondé à réglementer l'usage d'internet au sein de l'entreprise, les recommandations de la Commission nationale de l'informatique et des libertés mettent en évidence l'existence d'un usage dans les entreprises qui admet qu'une interdiction absolue à des fins non professionnelles n'est pas raisonnable et qu'est admis un usage raisonnable de ce système à des fins personnelles, comme est reconnu un usage de même nature du téléphone de l'entreprise ;

Cet usage constaté par la CNIL correspond à l'exigence de l'article L. 120-2 du Code du travail posant le principe de restriction proportionné et nécessaire des libertés du salarié par l'employeur. À cet égard le « Guide des bonnes conduites » de la société SFR contrevient à cet usage et au respect de ce texte en ce qu'il pose le principe que ce qui n'est pas expressément autorisé est interdit ;

En autorisant Monsieur X. à emporter l'ordinateur portable à son domicile la société SFR reconnaît nécessairement un usage privé de celui-ci, sauf à étendre le temps et lieu d'exécution du contrat de travail au domicile du salarié durant son temps de repos et de vie privée ce qu'elle ne revendique pas ;

Le droit de l'employeur de porter atteinte aux libertés du salarié au temps et lieu du travail est encore restreint par ce texte lorsque l'employeur entend limiter l'usage de ce matériel informatique et de l'accès à internet par le salarié lorsque celui-ci est au temps et lieu de la vie privé et/ou familiale du salarié ;

La société reproche donc à Monsieur X. un fait tiré de la vie privée du salarié ;

Les connexions effectuées sur internet les 8 et 9 octobre concernent des sites à l'intitulé libertin et des sites de jeux. L'existence de ces derniers accrédite l'affirmation de Monsieur X. de l'utilisation de l'internet par son fils ;

Monsieur X. démontre que l'utilisation reprochée de l'internet est le fait de son fils et donc ne lui est pas personnellement imputable ;

La société SFR ne prétend pas que l'utilisation qui a été faite ait causé un préjudice au système informatique. Le caractère abusif du « Guide des bonnes pratiques » ne permet pas d'opposer au salarié les restrictions d'emploi qu'il contient ;

Il demeure un défaut de vigilance de Monsieur X. sur l'utilisation du code d'accès. Ce fait établi est indépendant de l'usage privé ou professionnel de l'internet

mais il constitue une contravention légère en l'absence de précédent qui ne justifie pas en soit une cause réelle et sérieuse de licenciement ;

Le licenciement de Monsieur X. est sans cause réelle et sérieuse ;

Ce licenciement lui cause, à 47 ans, et après sept années de collaboration sans faille dans une entreprise importante, un important préjudice que la cour évalue à 54 000 euros ;

L'équité commande de mettre à la charge de la société SFR une somme de 1 830 euros ; en application de l'article 700 du Nouveau Code de procédure civile au profit de Monsieur X. au titre de l'instance d'appel ;

La société SFR doit être déboutée de ses demandes dont celle en application de l'article 700 du Nouveau Code de procédure civile ;

Par ces motifs :

La Cour, statuant publiquement par arrêt contradictoire, infirme le jugement et statuant à nouveau :

Condamne la société SFR (Société française de radiotéléphone) à payer à Monsieur X. la somme de : 54 000 euros d'indemnité de licenciement sans cause réelle et sérieuse ainsi que 1 830 euros en application de l'article 700 du Nouveau Code de procédure civile, et ce avec intérêt de droit au taux légal du jour de la notification de l'arrêt ;

Déboute la société SFR de sa demande en application de l'article 700 du Nouveau Code de procédure civile ;

Condamne la société SFR aux dépens.

ARRÊT DU CONSEIL D'ÉTAT DU 2 JUIN 2003 (Req. n° 194296)

Vu la décision en date du 6 novembre 2002 par laquelle le Conseil d'État statuant au contentieux a, avant dire droit sur les requêtes de M^me^ X. tendant à l'annulation de la décision en date du 29 septembre 1997 de la Commission nationale de l'informatique et des libertés prise sur sa demande tendant d'une part, à ce que lui soient communiquées les informations la concernant figurant dans le système informatique national du système d'information Schengen et d'autre part, à ce que ces données soient rectifiées ou effacées et à l'annulation de la décision implicite de rejet résultant du silence gardé par le ministre de l'Intérieur sur sa demande tendant à l'effacement des données la concernant et enregistrées dans le système informatique national du système d'information Schengen, ordonné, d'une part à la Commission nationale de l'informatique et des libertés de lui communiquer dans un délai de deux mois, les informations concernant l'inscription, à la date de sa décision du 29 septembre 1997, de M^me^ X. dans le système informatique national du système d'information Schengen et les vérifications auxquelles la commission s'est livrée en réponse à la demande présentée par M^me^ X en application des dispositions de l'article 39 de la loi du 6 janvier 1978 et, d'autre part, au ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, de lui communiquer, dans un délai de deux mois, les informations relatives à l'inscription de M^me^ X. dans le système informatique national du système d'information Schengen à la date de la décision implicite par laquelle il a rejeté la demande de M^me^ X. tendant à l'effacement des données la concernant et enregistrées dans le système d'information Schengen ;

Vu les autres pièces des dossiers ;

Vu la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 80-539 du 16 juillet 1980, notamment son article 6-1 ;

Vu la loi n° 91-737 du 30 juillet 1991 autorisant l'approbation de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique du Benelux, de la République fédérale d'Allemagne, de la République française relative à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi n° 78-17 du 17 juillet 1978 ;

Vu le décret n° 79-1160 du 28 décembre 1979 ;

Vu le décret n° 86-326 du 7 mars 1986 ;

Vu le décret n° 95-304 du 21 mars 1995 portant publication de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique du Benelux, de la République fédérale d'Allemagne, de la République française relative à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990 ;

Vu le décret n° 95-577 du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS ;

Vu le Code de justice administrative ;

Après avoir entendu en séance publique :

— le rapport de M. Herondart, auditeur ;
— les observations de la SCP Delaporte, Briard, Trichet, avocat de M^me^ X ;
— les conclusions de M^me^ Maugüé, commissaire du gouvernement ;

Considérant que, par une décision en date du 6 novembre 2002, le Conseil d'État statuant au contentieux, avant dire-droit sur les moyens soulevés par M^me^ X. et tirés de ce que les informations concernant son inscription dans le système informatique national du système d'information Schengen devaient lui être communiquées sur le fondement de l'article 39 de la loi du 6 janvier 1978 et qu'elles devaient être rectifiées ou effacées, a ordonné, d'une part, à la Commission nationale de l'informatique et des libertés de lui communiquer, dans un délai de deux mois, les informations concernant l'inscription, à la date de sa décision du 29 septembre 1997, de M^me^ X. dans le système informatique national du système d'information Schengen et les vérifications auxquelles la Commission s'est livrée en réponse à la demande présentée par M^me^ X. en application des dispositions de l'article 39 de la loi du 6 janvier 1978 et, d'autre part, au ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, de lui communiquer, dans un délai de deux mois, les informations relatives à l'inscription de M^me^ X. dans le système informatique national du système d'information Schengen à la date de la décision implicite par laquelle il a rejeté la demande de M^me^ X. tendant à l'effacement des données la concernant et enregistrées dans le système d'information Schengen ;

Considérant que l'article 92 de la convention d'application de l'accord de Schengen du 14 juin 1985 institue un système d'information Schengen composé d'une partie nationale auprès de chacune des parties contractantes et d'une fonction de support technique ; que ce système a pour objet, conformément à l'article 93 de ladite convention, de préserver l'ordre et la sécurité publics y compris la sûreté de l'État, et l'application des dispositions sur la circulation des personnes de la présente

convention, sur les territoires des parties contractantes à l'aide des informations transmises par ce système ; qu'aux termes de l'article 96 de cette même convention :
1) les données relatives aux étrangers qui sont signalés aux fins de non-admission sont intégrées sur la base d'un signalement national résultant de décisions prises, dans le respect des règles de procédure prévues par la législation nationale, par les autorités administratives ou les juridictions compétentes ;
2) les décisions peuvent être fondées sur la menace pour l'ordre public ou la sécurité ou sûreté nationales que peut constituer la présence d'un étranger sur le territoire national. Tel peut être notamment le cas :
a) d'un étranger qui a été condamné pour une infraction passible d'une peine privative de liberté d'au moins un an ;
b) d'un étranger à l'égard duquel il existe des raisons sérieuses de croire qu'il a commis des faits punissables graves, y inclus ceux visés à l'article 71, ou à l'égard duquel il existe des indices réels qu'il envisage de commettre de tels faits sur le territoire d'une partie contractante ;

Considérant qu'aux termes de l'article 106 de la convention d'application de l'accord de Schengen :
1) seule la partie contractante signalante est autorisée à modifier, à compléter, à rectifier ou à effacer les données qu'elle a introduites ;
2) si une des parties contractantes qui n'a pas fait le signalement dispose d'indices faisant présumer qu'une donnée est entachée d'erreur de droit ou de fait, elle en avise dans les meilleurs délais la partie contractante signalante qui doit obligatoirement vérifier la communication, et si nécessaire, corriger ou effacer la donnée sans délai ;
3) si les parties contractantes ne peuvent parvenir à un accord, la partie contractante qui n'est pas à l'origine du signalement soumet le cas pour avis à l'autorité de contrôle commune visée à l'article 115, paragraphe 1 ; que le droit d'accès au système d'information Schengen est régi par l'article 109 de la convention, qui stipule : *« Le droit de toute personne d'accéder aux données la concernant qui sont intégrées dans le système d'information Schengen s'exerce dans le respect du droit de la partie contractante auprès de laquelle elle le fait valoir. Si le droit national le prévoit, l'autorité nationale de contrôle prévue à l'article 114 paragraphe 1 décide si des informations sont communiquées et selon quelles modalités »* ; que l'article 110 de la même convention stipule : *« Toute personne peut faire rectifier des données entachées d'erreur de fait la concernant ou faire effacer des données entachées d'erreur de droit la concernant »* ; qu'aux termes de l'article 111 de la convention : *« 1. Toute personne peut saisir, sur le territoire de chaque partie contractante, la juridiction ou l'autorité compétentes en vertu du droit national, d'une action notamment en rectification, en effacement, en information ou en indemnisation en* raison d'un *signalement la concernant* [...] *»* ; qu'enfin l'article 114 stipule : *« 1. Chaque partie contractante désigne une autorité de contrôle chargée, dans le respect du droit national, d'exercer un contrôle indépendant du fichier de la partie nationale du système d'information Schengen et de vérifier que le traitement et l'utilisation des données intégrées dans le système d'information Schengen ne sont pas attentatoires aux droits de la personne concernée* [...] *». « 2. Toute personne a le droit de demander aux autorités de contrôle de vérifier les données la concernant intégrées dans le système d'information Schengen ainsi que l'utilisation qui est faite de ces données. Ce droit est régi par le droit national de la partie contractante auprès de laquelle la demande est introduite. Si les données ont été intégrées par une autre partie contractante, le contrôle se réalise en étroite coordination avec l'autorité de contrôle de cette partie contractante »* ;

Considérant qu'en application des stipulations précitées de l'article 106 de la convention d'application de l'accord de Schengen, il incombe aux autorités nationales, saisies par une personne qui conteste son inscription dans le système informatique national du système d'information Schengen, de procéder, dans le cas d'un signalement opéré par la France, à l'effacement des données entachées d'erreur de droit ou d'erreur de fait ; que, dans le cas d'un signalement opéré par un État autre que la France, il appartient aux autorités nationales, si elles estiment disposer d'indices faisant présumer qu'une donnée est entachée d'erreur de droit ou de fait, d'en aviser les autorités de cet État ;

Considérant, d'autre part, qu'aux termes de l'article 36 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : *« Le titulaire du droit d'accès peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant et qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte et l'utilisation, la communication ou la conservation est interdite »* ;

Considérant qu'aux termes des dispositions alors en vigueur de l'article 39 de la loi du 6 janvier 1978 : *« En ce qui concerne les traitements intéressant la sûreté de l'État, la défense et la sécurité publique, la demande est adressée à la Commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener toutes investigations utiles et faire procéder aux modifications* nécessaires. *Celui-ci peut se faire assister d'un agent de la Commission. Il est notifié au requérant qu'il a été procédé aux vérifications ; que, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, il peut comprendre, d'une part, des informations dont la communication à l'intéressé serait susceptible de mettre en cause les fins assignées à ce traitement et, d'autre part, des informations dont la communication ne mettrait pas en cause ces mêmes fins, et notamment des décisions administratives ou juridictionnelles qui ont été ou auraient dû préalablement être communiquées à l'intéressé ; que, pour les premières, il incombe à la Commission nationale de l'informatique et des libertés, saisie par la personne visée par ces informations, de l'informer qu'il a été procédé aux vérifications nécessaires ; que, pour les autres, il appartient au gestionnaire du traitement ou à la Commission nationale de l'informatique et des libertés, saisis par cette personne, de lui en donner communication, avec, pour la Commission, l'accord du gestionnaire du traitement »* ;

Considérant qu'aux termes de l'article 6 du décret du 6 mai 1995 relatif au système informatique national du système d'information Schengen, le droit d'accès aux données enregistrées dans ce système informatique s'exerce auprès de la Commission nationale de l'informatique et des libertés, conformément aux articles 109 et 114 de la convention et à l'article 39 de la loi du 6 janvier 1978 susvisée sans préjudice des dispositions réglementaires relatives aux données susceptibles d'être consultées directement par l'intéressé exerçant ce droit ;

Sur les conclusions tendant à l'annulation de la décision de la Commission nationale de l'informatique et des libertés en tant qu'elle a refusé la communication des informations concernant M^me^ X. dans le système informatique national du système d'information Schengen ;

Considérant que M^me^ X. a eu, dans le cadre de l'instruction écrite devant le Conseil d'État, communication des informations concernant son inscription dans le système informatique national du système d'information Schengen ; que, dès lors, les conclusions de sa requête tendant à l'annulation pour excès de pouvoir de la déci-

sion de la Commission nationale de l'informatique et des libertés en tant qu'elle lui refuse la communication de ces informations sont devenues sans objet ;

Sur les conclusions tendant à l'annulation de la décision de la Commission nationale de l'informatique et des libertés en tant qu'elle a refusé de faire procéder aux rectifications des données concernant Mme X. et à l'annulation de la décision implicite du ministre de l'Intérieur ;

Considérant qu'il ressort de l'examen des pièces produites par la Commission nationale de l'informatique et des libertés que le signalement concernant Mme X. a été opéré par l'Allemagne ; que, par suite, les autorités françaises ne pouvaient rectifier elles-mêmes ces données ;

Considérant qu'il ressort des pièces du dossier, et notamment des éléments produits par les autorités allemandes, que les autorités françaises ont pu, sans commettre d'erreur manifeste d'appréciation, estimer qu'elles ne disposaient pas d'indices faisant présumer que les données introduites par les autorités allemandes étaient entachées d'erreur de droit ou de fait, justifiant ainsi une information des autorités de cet État et, le cas échéant, une saisine de l'autorité commune de contrôle, en application des stipulations des 2. et 3. de l'article 106 de la convention d'application de l'accord de Schengen ; que, par suite, Mme X. n'est pas fondée à demander l'annulation de la décision de la Commission nationale de l'informatique et des libertés en tant qu'elle a refusé de faire procéder à la rectification des données la concernant dans le système national informatique du système d'information Schengen et la décision implicite du ministre de l'Intérieur refusant cette rectification ; que, par voie de conséquence, ses conclusions aux fins d'injonction ne peuvent être accueillies ;

Sur les conclusions tendant à l'application des dispositions de l'article L. 761-1 du Code de justice administrative ;

Considérant que les dispositions de l'article L. 761-1 du Code de justice administrative font obstacle à ce que l'État qui n'est pas, dans la présente instance, la partie perdante soit condamnée à verser à Mme X. la somme que celle-ci demande au titre des frais exposés par elle et non compris dans les dépens ;

Décide :

Article 1er : les requêtes de Mme X. sont rejetées.

Article 2 : la présente décision sera notifiée à Mme X., à la Commission nationale de l'informatique et des libertés et au ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales.

ARRÊT DU CONSEIL D'ÉTAT DU 30 JUILLET 2003 (Req. n° 246870)

Vu la requête, enregistrée le 13 mai 2002 au secrétariat du contentieux du Conseil d'État, présentée par l'association La Défense Libre, l'association SOS Défense, et M. X., résidant... ; l'association La Défense Libre, l'association SOS Défense et M. X. demandent au Conseil d'État :
1) d'annuler la décision implicite par laquelle le président de la Commission nationale de l'informatique et des libertés (CNIL) a rejeté leur demande tendant à ce que le parquet de Lyon soit saisi à la suite du refus du procureur de la République de Lyon de leur donner accès aux données nominatives les concernant contenues dans les traitements automatisés tenus par le ministère public ;
2°) d'enjoindre à la Commission nationale de l'informatique et des libertés de saisir le parquet et d'adresser une copie de cette dénonciation au ministre de la Justice

dans un délai de trente jours à compter de la notification de la décision du Conseil d'État sous peine d'une astreinte de cent euros par jour ;
3°) de condamner la Commission nationale de l'informatique et des libertés à leur verser la somme de 1 000 euros au titre des frais irrépétibles ;

Vu les autres pièces du dossier ;

Vu le Code pénal et notamment ses articles 226-16 à 226-24 ;

Vu le Code de procédure pénale et notamment son article 40 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 81-1142 du 23 décembre 1981 instituant des contraventions de police en cas de violation de certaines dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le Code de justice administrative ;

Après avoir entendu en séance publique :
— le rapport de M. Herondart, auditeur ;
— les conclusions de M^{me} Mitjavile, Commissaire du gouvernement ;

Considérant qu'aux termes de l'article 21 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : *« Pour l'exercice de sa mission de contrôle, la Commission nationale de l'informatique et des libertés* [...] *4) adresse aux intéressés des avertissements et dénonce au parquet les infractions dont elle a connaissance, conformément à l'article 40 du Code de procédure pénale ;* [...] *6) reçoit les réclamations, pétitions et plaintes ;* [...] *; qu'aux termes du deuxième alinéa de l'article 40 du Code de procédure pénale* [:..] *Toute autorité constituée, ou officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs » ;*

Considérant qu'il ressort des pièces du dossier que, par un courrier en date du 2 août 1999, M. X. et les associations La Défense Libre et SOS Défense ont demandé au procureur de la République près le tribunal de grande instance de Lyon de leur délivrer copie des données les concernant contenues par les diverses banques de données tenues par le ministère public ; qu'ils ont saisi la Commission nationale de l'informatique et des libertés d'une demande le 31 octobre 1999 pour obtenir l'accès à ces données ; que le président de la Commission nationale de l'informatique et des libertés a adressé un courrier au procureur de la République le 8 décembre 1999 ; qu'en l'absence de réponse du procureur de la République, la Commission nationale de l'informatique et des libertés lui a adressé une nouvelle demande le 8 août 2000 ; que, par des courriers du 15 octobre 2000 et du 20 février 2001, M. X. a demandé à la Commission nationale de l'informatique et des libertés de saisir le parquet à la suite du refus du procureur de la République près le tribunal de grande instance de Lyon de lui donner accès aux données nominatives le concernant ; que M. X. demande l'annulation de la décision implicite par laquelle la Commission nationale de l'informatique et des libertés a rejeté ses demandes ;

Considérant qu'en vertu des dispositions précitées de l'article 21 de la loi du 6 janvier 1978 et de l'article 40 du Code de procédure pénale, il appartient à la Commission nationale de l'informatique et des libertés d'aviser le procureur de la République des faits dont elle a connaissance dans l'exercice de ses attributions, si ces faits lui paraissent suffisamment établis et si elle estime qu'ils portent une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'appli-

cation, dès lors que la méconnaissance de ces dispositions est constitutive d'un crime ou d'un délit ; qu'en revanche, ces dispositions ne font pas obligation à la Commission nationale de l'informatique et des libertés de dénoncer des faits susceptibles d'être punis d'une contravention de police ; que le fait de refuser de répondre aux demandes de renseignements ou de communication présentées en application des articles 34 et 35 de la loi du 6 janvier 1978 est passible des peines prévues pour les contraventions de cinquième classe, en application de l'article 1er du décret du 23 décembre 1981 instituant des contraventions de police en cas de violation de certaines dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; que, par suite, les requérants ne sont pas fondés à soutenir que la Commission nationale de l'informatique et des libertés ne pouvait légalement refuser de saisir le parquet du refus de communication dont ils s'estiment victimes ; que leurs conclusions tendant à l'annulation de cette décision doivent, par suite, être rejetées ainsi que, par voie de conséquence, leurs conclusions à fins d'injonction ;

Sur les conclusions tendant à l'application des dispositions de l'article L. 761-1 du Code de justice administrative ;

Considérant que les dispositions de l'article L. 761-1 du Code de justice administrative font obstacle à ce que l'État qui n'est pas, dans la présente instance, la partie perdante soit condamnée à verser aux requérants la somme que ceux-ci demandent au titre des frais exposés par eux et non compris dans les dépens ;

Décide :

Article 1er : la requête de M. X., de l'association La Défense Libre et de l'association SOS Défense est rejetée.

Article 2 : la présente décision sera notifiée à M. X., à l'association La Défense Libre, à l'association SOS Défense, à la Commission nationale de l'informatique et des libertés et au garde des Sceaux, ministre de la Justice.

TRIBUNAL DE GRANDE INSTANCE DE DRAGUIGNAN, JUGEMENT CORRECTIONNEL DU 18 SEPTEMBRE 2003 (N° 02/15014)

Contradictoire

Collecte de données nominatives par un moyen frauduleux, déloyal ou illicite

Entrave au fonctionnement d'un système de traitement automatisé de données

Après en avoir délibéré conformément à la loi, le tribunal a statué en ces termes :

Le tribunal :

Attendu que M. X. a été cité par exploit d'huissier de justice en date du 3 février 2003 à son domicile, pour comparaître à l'audience du 27 février 2003 ; que la citation est régulière en la forme ;

Attendu que l'affaire a fait l'objet de plusieurs renvois contradictoires ;

Attendu que M. X. est prévenu :

D'avoir à Fréjus (83), en tout cas dans le ressort du TGI de Draguignan, les 1er et 3 octobre 2002, en tout cas depuis temps non couvert par la prescription, en qualité de gérant de la SARL « ALPHA 3 NET » collecté par un moyen déloyal et conservé sur des fichiers textes (Wanadoo 2 et 3 txt et Wanadoo 4 et 5. txt) des milliers de données informatiques nominatives (adresses électroniques) ;

Faits prévus par l'article 226-18 al. 1 du Code pénal ; l'article 25 loi 78-17 du 6 janvier 1978 et réprimés par l'article 41 loi 78-17 du 6 janvier 1978 ; l'article 226-18 al. 1 et l'article 226-31 du Code pénal ;

D'avoir à Fréjus (83), en tout cas dans le ressort du TGI de Draguignan, les 1er et 3 octobre 2002, en tout cas depuis temps non couvert par la prescription. En qualité de gérant de la SARL « ALPHA 3 NET » entravé ou faussé le fonctionnement d'un système de traitement automatisé de données ; notamment en utilisant, sur un ordinateur de bureau, un logiciel automate de collecte d'adresses électroniques valides *(Directe Email Collector)* volontairement connecté à la cible non pré-désignée du serveur de messageries exploité par la société Wanadoo interactive, pour accéder à des adresses effectivement attribuées, soit une aspiration d'annuaire à raison de 23 millions de *spamming* ou d'attaques sur cinq machines du serveur de courrier ;

Faits prévus par l'article 323-2 du Code pénal, et réprimés par l'article 323-2 et l'article 323-5 du Code pénal ;

Sur l'action publique :

Le 3 octobre 2002, des services techniques de la societe Wanadoo interactive ont constaté un phénomène dénommé « aspiration d'annuaire » ;

Selon l'analyse du journal de connexion d'un serveur de mails sur une journée, 1 600 interrogations ont été recensées, destinées à vérifier la validité des adresses électroniques ;

Au total, il est apparu que sur les trois journées des 1er 2 et 3 octobre 2002, a été réalisée une aspiration d'annuaire à raison de 23 millions de *spamming* ou d'attaques sur cinq machines du serveur de courrier ;

Monsieur X., gérant de la société ALPHA 3 NET n'a pas contesté avoir téléchargé plusieurs logiciels, dont *Direct Email Collecter* permettant effectivement la récupération d'adresses électroniques valides et de fichiers d'adresses ainsi créés ;

Il a toutefois soutenu avoir seulement voulu tester ce logiciel, sans savoir qu'il sélectionnerait d'initiative le serveur courrier Wanadoo, lui-même ignorant au départ, quelle serait la cible de l'application ;

Ces affirmations se trouvent démenties par la procédure même d'utilisation du logiciel qui n'a pas la capacité à découvrir, seul, l'existence d'un quelconque serveur ;

L'infraction d'entrave au fonctionnement d'un système de traitement automatisé est caractérisée par le nombre massif des requêtes adressées par le logiciel utilisé par le prévenu, sur une très courte période, générant une diminution de la capacité du serveur ou comme c'est le cas en l'espèce — un ralentissement —, comme l'indique, lors de son audition, Madame Y., responsable des affaires générales de la société Wanadoo ;

L'infraction de collecte des données par un moyen déloyal est également constituée dans la mesure où Monsieur X. a procédé à l'extraction non autorisée d'une base de donnée, propriété de la société Wanadoo interactive, par l'utilisation d'un logiciel permettant, à moindre coût, de se procurer ce fichier ;

Attendu qu'il ressort des éléments du dossier que M. X. a réellement commis les faits qui lui sont reprochés ;

Qu'il convient en conséquence de le retenir dans les liens de la prévention et de le condamner à la peine prévue dans le dispositif du présent jugement ;

Sur l'action civile :

Attendu que la société Wanadoo interactive se constitue partie civile et sollicite la somme de 1 euro à titre de dommages et intérêts outre celle de 3 000 euros sur le fondement de l'article 475-1 du Code de procédure pénale. Elle sollicite également de voir ordonner la confiscation du disque dur saisi dans les locaux de l'entreprise de Monsieur X., outre la publication de la décision dans les journaux suivants : *Les Échos* et *01 Informatique* ;

Attendu que cette constitution de partie civile est régulière et recevable en la forme ;

Attendu que le tribunal possède les éléments d'appréciation suffisants pour condamner Monsieur X. à verser à la société Wanadoo interactive la somme de un euro à titre de dommages et intérêts outre celle de 600 euros sur le fondement de l'article 475-1 du Code de procédure pénale ;

Par ces motifs :

Sur l'action publique :

Statuant publiquement, en premier ressort et par jugement contradictoire, à l'égard de M. X. ;

Déclare M. X. coupable des faits qui lui sont reprochés ;

Condamne M. X. :

— à l'amende délictuelle de 15 000 00 euros ;
— à deux mois d'emprisonnement avec sursis ;

Ordonne la confiscation de l'objet de l'infraction en l'espèce le disque dur saisi dans les locaux de l'entreprise de Monsieur X. ;

Ordonne la publication par extrait dudit jugement dans les journaux : *Les Échos* et *01 Informatique* ;

Pour l'infraction de collecte de données nominatives par un moyen frauduleux, déloyal ou illicite ;

Pour l'infraction d'entrave au fonctionnement d'un système de traitement automatisé de données ;

Sitôt le prononcé du jugement, Madame le président donne au condamné l'avertissement prévu par l'article 132-29 du Code pénal ;

Madame le président a averti le condamné, que s'il commet une nouvelle infraction, il pourra faire l'objet d'une nouvelle condamnation qui sera susceptible d'entraîner l'exécution de la première condamnation sans confusion avec la seconde et qu'il encourra les peines de la récidive dans les termes des articles 132-9 à 132-10 du Code pénal ;

La présente décision est assujettie à un droit fixe de procédure d'un montant de 90 euros dont est redevable chaque condamné ;

Dit que la contrainte par corps s'exercera suivant les modalités fixées par les articles 749 et 750, 751 du Code de procédure pénale, modifiés par la loi du 30 décembre 1985 ;

Le tout en application des articles 406 et suivants et 485 du Code de procédure pénale et des textes susvisés ;

Sur l'action civile :

Statuant publiquement, en premier ressort et par jugement contradictoire, à l'égard de la société Wanadoo interactive ;

Reçoit la société Wanadoo interactive en sa constitution de partie civile ;

Condamne Monsieur X. à verser à la société Wanadoo interactive la somme de 1 euro à titre de dommages et intérêts, outre celle de 600 euros sur le fondement de l'article 475-1 du Code de procédure pénale ;

Condamne Monsieur X. aux dépens de l'action civile.

ARRÊT DE LA COUR DE JUSTICE DES COMMUNAUTÉS EUROPÉENNES DU 6 NOVEMBRE 2003 [1]
(C -101/01)

1

Par ordonnance du 23 février 2001, parvenue à la Cour le 1er mars suivant, le *Göta hovrätt* a posé, en application de l'article 234 CE, sept questions préjudicielles relatives, notamment, à l'interprétation de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*JO* L 281, p. 31).

2

Ces questions ont été soulevées dans le cadre d'une procédure pénale poursuivie devant ladite juridiction contre Mme Y., accusée d'avoir enfreint la législation suédoise relative à la protection des données à caractère personnel en publiant sur son site internet des données à caractère personnel concernant un certain nombre de personnes qui travaillent, comme elle, à titre bénévole dans une paroisse de l'église protestante de Suède.

Le cadre juridique

La législation communautaire

3

La directive 95/46 vise, ainsi qu'il ressort de son article 1er, paragraphe 1, la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

4

L'article 3 de la directive 95/46, relatif au champ d'application de celle-ci, dispose :
« 1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

« 2. La présente directive ne s'applique pas au traitement de données à caractère personnel : R. 11 mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal, R. 11 effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques ».

5

L'article 8 de la directive 95/46, intitulé « Traitements portant sur des catégories particulières de données », prévoit :

1 Langue de procédure : le suédois.

« 1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle ».

« 2. Le paragraphe 1 ne s'applique pas lorsque :
a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée ;
ou
b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates ;
ou
c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
ou
d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées ;
ou
e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ».

« 3. Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente ».

« 4. Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle ».

« 5. Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique ».

« Les États membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique ».

« 6. Les dérogations au paragraphe 1 prévues aux paragraphes 4 et 5 sont notifiées à la Commission ».

« 7. Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement ».

6

L'article 9 de la directive 95/46, intitulé « Traitements de données à caractère personnel et liberté d'expression », dispose : *« Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ».*

7

L'article 13 de la directive 95/46, intitulé « Exceptions et limitations », prévoit que les États membres peuvent apporter des restrictions à certaines obligations mises par la directive à la charge du responsable du traitement de données, notamment quant à l'information des personnes concernées, dans la mesure où lesdites restrictions sont nécessaires à la sauvegarde, par exemple, de la sûreté de l'État, de la défense, de la sécurité publique, d'un intérêt économique ou financier important d'un État membre ou de l'Union européenne, ainsi qu'à la recherche et à la poursuite d'infractions pénales ou de manquements à la déontologie de professions réglementées.

8

L'article 25 de la directive 95/46, qui figure au chapitre IV intitulé « Transfert de données à caractère personnel vers des pays tiers », est libellé comme suit :

« 1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat ».

« 2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont pris en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

« 3. Les États membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 ».

« 4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause ».

« 5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4 ».

« 6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes ».

« Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission ».

9

Lors de l'adoption de la directive 95/46, le royaume de Suède a fait au sujet de l'article 9 de celle-ci une déclaration inscrite au procès-verbal du Conseil (document n° 4649/95 du Conseil, du 2 février 1995), qui énonce : *« Le royaume de Suède considère que la notion d'expression artistique et littéraire renvoie aux moyens d'expression plutôt qu'au contenu de la communication ou à sa qualité ».*

10

La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »), prévoit, à son article 8, le droit au respect de la vie privée et familiale et contient, à son article 10, des dispositions relatives à la liberté d'expression.

La législation nationale

11

La directive 95/46 a été transposée en droit suédois, par la *Personuppgiftslag*, SFS 1998, n° 204 (loi suédoise sur les données à caractère personnel, ci-après la « PUL »).

L'affaire au principal et les questions préjudicielles

12

Outre, qu'elle occupait un emploi salarié d'agent d'entretien, M^me^ Y. exerçait la fonction de formatrice de communiants dans la paroisse d'Alseda (Suède). Elle a suivi un cours d'informatique dans le cadre duquel elle devait notamment créer une page d'accueil sur internet. À la fin de l'année 1998, M^me^ Y. a créé, à son domicile et avec son ordinateur personnel, des pages internet dans le but de permettre aux paroissiens préparant leur confirmation d'obtenir facilement les informations dont ils pouvaient avoir besoin. À sa demande, l'administrateur du site internet de l'église de Suède a établi un lien entre ces pages et ledit site.

13

Les pages visées contenaient des informations sur M^me^ Y. et dix-huit de ses collègues de la paroisse, y compris leur nom complet ou parfois seulement leur prénom. M^me^ Y. a en outre décrit les fonctions occupées par ses collègues et leurs loisirs en termes légèrement humoristiques. Dans plusieurs cas, leur situation familiale, leur numéro de téléphone et d'autres informations ont été mentionnés. Par ailleurs, elle a indiqué qu'une de ses collègues s'était blessée au pied et qu'elle était en congé de maladie partiel.

14

M^me^ Y. n'avait ni informé ses collègues de l'existence de ces pages, ni recueilli leur consentement, ni déclaré sa démarche à la *Datainspektion* (organisme public pour la protection des données transmises par voie informatique). Elle a supprimé les pages visées dès qu'elle a appris que celles-ci n'étaient pas appréciées par certains de ses collègues.

15

Le ministère public a engagé des poursuites à l'encontre de M^me^ Y. pour infraction à la PUL et a conclu à sa condamnation, au motif qu'elle avait :

— traité des données à caractère personnel, dans le cadre d'un traitement automatisé, sans faire de déclaration écrite préalable auprès de la *Datainspektion* (article 36 de la PUL) ;

— traité sans autorisation des données à caractère personnel sensibles, à savoir celles relatives à une blessure au pied et à un congé de maladie partiel (article 13 de la PUL) ;

— transféré vers des pays tiers des données à caractère personnel traitées sans autorisation (article 33 de la PUL).

16

M^me^ Y. a reconnu les faits, mais a nié avoir commis une infraction. Condamnée par l'*Eksjö tingsrätt* (Suède) au paiement d'une amende, M^me^ Y. a interjeté appel de cette décision devant la juridiction de renvoi.

17

L'amende s'élevait à 4 000 SEK, compte tenu de l'application à la somme de 100 SEK, calculée en fonction de la situation financière de M^me^ Y., d'un multiplicateur de quarante, représentant la sévérité de l'infraction. M^me^ Y. a en outre été condamnée à verser 300 SEK à un fonds suédois destiné à aider les victimes d'infractions.

18

Éprouvant des doutes, sur l'interprétation du droit communautaire applicable en la matière, notamment de la directive 95/46, le *Göta hovrätt* a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) La mention d'une personne — par son nom ou par son nom et son numéro de téléphone — sur une page d'accueil sur internet est-elle une opération qui relève du champ d'application de la directive [95/46] *? Le fait de faire figurer, sur une page d'accueil sur internet que l'on a soi-même construite, un certain nombre de personnes, ainsi que des affirmations et des déclarations sur les* conditions de travail et les passe-temps de ces personnes, constitue-t-il un traitement de données à caractère personnel, automatisé en tout ou en partie ? ».

« 2) Au cas où la question précédente appellerait une réponse négative, le fait de créer, sur une page d'accueil sur internet, des pages spécifiques pour une bonne quinzaine de personnes, avec des liens entre les pages qui permettent une recherche par prénom, peut-il être considéré comme constituant un »traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier« au sens de l'article 3, paragraphe 1 ? ».

Si l'une des questions précédentes appelle une réponse affirmative, le *hovrätt* pose en outre les questions suivantes :

« 3) Le fait d'insérer des données de ce type sur des collègues de travail sur une page d'accueil privée, qui est cependant accessible à tous ceux qui connaissent l'adresse de la page, peut-il être considéré comme échappant au champ d'application de la directive [95/46] *en vertu de l'une des exceptions figurant à l'article 3, paragraphe 2 ? ».*

« 4) L'indication, sur une page d'accueil, qu'un collègue de travail mentionné par son nom s'est blessé au pied et est en congé de maladie partiel est-elle une donnée à caractère personnel relative à la santé qui, aux termes de l'article 8, paragraphe 1, ne peut faire l'objet d'un traitement ? ».

« 5) Le transfert de données à caractère personnel vers des pays tiers est interdit dans certains cas en vertu de la directive [95/46]. *Si une personne insère, en*

Suède, à l'aide d'un ordinateur, des données à caractère personnel sur une page d'accueil qui est stockée sur un serveur en Suède — de sorte que les données à caractère personnel deviennent accessibles à des ressortissants de pays tiers —, cela constitue-t-il un transfert de données vers des pays tiers au sens de la directive [95/46] *? La réponse reste-t-elle la même si, selon les informations dont nous disposons, aucun ressortissant d'un pays tiers n'a en fait pris connaissance des données ou si le serveur en question se trouve, d'un point de vue purement physique, dans un pays tiers ? ».*

« 6) Les dispositions de la directive [95/46] *peuvent-elles, dans un cas tel que celui de l'espèce, être considérées comme impliquant une restriction contraire aux principes généraux de liberté d'expression ou à d'autres droits et libertés applicables dans l'Union européenne et qui correspondent notamment à l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ? ».*

Enfin, le *hovrätt* pose la question suivante :

« 7) Un État membre peut-il, dans les domaines visés par les questions qui précèdent, disposer d'une protection plus forte des données à caractère personnel ou d'un champ d'application plus large que celui qui résulte de la directive [95/46], *même lorsque l'on ne se trouve pas en présence de l'un des intérêts mentionnés à l'article 13 ? ».*

Sur la première question

19

Par sa première question, la juridiction de renvoi demande si l'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un « traitement de données à caractère personnel, automatisé en tout ou en partie », au sens de l'article 3, paragraphe 1, de la directive 95/46.

Observations soumises à la Cour

20

Selon M^me^ Y., il n'est pas raisonnable de considérer que la simple mention du nom d'une personne ou de données à caractère personnel dans un texte contenu sur une page internet constitue un traitement automatisé de données. En revanche, la mention de telles données dans un mot clé des « balises méta » *(meta tags)* d'une page internet, qui permet de procéder à une indexation et de trouver cette page par un moteur de recherche, pourrait constituer un tel traitement.

21

Le gouvernement suédois soutient que la notion de « traitement de données à caractère personnel, automatisé en tout ou en partie », telle que visée à l'article 3, paragraphe 1, de la directive 95/46, inclut tout traitement sous un format informatique, c'est-à-dire en format binaire. Par conséquent, dès lors qu'une donnée à caractère personnel est traitée au moyen d'un ordinateur, que ce soit par exemple au moyen d'un programme de traitement de texte ou afin de l'insérer sur une page internet, elle ferait l'objet d'un traitement couvert par la directive 95/46.

22

Le gouvernement néerlandais fait valoir que l'insertion de données à caractère personnel sur une page internet se fait à l'aide d'un ordinateur et d'un serveur, ce qui constituerait une caractéristique importante de l'automatisation, de sorte qu'il faudrait considérer que ces données font l'objet d'un traitement automatisé.

23
La Commission soutient que la directive 95/46 s'applique à tout traitement de données à caractère personnel visé à l'article 3 de celle-ci, indépendamment des moyens techniques utilisés. La mise à disposition de données à caractère personnel sur internet constituerait par conséquent un traitement automatisé, en tout ou en partie, à condition qu'il n'existe pas de limitations techniques qui restreignent le traitement à une opération exclusivement manuelle. Une page internet relèverait donc, par sa nature même, du champ d'application de la directive 95/46.

Réponse de la Cour

24
La notion de « données à caractère personnel » employée à l'article 3, paragraphe 1, de la directive 95/46 englobe, conformément à la définition figurant à l'article 2, sous a), de celle-ci, *« toute information concernant une personne physique identifiée ou identifiable »*. Cette notion comprend assurément le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps.

25
Quant à la notion de « traitement » de telles données employées à l'article 3, paragraphe 1, de la directive 95/46, elle comprend, conformément à la définition figurant à l'article 2, sous b), de celle-ci, *« toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel »*. Cette dernière disposition mentionne plusieurs exemples de telles opérations, parmi lesquels figurent la communication par transmission, la diffusion ou toute autre forme de mise à disposition de données. Il s'ensuit que l'opération consistant à faire figurer, sur une page internet, des données à caractère personnel est à considérer comme un tel traitement.

26
Reste à déterminer si ce traitement est « automatisé en tout ou en partie ». À cet égard, il convient de relever que faire apparaître des informations sur une page internet implique, selon les procédures techniques et informatiques appliquées actuellement, de réaliser une opération de chargement de cette page sur un serveur ainsi que les opérations nécessaires pour rendre cette page accessible aux personnes qui se sont connectées à internet. Ces opérations sont effectuées, au moins en partie, de manière automatisée.

27
Il convient donc de répondre à la première question que l'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un « traitement de données à caractère personnel, automatisé en tout ou en partie », au sens de l'article 3, paragraphe 1, de la directive 95/46.

Sur la deuxième question

28
La première question, ayant reçu une réponse affirmative, il n'y a pas lieu de répondre à la deuxième question, qui n'a été posée que pour le cas où la première question appellerait une réponse négative.

Sur la troisième question

29
Par sa troisième question la juridiction nationale cherche en substance à savoir si un traitement de données à caractère personnel tel que celui visé par la première ques-

tion relève de l'une des exceptions figurant à l'article 3, paragraphe 2, de la directive 95/46.

Observations soumises à la Cour

30

M^me^ Y. soutient qu'une personne privée qui, usant de sa liberté d'expression, crée des pages internet dans le cadre d'une activité à but non lucratif ou de ses loisirs n'exerce pas une activité économique et échappe donc à l'application du droit communautaire. Si la Cour devait juger le contraire, se poserait alors la question de la validité de la directive 95/46, car, en l'adoptant, le législateur communautaire aurait outrepassé les compétences qui lui ont été conférées par l'article 100 A du traité CE (devenu, après modification, article 95 CE). En effet, le rapprochement des législations, qui aurait pour objet l'établissement et le fonctionnement du marché intérieur, ne saurait servir de base légale pour des mesures communautaires qui réglementent le droit des personnes privées à la liberté d'expression sur internet.

31

Le gouvernement suédois fait valoir que, lors de la transposition de la directive 95/46 en droit interne, le législateur suédois a considéré que le traitement de données à caractère personnel par une personne physique consistant à transmettre ces données à un nombre indéterminé de destinataires, par exemple au moyen d'internet, ne pouvait être qualifié d'*« activité exclusivement personnelle ou domestique »* au sens de l'article 3, paragraphe 2, second tiret, de la directive 95/46. En revanche, ce gouvernement n'exclut pas que l'exception prévue au premier tiret de ce paragraphe vise les cas où une personne physique publie des données à caractère personnel sur une page internet dans le seul cadre de l'exercice de sa liberté d'expression et sans aucun lien avec une activité professionnelle ou commerciale.

32

Selon le gouvernement néerlandais, un traitement automatisé de données tel que celui en cause au principal ne relève d'aucune des exceptions visées à l'article 3, paragraphe 2, de la directive 95/46. S'agissant plus particulièrement de l'exception prévue au second tiret de ce paragraphe, il relève que le créateur d'une page internet porte les données qui y ont été introduites à la connaissance d'un groupe de personnes qui est, en principe, indéterminé.

33

La Commission fait valoir qu'une page internet telle que celle en cause au principal ne peut pas être considérée comme échappant au champ d'application de la directive 95/46 en vertu de l'article 3, paragraphe 2, de celle-ci, mais constitue, compte tenu des finalités de la page internet en cause au principal, une création artistique et littéraire au sens de l'article 9 de ladite directive.

34

Elle considère que l'article 3, paragraphe 2, premier tiret, de la directive 95/46 se prête à deux interprétations différentes. L'une consisterait à limiter la portée de cette disposition aux domaines cités comme exemples, à savoir des activités qui relèvent essentiellement de ce qu'il est convenu d'appeler les deuxième et troisième piliers. L'autre interprétation consisterait à exclure du champ d'application de la directive 95/46 l'exercice de toute activité qui ne relève pas du droit communautaire.

35

La Commission soutient que le droit communautaire ne se limite pas aux seules activités économiques liées aux quatre libertés fondamentales. Se référant à la base juridique de la directive 95/46, à son objectif, à l'article 6 UE, à la charte des droits fondamentaux de l'Union européenne, proclamée à Nice le 18 décembre 2000

(*JOCE* 364, p. 1), et à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, elle conclut que cette directive vise à réglementer la libre circulation de données à caractère personnel comme l'exercice non seulement d'une activité économique, mais également d'une activité sociale dans le cadre de l'intégration et du fonctionnement du marché intérieur.

36

Elle ajoute qu'exclure d'une manière générale du champ d'application de la directive 95/46 les pages internet qui ne contiennent aucun élément commercial ou de prestation de services pourrait entraîner de graves problèmes de délimitation. Un grand nombre de pages internet contenant des données à caractère personnel, destinées à stigmatiser certaines personnes dans des buts particuliers, pourraient alors se trouver exclues du champ d'application de cette directive.

Réponse de la Cour

37

L'article 3, paragraphe 2, de la directive 95/46 prévoit deux exceptions au champ d'application de celle-ci.

38

La première exception concerne les traitements de données à caractère personnel, mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal.

39

Les activités de M^me^ Y. en cause au principal étant essentiellement non pas économiques mais bénévoles ainsi que religieuses, il convient d'examiner si elles constituent des traitements de données à caractère personnel *« mis en* œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire » au sens de l'article 3, paragraphe 2, premier tiret, de la directive 95/46.

40

La Cour a déjà jugé à propos de la directive 95/46, fondée sur l'article 100 A du traité, que le recours à cette base juridique ne présuppose pas l'existence d'un lien effectif avec la libre circulation entre États membres dans chacune des situations visées par l'acte fondé sur une telle base (voir arrêt du 20 mai 2003, *Österreichischer Rundfunk e. a., C-465/00, C-138/01* et *C-139/01*, non encore publié au Recueil, point 41 et jurisprudence citée).

41

Une interprétation contraire risquerait de rendre les limites du domaine d'application de ladite directive particulièrement incertaines et aléatoires, ce qui serait contraire à l'objectif essentiel de celle-ci, qui est de rapprocher les dispositions législatives, réglementaires et administratives des États membres afin d'éliminer les obstacles au fonctionnement du marché intérieur découlant précisément des disparités entre les législations nationales (arrêt *Österreichischer Rundfunk e. a.*, précité, point 42).

42

Dans ces conditions, il ne serait pas approprié d'interpréter l'expression *« activités qui ne relèvent pas du champ d'application du droit communautaire »* comme ayant une portée telle qu'il serait nécessaire de vérifier, au cas par cas, si l'activité spécifique en cause affecte directement la libre circulation entre États membres.

43
Les activités mentionnées à titre d'exemples à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 (à savoir les activités prévues aux titres V et VI du traité sur l'Union européenne ainsi que les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités relatives à des domaines du droit pénal) sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers.

44
Il y a donc lieu de considérer que les activités mentionnées en tant qu'exemples à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 sont destinées à définir la portée de l'exception y prévue, de sorte que cette exception ne s'applique qu'aux activités qui y sont ainsi expressément mentionnées ou qui peuvent être rangées dans la même catégorie *(ejusdem generis)*.

45
Or, des activités bénévoles ou religieuses, telles que celles exercées par M^me^ Y., ne sont pas assimilables aux activités mentionnées à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 et ne sont donc pas couvertes par cette exception.

46
S'agissant de l'exception prévue à l'article 3, paragraphe 2, second tiret, de la directive 95/46, le douzième considérant de celle-ci, relatif à cette exception, mentionne en tant qu'exemples de traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques la correspondance et la tenue de répertoires d'adresses.

47
Cette exception doit donc être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes.

48
Il convient donc, de répondre à la troisième question qu'un traitement de données à caractère personnel tel que celui mentionné dans la réponse à la première question ne relève d'aucune des exceptions figurant à l'article 3, paragraphe 2, de la directive 95/46.

Sur la quatrième question

49
Par sa quatrième question, la juridiction de renvoi demande, si l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46.

50
Eu égard à l'objet de cette directive, il convient de donner à l'expression *« données relatives à la santé »* employée à son article 8, paragraphe 1, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne.

51
Il convient donc de répondre à la quatrième question que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46.

Sur la cinquième question

52

Par sa cinquième question, la juridiction de renvoi, cherche en substance à savoir s'il existe un *« transfert vers un pays tiers de données »* au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page internet, stockée auprès d'une personne physique ou morale qui héberge le site internet sur lequel la page peut être consultée (ci-après le « fournisseur de services d'hébergement ») et qui est établie dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à internet, y compris des personnes se trouvant dans des pays tiers. La juridiction de renvoi demande en outre si la réponse à cette question est identique lorsqu'il apparaît que, en fait, aucun ressortissant d'un pays tiers n'a pris connaissance de ces données ou que le serveur où la page est stockée se trouve, d'un point de vue purement physique, dans un pays tiers.

Observations soumises à la Cour

53

La Commission et le gouvernement suédois, considèrent que l'insertion, à l'aide d'un ordinateur, de données à caractère personnel sur une page internet, de sorte que celles-ci deviennent accessibles à des ressortissants de pays tiers, constitue un transfert de données vers des pays tiers au sens de la directive 95/46. La réponse serait identique si aucun ressortissant d'un pays tiers ne prenait effectivement connaissance desdites données ou si le serveur où celles-ci sont stockées se trouvait, d'un point de vue purement physique, dans un pays tiers.

54

Le gouvernement néerlandais rappelle que la notion de « transfert », n'est pas définie par la directive 95/46. Il considère, d'une part, que cette notion doit être entendue comme visant un acte tendant délibérément à transférer des données à caractère personnel du territoire d'un État membre vers un pays tiers et, d'autre part, qu'une distinction ne peut être établie entre les différentes formes sous lesquelles des données sont rendues accessibles à des tiers. Il en conclut que l'introduction de données à caractère personnel sur une page internet au moyen d'un ordinateur ne peut pas être considérée comme un transfert vers un pays tiers de données à caractère personnel au sens de l'article 25 de la directive 95/46.

55

Le gouvernement du Royaume-Uni, fait valoir que l'article 25 de la directive 95/46 vise les transferts de données vers des pays tiers et non leur accessibilité à partir de pays tiers. La notion de « transfert » impliquerait la transmission d'une donnée par une personne située dans un lieu précis à une tierce personne située dans un autre lieu. Ce ne serait que dans l'hypothèse d'un tel transfert que l'article 25 de la directive 95/46 impose aux États membres de veiller au caractère adéquat du niveau de protection des données à caractère personnel dans un pays tiers.

Réponse de la Cour

56

La directive 95/46 ne définit ni à son article 25, ni dans aucune autre disposition, notamment pas à son article 2, la notion de « transfert vers un pays tiers ».

57

Afin de déterminer si l'inscription sur une page internet de données à caractère personnel, du seul fait qu'elle les rend accessibles aux personnes se trouvant dans un pays tiers, constitue un « transfert » de ces données vers un pays tiers au sens de l'article 25 de la directive 95/46, il est nécessaire de tenir compte, d'une part, de la

nature technique des opérations ainsi effectuées et, d'autre part, de l'objectif ainsi que de l'économie du chapitre IV de ladite directive, où figure son article 25.

58
Les informations qui se trouvent sur internet peuvent être consultées par un nombre indéfini de personnes résidant dans des lieux multiples et presque à tout moment. Le caractère ubiquitaire de ces informations résulte notamment du fait que les moyens techniques utilisés dans le cadre d'internet sont relativement simples et de moins en moins coûteux.

59
Selon les modalités d'utilisation d'internet, telles qu'elles sont devenues disponibles à des particuliers comme M^me^ Y. au cours des années 90, l'auteur d'une page destinée à être publiée sur internet transmet les données qui constituent cette page à son fournisseur de services d'hébergement. Celui-ci gère l'infrastructure informatique nécessaire pour assurer le stockage de ces données et la connexion du serveur qui héberge le site internet. Cela permet la transmission ultérieure de ces données à toute personne qui s'est connectée à internet et demande à les obtenir. Les ordinateurs qui constituent cette infrastructure informatique peuvent être situés, et même sont souvent situés, dans un ou plusieurs pays autres que celui du lieu d'établissement du fournisseur de services d'hébergement, sans que la clientèle de celui-ci en ait ou puisse raisonnablement en prendre connaissance.

60
Il ressort du dossier que, pour obtenir les informations figurant sur les pages internet dans lesquelles M^me^ Y. avait inséré des données relatives à ses collègues, un utilisateur d'internet devait non seulement se connecter à celui-ci mais aussi effectuer, par une démarche personnelle, les actions nécessaires pour consulter lesdites pages. En d'autres termes, les pages internet de M^me^ Y. ne comportaient pas les mécanismes techniques qui auraient permis l'envoi automatique de ces informations à des personnes qui n'avaient pas délibérément cherché à accéder à ces pages.

61
Il s'ensuit que, dans des circonstances telles que celles de l'espèce au principal, les données à caractère personnel qui arrivent sur l'ordinateur d'une personne située dans un pays tiers, en provenance d'une personne qui les a chargées sur un site internet, n'ont pas été transférées directement entre ces deux personnes mais au travers de l'infrastructure informatique du fournisseur de services d'hébergement où la page est stockée.

62
C'est dans ce contexte qu'il est nécessaire d'examiner si le législateur communautaire avait l'intention, aux fins de l'application du chapitre IV de la directive 95/46, d'inclure dans la notion de « transfert vers un pays tiers de données » au sens de l'article 25 de cette directive des opérations telles que celles effectuées par M^me^ Y. Il faut souligner que la cinquième question posée par la juridiction de renvoi ne concerne que ces opérations, à l'exclusion de celles effectuées par les fournisseurs de services d'hébergement.

63
Le chapitre IV de la directive 95/46, dans lequel figure l'article 25, met en place un régime spécial, comportant des règles spécifiques, qui vise à assurer un contrôle par les États membres des transferts de données à caractère personnel vers les pays tiers. Ce chapitre institue un régime complémentaire au régime général mis en place par le chapitre II de ladite directive concernant la licéité de traitements de données à caractère personnel.

64
L'objectif du chapitre IV est défini du 56e au 60e considérants de la directive 95/46, lesquels énoncent notamment que, si la protection des personnes garantie, dans la Communauté par cette directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat, ce caractère adéquat doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts. Lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit.

65
L'article 25 de la directive 95/46 impose pour sa part une série d'obligations aux États membres et à la Commission, visant à contrôler les transferts de données à caractère personnel vers les pays tiers compte tenu du niveau de protection accordé à de telles données dans chacun de ces pays.

66
En particulier, l'article 25, paragraphe 4, de la directive 95/46 prévoit que, lorsque la Commission constate qu'un pays tiers n'assure pas un niveau de protection adéquat, les États membres prennent les mesures nécessaires en vu d'empêcher tout transfert de données à caractère personnel vers le pays tiers en cause.

67
Le chapitre IV de la directive 95/46 ne contient aucune disposition concernant l'utilisation d'internet. Il ne précise notamment pas les critères permettant de déterminer si, en ce qui concerne les opérations effectuées par l'intermédiaire de fournisseurs de services d'hébergement, il convient de se fonder sur le lieu de l'établissement du fournisseur ou son domicile professionnel ou bien sur le ou les lieux où sont situés les ordinateurs qui constituent l'infrastructure informatique du fournisseur.

68
Eu égard, d'une part, à l'état du développement d'internet à l'époque de l'élaboration de la directive 95/46 et, d'autre part, à l'absence, dans son chapitre IV, de critères applicables à l'utilisation d'internet, on ne saurait présumer que le législateur communautaire avait l'intention d'inclure prospectivement dans la notion de « transfert vers un pays tiers de données » l'inscription, par une personne se trouvant dans la situation de Mme Y., de données sur une page internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers possédant les moyens techniques d'y accéder.

69
Si l'article 25 de la directive 95/46 était interprété en ce sens qu'il existe un « transfert vers un pays tiers de données » chaque fois que des données à caractère personnel sont chargées sur une page internet, ce transfert serait nécessairement un transfert vers tous les pays tiers où existent les moyens techniques nécessaires pour accéder à internet. Le régime spécial prévu par le chapitre IV de ladite directive deviendrait donc nécessairement, en ce qui concerne les opérations sur internet, un régime d'application générale. En effet, dès que la Commission constaterait, en application de l'article 25, paragraphe 4, de la directive 95/46, qu'un seul pays tiers n'assure pas un niveau de protection adéquat, les États membres seraient obligés d'empêcher toute mise sur internet de données à caractère personnel.

70
Dans ces conditions, il y a lieu de conclure que l'article 25 de la directive 95/46 doit être interprété en ce sens que des opérations telles que celles effectuées par Mme Y. ne constituent pas en elles-mêmes un « transfert vers un pays tiers de données ».

Il n'est donc pas nécessaire de rechercher si une personne d'un pays tiers a eu accès à la page internet concernée ou si le serveur de ce fournisseur est physiquement situé dans un pays tiers.

71

Il convient donc de répondre à la cinquième question qu'il n'existe pas de « transfert vers un pays tiers de données » au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page internet, stockée auprès de son fournisseur de services d'hébergement qui est établi dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à internet, y compris des personnes se trouvant dans des pays tiers.

Sur la sixième question

72

Par sa sixième question la juridiction de renvoi, demande s'il faut considérer que les dispositions de la directive 95/46 comportent, dans un cas comme celui de l'espèce au principal, une restriction contraire au principe général de la liberté d'expression ou à d'autres droits et libertés applicables dans l'Union européenne et correspondant notamment au droit prévu à l'article 10 de la CEDH.

Observations soumises à la Cour

73

Se référant, notamment, à l'arrêt du 6 mars 2001, *Connolly/Commission C-274/99 P*, Rec. p. I-1611, M^me^ Y. fait valoir que la directive 95/46 et la PUL, en ce qu'elles prévoient des conditions de consentement préalable et de notification préalable à une autorité de contrôle ainsi qu'un principe d'interdiction du traitement des données à caractère personnel de nature sensible, sont contraire au principe général de la liberté d'expression reconnu en droit communautaire. Plus particulièrement, elle soutient que la définition du « traitement de données à caractère personnel, automatisé en tout ou en partie », ne satisfait pas aux critères de prévisibilité et de précision.

74

En outre, selon elle le simple fait de citer nominativement une personne physique, de révéler ses coordonnées téléphoniques et ses conditions de travail ainsi que de donner des informations sur son état de santé et ses loisirs, informations qui seraient publiques, notoirement connues ou triviales, n'est pas constitutif d'une violation substantielle du droit au respect de la vie privée. M^me^ Y. considère que, en tout état de cause, les contraintes imposées par la directive 95/46 sont disproportionnées au regard de l'objectif recherché de protection de la réputation et de la vie privée d'autrui.

75

Le gouvernement suédois considère que la directive 95/46 permet de mettre en balance les intérêts en cause et, ainsi, de sauvegarder la liberté d'expression et la protection de la vie privée. Il ajoute que seul le juge national peut, compte tenu des circonstances de chaque cas particulier, apprécier la proportionnalité de la restriction à l'exercice du droit à la liberté d'expression qu'entraîne l'application de règles visant à la protection des droits d'autrui.

76

Le gouvernement néerlandais rappelle que tant la liberté d'expression que le droit au respect de la vie privée font partie des principes généraux du droit dont la Cour assure le respect et que la CEDH n'établit aucune hiérarchie entre les différents droits fondamentaux. Il considère dès lors que la juridiction nationale doit s'efforcer de

concilier les différents droits fondamentaux en cause en prenant en considération les circonstances du cas d'espèce.

77

Le gouvernement du Royaume-Uni note que sa proposition de réponse à la cinquième question, exposée au point 55 du présent arrêt, s'accorde parfaitement avec les droits fondamentaux, et permet d'éviter de porter atteinte de manière disproportionnée à la liberté d'expression. Il ajoute qu'une interprétation qui aurait pour effet qu'une publication de données à caractère personnel sous une forme particulière, à savoir sur une page internet, soit sujette à des restrictions beaucoup plus sévères que celles applicables aux publications réalisées sous d'autres formes de publication, telles que le papier, serait difficile à justifier.

78

La Commission soutient également que la directive 95/46 n'implique pas une restriction contraire au principe général de la liberté d'expression ou à d'autres droits et libertés applicables dans l'Union européenne et correspondant notamment au droit prévu à l'article 10 de la CEDH.

Réponse de la Cour

79

Il ressort du septième considérant de la directive 95/46 que l'établissement et le fonctionnement du marché intérieur, sont susceptibles d'être sérieusement affectés par les différences entre les régimes nationaux applicables au traitement des données à caractère personnel. Selon le troisième considérant de la même directive, l'harmonisation de ces régimes nationaux doit avoir pour objectifs non seulement la libre circulation de ces données entre États membres, mais également la sauvegarde des droits fondamentaux des personnes.

Ces objectifs peuvent évidemment entrer en conflit.

80

D'une part, l'intégration économique et sociale résultant de l'établissement et du fonctionnement du marché intérieur entraînera nécessairement une augmentation sensible des flux de données à caractère personnel entre tous les acteurs de la vie économique et sociale des États membres, qu'il s'agisse d'entreprises ou d'administrations des États membres. Lesdits acteurs ont, dans une certaine mesure, besoin de disposer de données à caractère personnel pour effectuer leurs transactions ou pour accomplir leur mission dans le cadre de l'espace sans frontières que constitue le marché intérieur.

81

D'autre part, les personnes concernées par le traitement de données à caractère personnel demandent à juste titre que ces données soient protégées de manière efficace.

82

Les mécanismes permettant de mettre en balance ces différents droits et intérêts sont inscrits, d'une part, dans la directive 95/46 elle-même, en ce qu'elle prévoit des règles qui déterminent dans quelles situations et dans quelle mesure le traitement des données à caractère personnel est licite et quelles sauvegardes doivent être prévues. D'autre part, ils résultent de l'adoption, par les États membres, de dispositions nationales assurant la transposition de cette directive et de l'éventuelle application de celles-ci par les autorités nationales.

83

Quant à la directive 95/46 elle-même, ses dispositions sont nécessairement relativement générales vu qu'elle doit s'appliquer à un grand nombre de situations très diverses. Contrairement à ce que prétend M^me^ Y., c'est donc à juste titre que cette

directive comporte des règles caractérisées par une certaine souplesse et qu'elle laisse dans de nombreux cas aux États membres le soin d'arrêter les détails ou de choisir parmi des options.

84
Il est vrai que les États membres disposent à maints égards d'une marge de manœuvre en vue de la transposition de la directive 95/46. Toutefois, rien ne permet de considérer que le régime que celle-ci prévoit manque de prévisibilité ou que ses dispositions sont, en tant que telles, contraires aux principes généraux du droit communautaire et, notamment, aux droits fondamentaux protégés par l'ordre juridique communautaire.

85
C'est donc plutôt au stade de la mise en œuvre sur le plan national de la réglementation transposant la directive 95/46 dans des cas d'espèce particuliers que doit être trouvé, un juste équilibre des droits et intérêts visés.

86
Dans ce contexte, les droits fondamentaux revêtent une importance particulière, ainsi que le démontre l'affaire au principal où il est en substance nécessaire de mettre en balance, d'une part, la liberté d'expression de M^me^ Y. dans le cadre de son travail comme formatrice de communiants ainsi que la liberté d'exercer des activités contribuant à la vie religieuse et, d'autre part, la protection de la vie privée des personnes à propos desquelles M^me^ Y. a fait figurer des données sur son site internet.

87
Par conséquent, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme à la directive 95/46, mais également de veiller à ne pas se fonder sur une interprétation de cette dernière qui entrerait en conflit avec les droits fondamentaux protégés par l'ordre juridique communautaire ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité.

88
S'il est vrai que la protection de la vie privée requiert l'application de sanctions efficaces à l'encontre des personnes traitant des données à caractère personnel, d'une manière non conforme à la directive 95/46, de telles sanctions doivent toujours respecter le principe de proportionnalité. Il en va d'autant plus ainsi que le champ d'application de la directive 95/46 apparaît très large et que les obligations des personnes qui procèdent à des traitements de données à caractère personnel sont nombreuses et importantes.

89
En application du principe de proportionnalité, il incombe à la juridiction de renvoi de prendre en considération toutes les circonstances de l'affaire dont elle est saisie, notamment la durée de la violation des règles mettant en œuvre la directive 95/46 ainsi que l'importance, pour les intéressés, de la protection des données divulguées.

90
Il convient donc de répondre à la sixième question que les dispositions de la directive 95/46 ne comportent pas en elles-mêmes, une restriction contraire au principe général de la liberté d'expression ou à d'autres droits et libertés applicables dans l'Union européenne et correspondant notamment à l'article 10 de la CEDH. Il appartient aux autorités et aux juridictions nationales chargées d'appliquer la réglementation nationale transposant la directive 95/46 d'assurer un juste équilibre des droits et intérêts en cause, y compris les droits fondamentaux protégés par l'ordre juridique communautaire.

Sur la septième question

91

Par sa septième question, la juridiction de renvoi demande en substance, s'il est loisible aux États membres de prévoir une protection des données à caractère personnel plus forte ou un champ d'application plus large que ceux résultant de la directive 95/46.

Observations soumises à la Cour

92

Le gouvernement suédois affirme que la directive 95/46 ne se contente pas de fixer des conditions minimales de protection des données à caractère personnel. Les États membres seraient, dans le cadre de la transposition de cette directive, obligés de réaliser le niveau de protection fixé par celle-ci et ils ne seraient pas habilités à prévoir une protection plus forte ou plus faible. Toutefois, il conviendrait de tenir compte de la marge d'appréciation dont disposent les États membres lors de ladite transposition pour préciser dans leur droit interne les conditions générales de licéité du traitement des données à caractère personnel.

93

Le gouvernement néerlandais soutient que la directive 95/46 ne s'oppose pas à ce que les États membres prévoient une protection plus forte dans certains domaines. Il ressortirait par exemple des articles 10, 11, paragraphe 1, 14, premier alinéa, sous a), 17, paragraphe 3, 18, paragraphe 5, et 19, paragraphe 1, de ladite directive que les États membres peuvent prévoir une protection plus large. En outre, les États membres seraient libres d'appliquer les principes de la directive 95/46 également à des activités qui ne relèvent pas du champ d'application de celle-ci.

94

La Commission fait valoir que la directive 95/46 est fondée sur l'article 100 A du traité et que, si un État membre souhaite maintenir, ou instaurer une législation qui déroge, à une telle directive d'harmonisation, il est tenu de la notifier à la Commission conformément au paragraphe 4 ou au paragraphe 5 de l'article 95 CE. La Commission soutient en conséquence qu'un État membre ne saurait prévoir une protection des données à caractère personnel plus étendue ou un champ d'application plus large que ceux qui résultent de ladite directive.

Réponse de la Cour

95

La directive 95/46 vise ainsi qu'il ressort notamment de son huitième considérant, à rendre équivalent dans tous les États membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. Son dixième considérant ajoute que le rapprochement des législations nationales applicables en la matière ne doit pas conduire à affaiblir la protection qu'elles assurent, mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté.

96

L'harmonisation desdites législations nationales ne se limite donc pas à une harmonisation minimale, mais aboutit à une harmonisation qui est, en principe, complète. C'est dans cette optique que la directive 95/46 entend assurer la libre circulation des données à caractère personnel, tout en garantissant un haut niveau de protection des droits et des intérêts des personnes visées par ces données.

97

Il est vrai que la directive 95/46 reconnaît aux États membres une marge de manœuvre dans certains domaines, et qu'elle les autorise à maintenir ou à introduire

des régimes particuliers pour des situations spécifiques ainsi qu'en témoignent un grand nombre de ses dispositions. Toutefois, de telles possibilités doivent être utilisées de la manière prévue par la directive 95/46 et conformément à son objectif consistant à maintenir un équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée.

98

En revanche, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46, à des domaines non inclus dans le champ d'application de cette dernière, pour autant, qu'aucune autre disposition du droit communautaire n'y fasse obstacle.

99

Au vu de ces considérations, il convient de répondre à la septième question que les mesures prises par les États membres pour assurer la protection des données à caractère personnel doivent être conformes, tant aux dispositions de la directive 95/46 qu'à son objectif consistant à maintenir un équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée. En revanche, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46 à des domaines non inclus dans le champ d'application de cette dernière, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle.

Sur les dépens

100

Les frais exposés par les gouvernements suédois, néerlandais et du Royaume-Uni, ainsi que par la Commission et l'autorité de surveillance AELE, qui ont soumis des observations à la Cour, ne peuvent faire l'objet d'un remboursement. La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens.

Par ces motifs :

La Cour ;

Statuant sur les questions à elle soumises par le *Göta hovrätt*, par ordonnance du 23 février 2001, dit pour droit :

1) L'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un « traitement de données à caractère personnel, automatisé en tout ou en partie », au sens de l'article 3, paragraphe 1, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

2) Un tel traitement de données à caractère personnel ne relève d'aucune des exceptions figurant à l'article 3, paragraphe 2, de la directive 95/46.

3) L'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46.

4) Il n'existe pas de « transfert vers un pays tiers de données » au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page internet, stockée auprès d'une personne physique ou morale qui héberge le site internet sur lequel la page peut être consultée et qui est établie dans ce même État ou un autre État membre, des données à caractère person-

nel, les rendant ainsi accessibles à toute personne qui se connecte à internet, y compris des personnes se trouvant dans des pays tiers.

5) Les dispositions de la directive 95/46 ne comportent pas, en elles-mêmes, une restriction contraire au principe général de la liberté d'expression ou à d'autres droits et libertés applicables dans l'Union européenne et correspondant notamment à l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950. Il appartient aux autorités et aux juridictions nationales chargées d'appliquer la réglementation nationale transposant la directive 95/46 d'assurer un juste équilibre des droits et intérêts en cause, y compris les droits fondamentaux protégés par l'ordre juridique communautaire.

6) Les mesures prises par les États membres pour assurer la protection des données à caractère personnel doivent être conformes tant aux dispositions de la directive 95/46 qu'à son objectif consistant à maintenir un équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée. En revanche, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46 à des domaines non inclus dans le champ d'application de cette dernière, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle.

Table des matières

Deuxième partie
LES DÉLIBÉRATIONS 2003
PAR SECTEUR D'ACTIVITÉ 227

Commission nationale
de l'informatique et des libertés

21, rue Saint-Guillaume
75340 Paris Cedex 07

Tél. 01 53 73 22 22
Télécopie : 01 53 73 22 00

POUR PLUS D' INFORMATIONS :

Site Internet : http://www.cnil.fr