Conférence de presse
10 juillet 2012

Présentation du 32ème rapport d'activité 2011

Chiffres clés de l'année 2011

- 5738 plaintes (+ 19% par rapport à 2010)
- 2099 demandes de droit d'accès indirect aux fichiers de police (+ 12% par rapport à 2010) et 3374 vérifications effectuées.
- 385 contrôles (+ 25% par rapport à 2010) dont 150 concernant la vidéoprotection
- 65 mises en demeure, 5 sanctions financières et 13 avertissements
- 82 243 traitements de données nominatives enregistrés, dont 92% de formalités effectuées en ligne
- 48 heures de délais pour recevoir un récépissé pour une déclaration simplifiée et 4 jours pour une déclaration
- 32 743 courriers reçus
- 138 979 appels téléphoniques reçus
- 8635 organismes ont désigné un correspondant
- 23 auditions devant le Parlement
- 1969 décisions et délibérations (+ 25,5 % par rapport à 2010)
  - 249 autorisations et 11 refus d'autorisation
  - 93 avis sur des traitements sensibles ou à risques et des projets de loi ou de décret
  - 744 autorisations relatives à des systèmes biométriques (autorisation unique)
  - 5993 déclarations relatives à des systèmes de vidéosurveillance

Temps forts 2011-2012

Mars 2011

- La loi du 29 mars 2011 relative au Défenseur des droits a apporté des modifications importantes aux pouvoirs de mises en demeure et de sanction de la CNIL. En application de ces nouvelles dispositions, la Commission a procédé à une nouvelle élection des 6 membres de la formation restreinte le 5 mai 2011.

- Sanction de 100 000 euros à l'encontre de Google pour son dispositif Street View.

Avril à décembre 2011

- La CNIL a suivi l'ensemble du processus de Primaires citoyennes organisées par le Parti Socialiste : avant (examen a priori des 3 fichiers mis en œuvre), pendant (23 contrôles sur place pendant les deux tours des élections) et après (3 contrôles au terme du second tour).

Juillet 2011

- Réseaux sociaux : quelles sont les pratiques des enfants ? Quel peut être le rôle des parents ? Etude réalisée par TNS SOFRES en partenariat avec l'UNAF et Action Innocence.

Juin 2011

- Participation aux travaux du Comité chargé de préfigurer la création d'un registre national des crédits aux particuliers. La mission de ce comité consistait à étudier les modalités pratiques de la mise en place d'un tel registre.

Octobre 2011

- Présentation des observations sur la proposition de loi relative à la protection de l'identité.

Octobre à décembre 2011

- Consultation publique à destination des acteurs professionnels du Cloud computing.

Décembre 2011

- Smartphone et vie privée, un ami qui vous veut du bien ? La CNIL a cherché à mieux comprendre les pratiques des Français avec ces nouveaux accessoires technologiques. Quelles données personnelles stockent-ils (photos, contacts, coordonnées bancaires, codes secrets, informations médicales) ? Ont-ils conscience de la sensibilité de ces données ? Comment les protègent-ils ? La CNIL a demandé à Médiamétrie de réaliser une enquête en ligne auprès de 2 315 utilisateurs de smartphones et notamment auprès des 15-17 ans. Présentation de 10 conseils pour sécuriser son smartphone.

Janvier 2012

- La Commission européenne a adopté un projet de règlement et un projet de directive réformant le cadre de la protection des données. Dès le lendemain, la CNIL publiait sa première analyse sur ce projet. Tout en saluant les avancées du projet notamment en ce qui concerne le renforcement des droits des personnes, elle pointait certaines dispositions nécessitant une clarification ou pouvant poser problème.

- Présentation de la nouvelle recommandation sur la communication politique et du guide pratique à destination des candidats et partis. Mise en place d'un Observatoire des élections 2012.

Février 2012

- La CNIL est désignée par les autres autorités de protection des données européennes (G29) pour mener l'analyse des nouvelles règles de confidentialité de Google.

Mars 2012

- Lancement de la vidéo interactive « Share the Party » sur Youtube.
- Organisation, en association avec des acteurs du numérique, du premier Privacy camp en France.
- L'Assemblée Nationale et le Sénat adoptent une proposition de résolution européenne relative au projet de Règlement européen. Ces deux résolutions européennes constituent une première étape dans l'engagement des pouvoirs publics français sur cette question.

Mai 2012

- Création d'un comité de la prospective faisant appel à des experts extérieurs pour renforcer la mission de veille et de réflexion prospective de la CNIL.

Juin 2012

- Vidéoprotection/vidéosurveillance : la CNIL présente les bonnes pratiques pour des systèmes plus respectueux des droits des personnes et s'associe à l'AMF (Association des Maires de France) pour des recommandations spécifiques à destination des maires.

- Sur la base des 49 réponses reçues à l'occasion de la consultation publique, la CNIL précise son analyse du cadre juridique et propose aux entreprises qui recourent au Cloud des recommandations pratiques.

- Les 5 premiers labels CNIL sont délivrés. Ils concernent les formations « Informatique et Libertés » et les procédures d'audit.

Juillet 2012

- Après le guide sécurité destiné aux PME et présenté en 2010, la CNIL publie deux guides sécurité "avancés". Ils se composent d'une méthode et d'un catalogue de mesures pour aider les organismes à gérer les risques sur la vie privée.

Bilan 2011 : des plaintes en hausse et des compétences élargies

L'année 2011 a une fois encore montré une activité en forte croissance avec 1969 décisions adoptées (+25,5 % par rapport à 2010), 5738 plaintes enregistrées (+19% par rapport à 2010) et 385 contrôles réalisés (+25% par rapport à 2010). Au-delà de ces chiffres, cette année marque indéniablement une extension des compétences de la CNIL : contrôle de la vidéoprotection, labellisation, notification des violations de données à caractère personnel et premiers travaux issus de la direction de la prospective.

1. Un nombre record de plaintes

Le chiffre de 5738 plaintes reçues est le plus élevé jamais enregistré par la CNIL. Il témoigne de l'intérêt de plus en plus marqué des personnes pour la protection de leurs données et de la sensibilité de cette question à l'ère du numérique. Le service de plaintes en ligne disponible depuis 2010 facilite également la démarche des citoyens (26% des plaintes ont été reçues via cnil.fr en 2011, chiffre désormais supérieur à 40% depuis le début de l'année 2012).

Au-delà de ce volume important, l'année 2011 a été marquée par de nouvelles tendances quant à l'objet des plaintes.

- Ainsi, **les problématiques de « droit à l'oubli » sur internet** - suppression de textes, photographies ou vidéos en ligne – enregistrent une progression de 42% par rapport à 2010 avec 1 000 plaintes enregistrées.

- De même, **les plaintes liées à la gestion des ressources humaines** représentent 670 plaintes, soit 12% du total des plaintes ; la moitié de ces plaintes concerne spécifiquement la surveillance des salariés. A titre d'illustration, on constate des hausses importantes par rapport à 2010 notamment en matière de :

  - cybersurveillance (+59%) : il s'agit des dispositifs mis en œuvre par l'employeur pour contrôler l'utilisation des outils informatiques et l'accès à la messagerie électronique ;
  - sécurité des données de ressources humaines (+27%) : faille de sécurité du réseau informatique ou erreur humaine ayant pour conséquence la divulgation, aux collègues ou plus largement sur internet, de données telles que le numéro de sécurité sociale, les revenus ou les coordonnées des salariés.

Enfin, la CNIL reçoit toujours un nombre important de plaintes dans les secteurs de la banque et du crédit, ainsi qu'en matière de fichiers commerciaux (gestion des fichiers clients ou envoi de publicité).

2. Des compétences élargies décidées par le Législateur : contrôle de la vidéoprotection et notification des violations de données à caractère personnel

La CNIL contrôlait jusqu'alors les seuls dispositifs de vidéosurveillance dans les lieux non-ouverts au public. Depuis la LOPPSI 2 du 14 mars 2011, la CNIL est également compétente pour contrôler les dispositifs de vidéoprotection (pour les lieux ouverts au public et la voie publique) afin de s'assurer qu'ils sont conformes aux obligations légales. Elle est la seule, depuis mars 2011, à pouvoir diligenter des contrôles sur les dispositifs de vidéoprotection et de vidéosurveillance sur l'ensemble du territoire national. En tout, près de 950 000 dispositifs sont concernés.

La CNIL a procédé à 150 contrôles de dispositifs de vidéoprotection en 2011 et déjà 80 en 2012. Ces contrôles peuvent être diligentés par la Commission à son initiative, à la demande de la commission départementale de vidéoprotection ou encore à la demande du responsable d'un dispositif de vidéoprotection. Le contrôle mené par la CNIL consiste en une visite sur place.

Ces différents contrôles ont révélé des lacunes ou des manquements :
- une nécessaire clarification du régime juridique ;
- une information des personnes insuffisante ou inexistante ;
- une mauvaise orientation des caméras ;
- des mesures de sécurité insuffisantes.

Forte de ces constats, la CNIL, tout en poursuivant sa politique de contrôle, accompagne les professionnels et les particuliers pour que ces dispositifs soient plus respectueux de la vie privée. Elle a ainsi élaboré une « boîte à outils » constituée de fiches pratiques leur expliquant concrètement comment installer des dispositifs dans le respect de la loi et du droit des personnes filmées. Ces fiches portent sur :

- La vidéoprotection sur la voie publique
- La vidéosurveillance au travail
- Les caméras dans les commerces
- La vidéosurveillance dans les établissements scolaires
- La vidéosurveillance dans les immeubles d'habitation
- La vidéosurveillance chez soi

En outre, elle a élaboré avec l'AMF (Association des Maires de France) un vadémécum de bonnes pratiques à destination des maires qui souhaitent installer des systèmes de vidéoprotection dans le respect des libertés individuelles. Ces 10 conseils sont disponibles sur les sites de l'AMF et de la CNIL.

La seconde extension de compétences procède de la transposition de la directive révisant le « paquet télécom » qui impose aux fournisseurs de services de communication électronique de notifier à la CNIL les violations de données à caractère personnel. Cette obligation a été insérée dans la loi informatique et libertés et le décret n°2012-436 du 30 mars 2012 a précisé les mesures d'application.

Les opérateurs concernés sont désormais obligés d'informer la CNIL en cas de violation de l'intégrité ou de la confidentialité des ces données. La CNIL peut ensuite exiger que le fournisseur avertisse les personnes concernées en cas de risque d'atteinte aux données à caractère personnel ou à la vie privée de la personne. Cette compétence nouvelle, dont l'ampleur n'est pas encore connue va impacter l'activité de la CNIL et exiger une réactivité et une expertise technologique renforcées. Elle témoigne aussi de l'adaptation du champ des compétences de la CNIL aux évolutions technologiques impliquant le recours à des données personnelles.

3. De nouveaux outils et une approche prospective pour un environnement évolutif

Dans la logique de mise en conformité dynamique qui est la sienne, **la CNIL a été autorisée par le législateur à délivrer des labels à des procédures ou à des produits respectueux des principes et règles de la loi « informatique et libertés ».** A la demande d'organisations professionnelles et d'institutions, la CNIL a créé en octobre 2011 deux premiers référentiels : un pour les procédures d'audit et un pour les formations. Depuis, elle a reçu près de vingt demandes de délivrance de labels. Les cinq premiers labels ont été délivrés le 14 juin 2012 (4 labels ont été attribués à des formations et un à une procédure d'audit). Le label CNIL offre la possibilité aux entreprises de se distinguer par la qualité de leur service. Pour les utilisateurs, c'est un indicateur de confiance dans les produits ou procédures labellisés, qui permet ainsi d'identifier et privilégier les organismes qui garantissent un haut niveau de protection de leurs données personnelles. **La CNIL contribue ainsi à bâtir un pacte de confiance entre les citoyens et les utilisateurs de données personnelles.**

Créée en janvier 2011, la Direction des études, de l'innovation et de la prospective (DEIP) est un centre de ressources, de prospective et de veille. Elle contribue à l'identification et l'analyse des usages innovants des technologies et leurs évolutions sur la régulation. La CNIL souhaite ainsi anticiper sur l'innovation technologique, sociale et juridique, la comprendre et l'accompagner pour un meilleur respect des droits et libertés du citoyen.

La DEIP a ainsi fait réaliser un sondage par Médiamétrie en 2011, pour mieux connaître et comprendre les usages quotidiens des utilisateurs de smartphones et évaluer leur perception des enjeux de protection des données personnelles. Les principaux constats dégagés, à savoir une opacité sur les données utilisées et un défaut de sécurisation du smartphone ont conduit à un plan d'action axé sur une pédagogie des usages. Un tutoriel vidéo expliquant comment sécuriser son smartphone a ainsi été mis en ligne en janvier.

Un laboratoire a également été crée pour tester et expérimenter des produits et applications innovantes. L'objectif est ainsi de procéder à un examen complet, à la fois juridique et technologique, des dispositifs soumis à la CNIL. Les tests réalisés par ce laboratoire sont ainsi en partie à l'origine d'un « guide pratique sécurité », mis en ligne en juillet 2012, destiné aux responsables de systèmes d'informations, publics ou privés, pour identifier les menaces et les risques pesant sur les données personnelles qu'ils utilisent, et y remédier.

De même, pour la première fois, la CNIL a organisé en mars 2012, en association avec des acteurs du numérique, un événement participatif et ouvert (barcamp) autour de la protection des données personnelles. Cet événement s'est déroulé à La Cantine, lieu d'échange et espace collaboratif de coworking animé pour et par les acteurs du numérique.

Enfin, un Comité de la prospective a été créé en mai 2012 afin de renforcer la mission de veille et de réflexion prospective de la CNIL. Ce comité qui réunit des experts extérieurs témoigne d'une démarche pluridisciplinaire d'ouverture et de confrontation d'idées.

La CNIL et l'encadrement de l'action publique

La numérisation croissante et la dématérialisation des données concernent également la sphère publique. La CNIL exerce son rôle de régulateur des données personnelles en encadrant, à son niveau, l'action publique. Quelques temps forts de l'année 2011.

_____

1. Accompagner et encadrer l'action de l'administration et des collectivités locales

• **Concilier la protection de la vie privée et la réutilisation des archives publiques sur internet.** Les services d'archives publics diffusent sur internet des documents archivés comportant des données à caractère personnel qui peuvent concerner des personnes physiques potentiellement encore vivantes et/ou des personnes certes décédées mais dont la divulgation des données est susceptible d'avoir des conséquences sur la vie privée de leurs ayants-droit. En effet, les documents d'archives, que sont notamment les actes de l'état civil, comportent souvent en marge tous les actes de sa vie civile : adoption, légitimation, reconnaissance, changement de nom, de sexe, mariage, divorce, PACS, mentions du répertoire civil (placement sous tutelle, curatelle, changement de régime matrimonial), disparition, décès. Ce sont autant de données révélatrices de la vie privée qui, à l'expiration d'un délai de 75 ans à compter de la clôture du registre deviennent librement communicables.

La CNIL, confrontée aux difficultés soulevées par l'application combinée de la loi informatique et libertés, de la loi CADA et du code du patrimoine, a souhaité encadrer la diffusion en ligne de données issues des archives. Elle a adopté une autorisation unique (AU-029) applicable à l'ensemble des services d'archives publiques après concertation avec la Direction générale des patrimoines du ministère de la Culture. Cette autorisation précise les cas où la diffusion d'archives en ligne est possible ainsi que les précautions à prendre en vue de cette mise en ligne. Elle prévoit en particulier l'occultation, durant un certain délai, des données dites sensibles et pour les actes d'état civil, des mentions marginales, ainsi qu'une large information des personnes sur les modalités d'exercice de leur droit d'opposition après publication des données les concernant.

• **Élaboration d'un *vademecum* des bonnes pratiques en matière de vidéoprotection** : la CNIL et l'AMF ont élaboré un *vademecum* de recommandations aux maires qui souhaitent installer des systèmes de vidéoprotection sur la voie publique ou dans les lieux ouverts au public de leur commune. Ce document rappelle, en 10 points, les conditions que doit respecter la mise en place de tels dispositifs.

• **Création d'un observatoire des élections** : en janvier 2012, la CNIL a mis en place un « Observatoire des élections » chargé de veiller au respect de la protection des données personnelles par les partis politiques et leurs candidats. A l'issue des élections présidentielle et législatives, l'Observatoire a dressé le bilan de ses travaux et il en ressort que la protection des données personnelles des électeurs doit être améliorée. La CNIL adressera prochainement au Gouvernement des propositions de modifications du cadre juridique en

matière de prospection politique, tout particulièrement en ce qui concerne la communication électronique.

2. Le contrôle des fichiers régaliens

Le projet de carte d'identité nationale. Dans le cadre du débat parlementaire concernant la proposition de loi relative à la protection de l'identité, la CNIL a fait connaître son analyse en publiant en ligne une note d'observations. La proposition de loi prévoyait la délivrance de cartes d'identité biométriques (munies d'une puce électronique contenant notamment deux empreintes digitales) et la création d'une base de données contenant l'ensemble des informations requises pour la délivrance du titre et notamment huit empreintes digitales du demandeur. La Cnil a fait porter ses observations sur quatre points :

- Elle a rappelé la légitimité de la délivrance de titres biométriques tout en insistant sur la mise en place de garanties complémentaires (par exemple, un âge minimal de collecte des identifiants biométriques) ;

- S'agissant de la création d'une base de données biométriques, la CNIL a rappelé la nécessité de respecter le principe de proportionnalité au regard des objectifs poursuivis (limitation du nombre d'empreintes digitales enregistrées dans la base centrale, absence de lien entre les données biométriques enregistrées dans le traitement central et les données d'état civil, interdiction de procéder à des recherches d'identification sur la base des éléments biométriques enregistrés dans la base) ;

- La CNIL a émis des réserves sur la possibilité de mettre en œuvre des dispositifs de reconnaissance faciale (possibilité de recourir à des fonctionnalités d'identification des personnes à partir de l'analyse biométrique de la morphologie de leur visage) ;

- S'agissant des fonctions électroniques de la carte nationale d'identité, la CNIL a rappelé le caractère facultatif de ces fonctions et la nécessité d'obtenir le consentement des personnes au traitement de leurs données à des fins d'utilisation de téléservices de l'administration.

Le Conseil constitutionnel s'est prononcé sur la loi relative à la protection de l'identité le 22 mars 2012. Il a considéré que la collecte et l'enregistrement des empreintes digitales dans une puce électronique jointe à la carte d'identité offrait une meilleure identification des personnes, au même titre que le passeport électronique. En revanche, il a rejeté la proposition d'une base de données centrale contenant les données biométriques de quasiment toute la population considérant que les finalités de police administrative ou judiciaire projetées au moyen de ce traitement portaient atteinte au droit au respect de la vie privée et étaient disproportionnées au regard des données collectées pour l'objectif initial de délivrance de titres d'identité et de voyage.

Le Conseil a considéré en outre que la deuxième puce électronique ayant pour finalités l'authentification et la signature électronique sur les réseaux de communications électroniques ne satisfaisait pas les garanties légales pour assurer l'intégrité et la confidentialité des données enregistrées.

Le traitement d'antécédents judiciaires (TAJ) : le décret n° 2011-652 du 4 mai 2012, pris après l'avis de la CNIL, a créé le traitement d'antécédents judiciaires (TAJ). Il s'agit d'un fichier d'antécédents commun à la police et à la gendarmerie nationales. Il remplace les fichiers STIC et JUDEX, qui seront définitivement supprimés le 31 décembre 2013. Il sera utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et des enquêtes administratives (comme celles préalables à certains emplois publics ou sensibles). Ses principales caractéristiques sont également semblables à celles des fichiers STIC et JUDEX (données enregistrées, durées de conservation, destinataires).

De nouvelles garanties ont été apportées :

- Les conditions mise à jour des données ont été améliorées. Les suites décidées par l'autorité judiciaire seront renseignées automatiquement dans TAJ grâce à une interconnexion avec le traitement CASSIOPEE utilisé par les juridictions. Cette évolution permettra d'éviter l'absence de mise à jour à la suite de la procédure judiciaire (classement sans suite, acquittement, non lieu).

- En outre, la mise en œuvre de ce fichier est entourée des nouvelles garanties prévues par la LOPPSI à la suite des recommandations de la CNIL :

  • Toutes les décisions de classement sans suite seront dorénavant mentionnées ;
  • Il sera impossible de consulter les données relatives aux personnes ayant fait l'objet d'une mention dans le cadre des enquêtes administratives ;
  • Les procureurs transmettront directement au ministère de l'intérieur les décisions de rectification ou d'effacement.

Néanmoins, la CNIL considère qu'il est indispensable de procéder à un important travail de mise à jour des données enregistrées dans les fichiers STIC et JUDEX avant de procéder à leur versement dans TAJ. Il importe en effet que TAJ ne soit pas affecté, dès sa mise en œuvre, par les résultats des dysfonctionnements de ces fichiers auquel il est précisément censé mettre un terme.

Tout comme le fichier STIC en 2007 et 2008, ce nouveau traitement fera l'objet d'un contrôle global de la Commission à l'issue de son déploiement sur l'ensemble du territoire national.

Par ailleurs, le contrôle des fichiers de sécurité publique est inscrit au programme des contrôles de la CNIL pour l'année 2012.

Observatoire des élections : bilan de l'utilisation des fichiers pendant les campagnes électorales de 2012

En janvier 2012, la CNIL a mis en place un « Observatoire des élections » chargé de veiller au respect de la protection des données personnelles par les partis politiques et leurs candidats. A l'issue des élections présidentielle et législatives, l'Observatoire a dressé un bilan de ses travaux, duquel il ressort que la protection des données personnelles des électeurs doit être améliorée. La CNIL adressera donc prochainement au Gouvernement des propositions de modifications du cadre juridique en matière de prospection politique, tout particulièrement en ce qui concerne la communication électronique.

_____

A l'occasion des élections présidentielle et législatives, les candidats et les partis qui les soutiennent ont effectué de larges opérations de communication politique, s'appuyant notamment sur des fichiers de membres, de contacts réguliers ou encore de simples prospects.

C'est pourquoi la CNIL a précisé, à l'approche des échéances électorales de 2012 et après consultation des principales formations politiques, les modalités d'application des principes de protection des données aux fichiers mis en œuvre à des fins de communication politique. Une nouvelle recommandation a ainsi été adoptée (délibération n° 2012-020 du 26 janvier 2012 : *lien internet*), ainsi qu'un guide pratique à l'attention des partis politiques et des candidats (*lien internet*).

Dans ce cadre, un « Observatoire des élections 2012 » a été mis en place. Il a assuré une veille, un dialogue avec les partis politiques et l'information régulière du public, notamment grâce à un site internet dédié comportant des informations à destination des électeurs et des partis politiques. Ce site proposait également d'adresser des « témoignages » à la CNIL.

1. Le bilan de l'utilisation de fichiers durant les campagnes électorales

Il ressort du bilan dressé par l'Observatoire à l'issue des élections que **la protection des données personnelles des électeurs doit être sensiblement améliorée sur certains points, tout particulièrement en matière de communication électronique**. La réception de messages électroniques non sollicités constitue en effet le motif principal des plaintes et témoignages reçus et provoque de fortes réactions chez certains électeurs.

Les Français de l'étranger, dont les adresses électroniques figurent sur les listes électorales consulaires librement consultables par les partis politiques, ont ainsi adressé de nombreux témoignages à l'Observatoire :

Exemple de témoignage : « *Je suis sans arrêt spammé par de multiples partis politiques. Je n'ai pas donné mon accord au Consulat français de [X] pour communiquer mon email personnel aux partis*. »

Ces réactions sont souvent amplifiées par la fréquence importante de certains messages :

Exemple : « *Cela fait 5 fois que je suis contacté par l'équipe de [X], suite à la récupération de mon email sur le site consulaire. C'est inadmissible, cet email est important et est à présent pollué par ces spams.* »

Les électeurs résidant en France se sont également plaints de la réception de courriels non sollicités – les adresses électroniques étant alors obtenues par location de bases de données commerciales :

Exemple : « *J'ai reçu un mailing de campagne sur ma boîte personnelle alors que je n'ai absolument pas fourni cette adresse (ni à aucun autre candidat). Je leur ai demandé, en vain, comment ils avaient eu mon adresse…* »

Les difficultés à se désinscrire de telles listes de diffusion ont également été à l'origine de plaintes :

« *J'ai reçu, à plusieurs reprises et sans aucune sollicitation de ma part, des messages du candidat [X]. Mes diverses demandes de désinscription ne sont pas effectives à ce jour.* »

« *Malgré trois désinscriptions sur le site indiqué en bas du mail, j'ai reçu 6 messages en 4 jours. Je ne me suis à aucun moment inscrite sur des sites politiques.* »

« *Malgré ma demande de ne plus recevoir de spam venant de ce candidat (en cliquant sur le lien de désinscription en fin du mail, à la fois pour le site [LE SLOGAN] et le [parti politique]), je viens à nouveau d'en recevoir un. L'adresse d'envoi n'est plus la même : la première fois, il s'agissait de [candidat@communication.leslogan.fr] et maintenant de [campagne@communication.leslogan.fr] Ce changement d'adresse leur a ainsi permis de contourner mon anti-spam.* »

La plupart des difficultés rencontrées par les électeurs dans le cadre de la campagne pour l'élection présidentielle auraient été évitées si les candidats et partis politiques avaient davantage respecté les dispositions de la loi « Informatique et Libertés » et les recommandations de la CNIL.

2. Les propositions de la CNIL pour améliorer la protection des données traitées dans le cadre de la communication politique

Les problèmes identifiés par l'Observatoire durant ces campagnes électorales montrent la **nécessité de mieux encadrer la prospection politique, tout particulièrement en matière de communication électronique**. La CNIL adressera donc prochainement au Gouvernement des propositions de modification du cadre juridique actuel.

En particulier, il apparaît nécessaire **d'aligner la protection dont bénéficient les électeurs sur celle accordée aux consommateurs en matière de prospection électronique**. C'est pourquoi la CNIL, comme elle l'avait indiqué lors des précédentes élections générales, est favorable à ce que les messages électroniques de prospection politique ne soient adressés

qu'aux personnes ayant **préalablement consenti** à cette utilisation de leurs données, tout comme cela est le cas en matière de prospection commerciale.

La CNIL souhaite également que des **dispositions spécifiques concernant la prospection par voie électronique en période de campagne officielle soient intégrées au code électoral**. Les témoignages adressés à la CNIL montrent notamment la nécessité d'un débat sur les règles de communication et d'utilisation des listes électorales, ainsi que la clarification des règles relatives aux modalités et délais de traitement des demandes d'opposition des personnes à recevoir des messages ultérieurs ou encore aux mentions d'information minimales à faire figurer dans chaque message de prospection politique adressé durant cette période.

L'amélioration de la protection des données traitées par les partis politiques et les candidats passe enfin, nécessairement, par un **travail de collaboration et de sensibilisation** de ces acteurs à cette problématique.

Après avoir consulté les **principaux partis politiques** avant l'adoption de sa recommandation de janvier 2012 et leur avoir rappelé, entre l'élection présidentielle et les élections législatives, les recommandations principales de la Commission en matière de prospection politique, la CNIL va leur présenter ce bilan des campagnes électorales du point de vue de la protection des données personnelles. Des réunions seront organisées avec les principales formations politiques et les principales entreprises du secteur (prestataires réalisant les campagnes de prospection, entreprises louant leurs bases de données aux partis politiques) afin de mieux leur faire connaître les recommandations de la CNIL et d'accompagner la généralisation des bonnes pratiques en la matière.

Les premiers labels

La loi Informatique et Libertés permet à la CNIL de délivrer des labels "*à des produits ou des procédures tendant à la protection des personnes à l'égard du traitement des données*" (article 11.3). L'obtention des labels CNIL est soumise au respect des exigences définies dans des référentiels. A la demande d'organisations professionnelles et d'institutions, la CNIL a créé en octobre 2011 deux référentiels : un pour les procédures d'audit et un pour les formations. Depuis, elle a reçu près de vingt demandes de délivrance de labels. Les cinq premiers labels ont été délivrés par la Commission jeudi 14 juin 2012.

_____

Le label CNIL permet aux entreprises de se distinguer par la qualité de leur service. Pour les utilisateurs, c'est un indicateur de confiance dans les produits ou procédures labellisés, qui permet ainsi d'identifier et privilégier les organismes qui garantissent un haut niveau de protection de leurs données personnelles.

Lors de sa séance plénière du 14 juin 2012, la CNIL a délivré les cinq premiers labels : quatre pour les formations et un pour l'audit de traitement.

Ont obtenu **le label CNIL « formation »**, dans l'ordre alphabétique des organismes formateurs, les formations suivantes :

- « Lexing® *Informatique et Libertés* » proposée par le cabinet BENSOUSSAN SELAS ;
- « *Les enjeux du droit à la protection des données à caractère personnel* » proposée par le cabinet HAAS ;
- « *Correspondant Informatique et Libertés* » proposée par le cabinet HSC (Hervé Schauer Consultants ;
- « *Formation loi Informatique et Libertés - le régime juridique des traitements et des fichiers* » proposée par Maître MOLE conjointement avec le cabinet COMUNDI. Plusieurs personnes peuvent en effet solliciter un label de manière conjointe, aux fins de faire un usage commun du produit ou de la procédure labellisée.

Afin de clarifier le champ d'application du label délivré, la liste des éléments de la formation concernée est énumérée dans chacune des délibérations.

Lors de cette séance, la procédure d'audit du cabinet HAAS, intitulée « *Audit 'Informatique et libertés'* » a obtenu **le label CNIL « audit de traitements »**.

Les délibérations portant délivrance des labels seront publiées au Journal Officiel.

A propos des labels CNIL

Les labels sont délivrés pour une durée limitée de trois ans. Si les formations ou procédures d'audit concernées font l'objet d'une modification dans ce délai, la Commission devra en être automatiquement informée.

En outre, l'utilisation de la marque « Label CNIL » est soumise au respect du règlement d'usage de la marque collective. La Commission s'attachera à vérifier l'utilisation qui sera faite de ces labels. Parmi les mesures de contrôle prévues pour les labels qui ont été délivrés, figure notamment la transmission d'un bilan d'activité annuel.

La procédure à suivre pour obtenir un label CNIL est la suivante :

1. Dépôt de la demande au moyen du formulaire spécifique, accessible en ligne,
2. Examen de la recevabilité de la demande dans les deux mois,
3. Evaluation de la conformité au référentiel par le Comité de labellisation, composé de trois commissaires,
4. Présentation en séance plénière de la Commission qui décide alors de délivrer, ou non, le label CNIL.

Cette nouvelle activité de la CNIL pourrait se développer fortement dans les années à venir sous réserve de l'évaluation du dispositif qui sera faite au terme de la période de trois ans.

L'action européenne et internationale de la CNIL

La protection des données personnelles revêt une dimension à la fois démocratique et économique, aussi bien au plan national qu'international. L'extraordinaire développement de ces données, qui sont au cœur de l'ère numérique, conduit en effet les différents pays ou régions du monde à définir des règles ou à instaurer des régulations. L'enjeu est désormais d'adapter le cadre normatif européen à ce nouveau contexte, et d'assurer l'interopérabilité de ces systèmes sans renoncer au haut niveau de protection du citoyen, qui est et doit rester au cœur du dispositif.

_____

1. La participation active de la CNIL aux travaux de révision de la directive européenne

La Commission européenne a présenté le 25 janvier 2012 un projet de règlement communautaire destiné à servir de cadre normatif à la protection des données personnelles en Europe pour les prochaines décennies. La Cnil est mobilisée pour le maintien d'un haut niveau de protection en Europe. Si elle a salué les avancées du projet en ce qui concerne le renforcement des droits des personnes, plusieurs aspects du texte ne lui semblent pas adaptés à un système de protection participatif et décentralisé plus en phase avec le monde numérique et la diversité des situations rencontrées. En particulier, le critère de « l'établissement principal » fondant la compétence de l'autorité nationale de protection des données risque d'être source d'insécurité juridique de défiance pour les citoyens comme les entreprises. Des travaux sont menés tant avec la Commission européenne que le Parlement européen sur le sujet. **L'Assemblée nationale et le Sénat ont d'ores et déjà adopté deux résolutions sur ce projet de texte, en des termes identiques, se faisant l'écho des réserves de la CNIL.**

2. L'implication au quotidien dans les instances européennes et internationales

- **L'implication dans les travaux européens du « G29 »**

La CNIL s'investit particulièrement dans les travaux européens menés par le « G29 », c'est-à-dire le groupe des « CNIL » européennes. A ce titre, elle a poursuivi, en 2011, sa participation dans les différents groupes et sous-groupes de travail auxquels elle appartient: le groupe technologie, BCR, affaires financières, futur de la vie privée….

Dans ce cadre, elle a été désignée par ses homologues européens pour instruire et **analyser les nouvelles règles de confidentialité de Google** (**en 2012)**. En effet, la CNIL et les autorités européennes sont vigilantes sur les nouvelles propositions de Google en matière de vie privée et notamment les possibilités de croisement de données entre les services proposés. Après l'analyse détaillée des réponses de Google, la CNIL présentera son rapport au G29, qui définira sa position et les éventuelles améliorations que Google devra apporter à ces règles de confidentialité, pour être en conformité avec le cadre européen de protection des données.

- **La contribution de la CNIL à l'instauration d'une régulation internationale efficace**

La CNIL, agissant au titre de représentant de la Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée, a poursuivi sa participation au sein des plus hautes instances internationales :

→ **L'OCDE :** participation au groupe des volontaires concernant la révision des lignes directrices sur la protection de la vie privée et des transferts de données. En 2011, l'OCDE a consulté les parties prenantes via un questionnaire et la CNIL a été chargée par le gouvernement français de préparer la réponse de la France
→ **Le Conseil de l'Europe** : suivi des travaux de modernisation de la convention 108
→ **L'APEC** : participation au sous-groupe sur la protection de la vie privée

La CNIL a également participé à la **Conférence internationale des Commissaires à la protection des données et à la vie privée qui s'est tenue du 1er au 3 novembre 2011 à Mexico.**

Cette conférence a été l'occasion pour les autorités d'afficher leur volonté d'accroître et d'améliorer leur coopération afin de répondre plus efficacement aux défis de la mondialisation en matière de protection des données. La CNIL y a défendu une approche fondée sur la détermination de principes communs à l'ensemble des parties prenantes au niveau mondial, objectif qui ne saurait être atteint sans l'implication des gouvernements.

- **La participation aux travaux de l'ISO**

La CNIL a poursuivi sa contribution aux travaux de normalisation sur les projets de normes ISO (International Standardisation Organisation). Elle suit tout particulièrement le projet de norme appelé ISO 29100 "Privacy Framework" (cadre de protection de la vie privée) qui détermine des exigences et une terminologie communes en matière de protection de la vie privée à l'échelle internationale

- **La réception de délégations étrangères**

En 2011, la CNIL a reçu la visite de plusieurs délégations étrangères (15) provenant de 4 continents différents dans le but de mieux connaitre son fonctionnement et ses actions: Allemagne, Chine, Corée du Sud, Etats-Unis, Japon, Liban, Maroc, Mexique, Québec, Suisse, Taiwan, Ukraine.

3. La poursuite de la promotion d'une « culture informatique et libertés » au sein de la Francophonie

Depuis une dizaine d'années, la CNIL s'est engagée dans une action de promotion de la culture "Informatique et Libertés" au sein des pays francophones. Ces actions ont abouti à la création, en 2007, de l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), en partenariat notamment avec l'Organisation Internationale de la Francophonie (OIF).

En 2011**,** l'AFAPDP a engagé un programme annuel d'action. Ce programme a notamment contribué à mettre en place un programme de missions d'expertise auprès d'autorités nouvellement créées, tandis que la CNIL a participé, à Dakar, à la première rencontre régionale sur la protection des données personnelles et de la vie privée organisée le 19 septembre 2011. Cette rencontre a été suivie les 20 et 21 septembre 2011 d'un séminaire de formation sur la protection des données réunissant des experts francophones du monde entier.

Enfin l'AFAPDP a tenu sa 5ème conférence annuelle francophone à Mexico, en marge de la 33ème Conférence internationale des commissaires à la protection des données (octobre 2011).

Ce réseau des CNIL francophones permet ainsi de partager et de promouvoir une approche humaniste, fondée sur la protection du citoyen, entre des autorités de tous les continents, indispensable à l'ère du numérique.

Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces services

Les offres de « Cloud computing » se sont fortement développées ces dernières années. Cependant, le recours par les entreprises à ces services pose des questions nouvelles en termes juridiques et de gestion des risques. Afin de préciser le cadre juridique applicable, la CNIL a lancé fin 2011 une consultation publique sur le Cloud computing. Forte des 49 contributions recueillies, la CNIL a publié, le 25 juin 2012, son analyse sur le cadre juridique applicable ainsi que des recommandations pratiques à destination des entreprises françaises, et notamment des PME, qui souhaitent avoir recours à des prestations de Cloud.

_____

L'expression « informatique en nuage » ou « Cloud computing » désigne le déport vers « le *nuage Internet*[1] *» de données et d'applications qui auparavant étaient situées sur les serveurs et ordinateurs des sociétés, des organisations ou des particuliers. Le modèle économique associé s'apparente à la location de ressources informatiques avec une facturation en fonction* de la consommation.

La gamme d'offres correspondantes a connu un fort développement ces quatre dernières années, notamment au travers du stockage et de l'édition en ligne de documents ou même des réseaux sociaux par exemple.

De nombreuses offres de services de Cloud computing sont désormais disponibles sur le marché, que ce soit pour l'hébergement d'infrastructures (IaaS – Infrastructure as a Service), la fourniture de plateformes de développement (PaaS – Platform as a Service) ou celle de logiciels en ligne (SaaS – Software as a Service). Ces offres sont proposées dans des Clouds publics (service partagé et mutualisé entre de nombreux clients), privés (Cloud dédié à un client) ou hybrides (combinaison des modèles public et privé).

Une nécessaire clarification du cadre juridique

Le Cloud computing représente pour les entreprises une évolution majeure de leurs services informatiques et propose de nombreux avantages, notamment celui de mutualiser les coûts d'hébergement et d'opérations.

Les questions de sécurité, de qualification du prestataire, de loi applicable et de transfert des données sont particulièrement délicates dans le cadre du Cloud computing. Les entreprises souhaitant recourir à ces services ont donc besoin d'une clarification des responsabilités y afférant.

[1] Bien avant qu'apparaisse l'expression « Cloud Computing », les architectes réseau schématisaient Internet par un nuage. En anglais, le terme « the Cloud » était couramment utilisé pour désigner Internet.

La standardisation des offres et le recours par les prestataires de Cloud à des contrats d'adhésion pour formaliser leurs relations contractuelles avec leurs clients laissent peu de marge de négociation à ces derniers. De plus, il apparaît que les prestataires fournissent généralement peu d'informations à leurs clients quant aux mesures techniques et organisationnelles mises en œuvre permettant de garantir la sécurité et la confidentialité des données traitées pour le compte des clients. Cette insuffisance de transparence de la part des prestataires fait défaut aux clients, puisqu'ils ne disposent pas de toutes les informations nécessaires leur permettant de remplir leurs obligations en tant que responsables de traitement.

Le 25 juin 2012, la CNIL a publié son analyse du cadre juridique applicable au Cloud computing ainsi que des recommandations pratiques destinées principalement aux PME. La CNIL a également publié une liste des éléments essentiels devant figurer dans un contrat de prestation de services de Cloud computing.

Les perspectives pour 2012-2013 : la régulation des données personnelles au service d'une véritable « éthique du numérique »

La CNIL est aujourd'hui à une étape décisive de son évolution et fait face à des mutations structurelles liées au développement du numérique. Elle est aussi au cœur d'un débat international qui va fixer le cadre de la protection des données du XXI ème siècle. Cet environnement international est marqué par une forte concurrence en matière de régulation entre les grandes régions économiques. Cette période exceptionnelle nous invite à renouveler notre action afin d'affirmer le rôle de régulateur des données personnelles de la CNIL pour construire le cadre éthique de l'écosystème numérique.

1. Un changement d'ère : de l'informatique au numérique, des fichiers aux données

En quelques années, avec la numérisation croissante des activités et leur dématérialisation, les données personnelles ont investi tous les domaines de l'activité humaine et tous les secteurs. Le numérique est devenu ambiant, omniprésent et les données sont l'élément central de cet univers. Elles concernent les individus, les entreprises, les acteurs publics mais aussi les objets. Elles constituent aussi une valeur marchande considérable au cœur des enjeux économiques internationaux du XXI ème siècle.

Ce nouvel environnement ne peut plus être régulé comme avant. C'est pourquoi la CNIL doit repenser son action et ses outils d'intervention pour pouvoir traiter ces flux de données à s'adresser à des interlocuteurs très variés. Face à la complexité de l'écosystème numérique, l'enjeu du régulateur et de construire des relais qui permettent d'associer et de responsabiliser les acteurs afin de partager la charge de la régulation avec eux. Cela consiste notamment à mettre à la disposition des différents relais identifiés des boîtes à outils leur permettant de mettre en œuvre concrètement, et le plus en amont possible, les principes « Informatique et Libertés ». Qu'il s'agisse de codes de bonne conduite, bonnes pratiques, chartes, labels, pack de conformité, correspondants informatique et libertés, tous ces leviers sont au service de la conformité des entreprises.

2. De nouveaux rapports à la vie privée

Le développement d'internet et notamment des réseaux sociaux conduit les individus à exposer davantage leur vie privée et ce, de plus en plus tôt (20 % des moins de 13 ans ont un compte sur un réseau social selon l'étude menée par TNS Sofres en juillet 2011 pour la CNIL, l'UNAF et Action innocence). Les utilisateurs, même s'ils n'ont pas toujours conscience de l'utilisation qui est faite de leurs données personnelles, souhaitent plus de transparence et des outils leur permettant de maîtriser leurs données. La CNIL doit donc s'adapter à cette nouvelle demande sociale et proposer au grand public une pédagogie des solutions, c'est-à-dire lui donner les clés pour un usage maîtrisé et responsable du numérique. Ceci passe notamment par une éducation numérique partagée et portée par différents acteurs.
Pour être capable d'anticiper les nombreux usages, la CNIL peut désormais s'appuyer sur les travaux de sa Direction des études, de l'innovation et de la prospective et de son

Laboratoire. Elle entend aussi poursuivre sa démarche d''ouverture et de dialogue déjà engagée au travers par exemple du « chantier vie privée 2020 », de l'organisation d'un *Privacy camp* en mars ou de la création récente d'un comité de la prospective.

3. Un environnement international marqué par une forte concurrence des modes de régulation

L'Europe, l'Asie et les Etats-Unis s'efforcent de développer des systèmes de régulation permettant l'articulation entre protection des données personnelles et développement de l'économie numérique. En Europe, cela passe par la nécessaire révision de la directive européenne de 1995. L'enjeu est de garantir un haut niveau de protection aux citoyens européens à l'ère du numérique et de bâtir une interopérabilité des mécanismes encadrant les transferts internationaux de données. Dans ce contexte de forte concurrence, l'Europe doit montrer ses capacités à moderniser son modèle tout en réaffirmant la vie privée en tant que droit fondamental. Elle doit proposer un modèle permettant de créer de la confiance, élément déterminant pour la croissance de l'économie numérique.

C'est dans ce contexte que la Commission européenne a rendu public un projet de règlement européen le 25 janvier 2012. Ce texte comporte des avancées importantes, en consacrant ou renforçant les droits des citoyens, et conforte l'évolution des métiers et des pratiques de la CNIL en supprimant les formalités préalables au profit d'un accompagnement des organismes pour leur permettre une mise en conformité. Dans cette nouvelle configuration, le pilotage de la conformité sera au cœur des métiers de la CNIL pour les années à venir.

Mais pour que ce nouveau cadre juridique soit réellement protecteur et novateur, il doit définir une gouvernance efficace de la protection des données personnelles par les autorités de contrôle nationales. C'est précisément à cette fin que la CNIL a, tout au long de l'année 2011 et plus encore en 2012, confortée en cela par deux résolutions parlementaires adoptées dans les mêmes termes au premier trimestre 2012, entrepris de proposer des adaptations du projet de texte en question.

4. Vers une constitutionnalisation de la protection des données personnelles ?

La protection des données personnelles constitue un droit fondamental, complémentaire des droits et libertés constitutionnellement garantis que sont la protection de la vie privée, le droit de propriété, la liberté d'expression ou encore la liberté d'aller et venir. Ce droit est d'autant plus fondamental aujourd'hui à l'heure où les données personnelles constituent le « carburant » du numérique.

Pourtant, alors même que cette protection **est consacrée par la Charte des droits fondamentaux de l'Union européenne**, mais aussi dans les constitutions ou normes suprêmes de 13 pays en Europe, notre Constitution est muette sur le sujet. Or, aucun des droits et libertés actuellement consacrés par notre Constitution n'épuise la question des données personnelles.

La CNIL promeut donc l'objectif d'inscrire, dans la Constitution, le droit à la protection des données personnelles. Une telle reconnaissance constituerait un acte fort, moderne, au service d'une protection effective du citoyen.

Pour Isabelle Falque-Pierrotin, Présidente de la CNIL : ***« La question de la protection des données personnelles est aujourd'hui au centre des préoccupations, économiques, sociales, commerciales mais aussi politiques, car pour la traiter il est nécessaire d'élaborer une vision collective et partagée de la société. En tant que régulateur des données personnelles, le rôle de la CNIL est de contribuer à la recherche de ce pacte social à partir du modèle humaniste hérité de la loi Informatique et Libertés qui place la personne au centre du dispositif. Il s'agit aussi de repenser notre action et nos outils d'intervention pour animer cet écosystème numérique en pleine mutation et accompagner les différents acteurs.»***