CNIL
Commission Nationale de l'Informatique et des Libertés

Le Président

Note d'observation de la Commission nationale de l'informatique et des libertés relative à certaines dispositions du projet de loi d'orientation et de programmation de la performance de la sécurité intérieure (LOPPSI)

Adoptée en séance plénière le 6 mai 2010

Le projet de loi d'orientation et de programmation de la performance de la sécurité intérieure (LOPPSI) a été adopté en première lecture à l'Assemblée nationale le 16 février 2010, et devrait être débattu au Sénat en juin.

Dans la mesure où de nombreuses dispositions du projet de loi ont pour objet ou pour effet de mettre en œuvre ou de modifier des traitements de données à caractère personnel, et conformément aux dispositions de l'article 11 de la loi du 6 janvier 1978 modifiée, le ministère de l'intérieur a saisi pour avis la Commission nationale de l'informatique et des libertés, en janvier 2009, de sept articles de l'avant-projet de loi. Ces dispositions concernent la captation de données informatiques, l'identification des personnes par leurs empreintes génétiques (FNAEG), les fichiers d'antécédents, les fichiers d'analyse sérielle, le fichier relatif aux auteurs d'infractions sexuelles (FIJAIS) et la consultation des fichiers de police à des fins d'enquête administrative.

Tout en regrettant de ne pas avoir été saisie de l'ensemble des dispositions du projet de loi, et notamment des dispositions relatives à la vidéosurveillance (vidéoprotection), la CNIL a rendu son avis par la délibération n° 2009-200 du 16 avril 2009. Pour la première fois, en application de l'article 104 de la loi du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, cet avis, joint au présent document, a été rendu public à la demande du Président de la Commission des Lois de l'Assemblée Nationale.

On notera que le rapporteur du texte au Sénat a sollicité du Président de la CNIL les observations de la Commission sur les principales dispositions du projet de loi. Or, le projet de texte sur lequel elle s'est prononcée le 16 avril 2009 est sensiblement différent de celui qui a été adopté en première lecture à l'Assemblée Nationale.

La présente note, examinée en séance plénière, a donc pour objet de présenter les principales observations de la Commission s'agissant des nouvelles dispositions législatives relatives aux fichiers de police au sens large, à la vidéosurveillance (vidéoprotection), aux scanners corporels et à la captation de données informatiques.

A titre liminaire, il convient de noter que plusieurs des recommandations formulées par la Commission dans son avis du 16 avril 2009 ont été prises en compte par le Gouvernement et par l'Assemblée nationale.

Il en est ainsi des modalités de mise à jour et d'effacement des données enregistrées dans les fichiers d'antécédents judiciaires (article 10 du projet de loi). Conformément à ses propositions, les cas de mise à jour des données de ces fichiers (STIC et JUDEX) ont en effet été élargis à de nouvelles décisions judiciaires. Ainsi, toutes les décisions de classement sans suite, et non plus les seules décisions prises aux motifs d'absence d'infraction et d'infraction insuffisamment caractérisée, feront dorénavant l'objet d'une mention dans ces fichiers.

La Commission estime cependant que le projet de nouvel article 230-8 du Code de procédure pénale devrait être complété afin de préciser expressément que la mention dans les fichiers des suites judiciaires a pour effet, dans le cadre des enquêtes administratives, de rendre impossible la consultation des fiches ayant bénéficié d'une telle mise à jour.

La Commission rappelle à nouveau que la consultation des fichiers de police judicaire à des fins d'enquête administrative a toujours suscité de sa part une réserve de principe, compte tenu de la finalité initiale de ces fichiers et des graves conséquences pour les personnes qui

peuvent résulter de leur insuffisante mise à jour, notamment en terme d'accès ou de maintien dans l'emploi.

Par ailleurs, des garanties supplémentaires ont été introduites dans le projet de loi s'agissant de l'identification d'une personne par ses empreintes génétiques (articles 5 à 9). Dans son avis du 16 avril 2009, la CNIL a souligné que l'enregistrement de données génétiques recueillies, non plus seulement dans le cadre de procédures judiciaires, mais également de procédures administratives d'identification, tend à conférer une nouvelle finalité au FNAEG, actuellement conçu comme un fichier d'identification judiciaire. C'est pourquoi les dispositions du projet de LOPPSI prévoient dorénavant que les données recueillies dans un cadre judiciaire ne pourront pas être rapprochées de celles recueillies à des fins civiles d'identification. Il est ainsi expressément prévu que les empreintes génétiques des parentèles des personnes dont l'identification est recherchée font l'objet d'un enregistrement distinct dans le FNAEG. Des dispositions réglementaires, qui seront soumises à l'avis de la CNIL, sont également prévues afin de préciser que les empreintes génétiques des cadavres non identifiés, des mineurs ou majeurs protégés dont le décès est supposé, ainsi que des victimes de catastrophes naturelles, seront conservées dans une sous-base étanche du FNAEG. Ces dispositions devraient également prévoir que les profils génétiques des parentèles ne pourront être comparés qu'avec les seules empreintes génétiques des cadavres non identifiés, et non avec le reste de la base.

Enfin, l'article 23 du projet de loi insère de nouvelles dispositions dans le Code de procédure pénale autorisant, dans le cadre d'une information judiciaire en matière de criminalité organisée, l'utilisation de dispositifs de captation de données informatiques à l'insu des intéressés. Peuvent ainsi être enregistrées, conservées et transmises au moyen d'outils matériels et logiciels de captation, en tous lieux, toute donnée informatique, telle qu'elle s'affiche à l'écran pour l'utilisateur ou telle qu'elle est saisie par lui, sur un ou plusieurs ordinateurs placés sous surveillance.

Le texte soumet l'utilisation de ces outils de surveillance à une ordonnance écrite spécialement motivée du juge d'instruction, après avis du procureur de la République. La durée de la surveillance est limitée à quatre mois renouvelables une fois. Par ailleurs, les enregistrements des données informatiques captées sont « *placés sous scellés fermés* », et sont « *détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique* ».

La Commission se félicite qu'ait été suivie sa recommandation appelant à limiter la collecte de données aux seuls enregistrements utiles à la manifestation de la vérité et aux seules séquences liées aux infractions, conformément à la décision du Conseil constitutionnel DC n° 2004-492 du 2 mars 2004. En effet, le projet de loi adopté par l'Assemblée nationale prévoit désormais explicitement que seules sont transcrites dans le procès-verbal versé au dossier les « *données qui sont utiles à la manifestation de la vérité* », et qu' « *aucune séquence relative à la vie privée étrangère aux infractions visées dans les décisions autorisant la mesure ne peut être conservée dans le dossier de la procédure* ».

La Commission relève également que les dispositions relatives à la protection de certaines personnes et lieux (notamment médecins, avocats, magistrats et sociétés de presse) ont été modifiées conformément à ses recommandations, en particulier grâce à la suppression de l'adverbe « *habituellement* ». Elle avait en effet exprimé une réserve concernant l'emploi de

ce terme, qui créait un aléa et un risque d'insécurité juridique disproportionnés au regard des finalités poursuivies.

Le projet de loi prévoit, par ailleurs, l'utilisation des outils de captation des données informatiques dans les points publics d'accès à Internet. Or, une telle utilisation présente un caractère particulièrement sensible, puisqu'elle conduit à placer sous surveillance l'ensemble des postes informatiques mis à disposition du public. La Commission rappelle que le recours à des dispositifs de captation dans les points publics d'accès à Internet doit revêtir un caractère exceptionnel. Une traçabilité des accès aux outils de captation et de leur utilisation devrait donc être mise en œuvre. Le projet de loi pourrait renvoyer la définition de ces mesures techniques de traçabilité à des dispositions réglementaires prises après avis de la CNIL.

I. Les fichiers d'analyse sérielle

Les fichiers d'analyse sérielle visent à opérer des rapprochements entre les procédures judiciaires afin d'identifier et de poursuivre les auteurs de crimes ou délits commis en série, dans le domaine de la criminalité violente.

Le projet de loi a notamment pour objet d'élargir le champ d'utilisation de ces traitements à la lutte contre la petite et la moyenne délinquance de masse. Il prévoit, à cet effet, d'étendre le nombre des infractions concernées par ces traitements, par le biais de l'abaissement du seuil des peines encourues à cinq ans d'emprisonnement contre plus de sept ans concernant les crimes ou délits portant atteintes aux biens (article 10).

Tout en prenant acte que la collecte des données personnelles relatives à toute personne citée dans une procédure judiciaire a été abandonnée, la Commission rappelle son extrême réserve sur l'extension du champ d'application des traitements d'analyse sérielle. En effet, la mise en œuvre de tels traitements doit être circonscrite à un champ restreint d'infractions qui doivent revêtir un caractère exceptionnellement grave.

II. Les logiciels de rapprochement judiciaire

Le projet de loi prévoit la création de logiciels de rapprochement judiciaire (article 11 *ter*), qui ont également trait à la sérialité des infractions. Ils doivent cependant être différenciés des fichiers d'analyse sérielle, dans la mesure où ils traitent essentiellement de données relatives aux modes opératoires caractéristiques des infractions. A cet égard, ces traitements n'ont donc pas pour objet premier de constituer des fichiers sur les personnes.

Cependant, dans la mesure où ces logiciels ont pour objectif d'améliorer le taux d'élucidation des faits de petite et moyenne délinquance, et notamment d'identifier les auteurs récidivistes de telles infractions, ils doivent nécessairement enregistrer des données relatives aux personnes mises en cause ainsi qu'aux victimes. Or, le projet de loi ne précise pas la nature des données à caractère personnel susceptibles d'être enregistrées, ni les infractions visées, ni les personnes concernées par ces traitements.

En outre, les données enregistrées dans ces logiciels devraient être conservées durant une période limitée. Or, en l'état actuel du texte, il est prévu une durée de conservation de trois ans à compter du dernier acte d'enregistrement. La notion de dernier acte d'enregistrement ne

semble pas pertinente puisqu'elle pourrait aboutir à des durées de conservation extrêmement longues, du fait des mises à jour successives des informations.

III. La vidéosurveillance (vidéoprotection)

Les articles 17A à 18bis du projet de loi modifient les dispositions de la loi du 21 janvier 1995 relatives à la vidéosurveillance (vidéoprotection).

Ils visent notamment à étendre les finalités pour lesquelles le recours à la vidéosurveillance (vidéoprotection) de voie publique peut être autorisé. Ces nouvelles finalités concernent la régulation des flux de transport, la prévention de lieux particulièrement exposés au trafic de stupéfiants ou de trafics illicites, et la prévention des risques naturels ou technologiques.

Par ailleurs, le texte donne la possibilité aux autorités publiques, après information préalable du maire, de déléguer l'exploitation de leur système de vidéosurveillance (vidéoprotection) à des opérateurs publics ou privés agissant pour leur compte, sur la base d'une convention type agréée par le Préfet. Une procédure d'agrément des opérateurs (agents et salariés) chargés de visionner les images par le préfet, ainsi que l'interdiction pour les salariés ou agents de l'opérateur d'accéder aux images enregistrées sont également prévues.

La Commission relève qu'une telle délégation à des opérateurs privés est susceptible de porter atteinte à l'intégrité du processus en termes de fiabilité et de sécurité. Elle souligne en outre que ces dispositions comportent un risque de sous-traitance externalisée des opérations de vidéosurveillance (vidéoprotection) vers des pays tiers, rendant ainsi impossible tout contrôle sur le territoire national.

La question du contrôle des dispositifs de vidéosurveillance (vidéoprotection)

La nécessité du contrôle, par un organisme indépendant, des dispositifs de vidéosurveillance (vidéoprotection), autrement dit le contrôle des surveillants, constitue une exigence fondamentale afin d'asseoir la légitimité de ces systèmes dans le respect des droits et libertés des citoyens.

L'émergence de formes plus évoluées de la technologie de vidéosurveillance (vidéoprotection) rend ce contrôle indépendant plus nécessaire encore qu'auparavant. Les systèmes de vidéosurveillance (vidéoprotection) dite « *intelligente* », capables de détecter dans une foule des mouvements ou des sons « *anormaux* », ou encore de reconnaître des visages de personnes, sont déjà en cours d'expérimentation.

Ainsi que l'a rappelé le Conseil constitutionnel par sa décision n°2010-604 du 25 février 2010 sur la loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public, le Législateur ne peut créer de nouveaux usages en matière de vidéosurveillance (vidéoprotection) sans prévoir les garanties nécessaires à la protection de la vie privée. L'adoption d'un dispositif de contrôle national indépendant constitue l'une de ces garanties fondamentales nécessaire au contrôle démocratique de ces dispositifs.

Or, l'encadrement juridique des systèmes de vidéosurveillance (vidéoprotection) demeure incertain. Ainsi, il n'existe pas, dans le dispositif législatif actuel, d'organisme indépendant

chargé de superviser le contrôle de ces dispositifs sur l'ensemble du territoire national, afin d'en harmoniser le développement.

Comme l'a proposé le rapporteur du texte au Sénat, le contrôle des dispositifs de vidéosurveillance (vidéoprotection) de voie publique et des lieux ouverts au public serait toujours confié aux commissions départementales mais aussi à la CNIL, qui l'exerce déjà pour les lieux privés et pour les dispositifs combinés à des traitements automatisés de données. La Commission serait ainsi amenée à vérifier notamment les destinataires des images, leur durée de conservation, ainsi que la sécurité du système. La CNIL pourrait ainsi assurer l'harmonisation de l'ensemble des contrôles opérés .

La CNIL dispose d'un corps de contrôleurs de métier (juristes et ingénieurs) habilités par le Premier ministre, immédiatement opérationnels qu'il suffirait de renforcer. Elle est autorisée, de par la loi, à mener des contrôles sur place et sur pièces sur l'ensemble du territoire national. Elle dispose également de services spécialisés dans le traitement des plaintes des citoyens et d'une formation contentieuse, chargée de décider de sanctions administratives ou pécuniaires.

Elle dispose aussi d'une longue pratique des problématiques liées à la vidéosurveillance (vidéoprotection). Chaque année, elle reçoit de nombreuses plaintes sur le sujet ainsi que plusieurs milliers de déclarations et procéde à une centaine de contrôles. Son action s'appuie donc sur des services dédiés, professionnalisés et aguerris, en matière d'expertise juridique et technique. Elle est ainsi capable de suivre les évolutions technologiques des systèmes de vidéosurveillance (vidéoprotection) et d'en mesurer les enjeux.

La CNIL jouit en outre de réelles garanties d'indépendance, notamment grâce à sa composition collégiale et pluraliste.

Elle pourrait proposer au préfet d'ordonner, sur la base d'un rapport de contrôle qui lui serait adressé, ainsi qu'au responsable du système (c'est-à-dire souvent au maire), les mesures appropriées susceptibles d'assurer un fonctionnement du dispositif conforme à l'autorisation délivrée.

Elle rendrait public chaque année un rapport sur les contrôles opérés et les éventuelles recommandations qui en découleraient.

IV. Les scanners corporels

L'article 18 bis du projet de LOPPSI prévoit la possibilité de recourir, à titre expérimental et pour une durée de trois ans, à des scanners corporels pour effectuer les fouilles et visites des bagages et des personnes se trouvant dans les zones des aéroports non librement accessibles au public.

La démarche expérimentale retenue devrait permettre aux autorités françaises d'apprécier l'intérêt du déploiement des scanners corporels. Afin de tirer tout le parti possible de cette démarche, une évaluation précise de ces expérimentations doit être effectuée, et pourrait donc être expressément prévue par ces dispositions.

Il est à noter que le projet de LOPPSI prévoit des garanties entourant l'utilisation des scanners corporels. Ainsi, seuls les dispositifs utilisant la technologie des ondes millimétriques pourront être mis en œuvre, aucun stockage ou enregistrement des images n'est autorisé, les

opérateurs visualisant les images des personnes ne pourront connaître l'identité de celles-ci, ce qui se traduit notamment par l'isolement physique des locaux de visionnage. Enfin, le consentement des voyageurs sera recueilli préalablement au passage dans le sas du scanner corporel.

Ces caractéristiques apportent, en l'état, des garanties réelles du point de vue de la protection de la vie privée des personnes.

Cependant, l'encadrement juridique des scanners corporels devrait être le plus précis possible, afin de maintenir le nécessaire équilibre entre le respect de la vie privée et la sécurité publique. C'est pourquoi l'application de ces dispositions devrait être précisée par un décret en Conseil d'Etat afin d'en fixer les modalités d'application, et non pas seulement de déterminer la liste des seuls aéroports et destinations concernés comme le prévoit l'article 18 *bis* du projet de loi. Ce décret devrait ainsi fixer des modalités précises de consultation des images des scanners corporels par les personnels habilités, des sécurités techniques à mettre en œuvre, de l'exercice effectif des droits des personnes concernées (en précisant en particulier les modalités de recueil de leur consentement et de leur information), ainsi que des modalités d'habilitation des agents publics autorisés à visualiser les images.

Enfin, dans la mesure où ces nouveaux dispositifs d'imagerie constituent par nature des traitements de données à caractère personnel, ils relèvent des dispositions de la loi du 6 janvier 1978 modifiée. Dès lors, ce décret doit être pris en Conseil d'Etat après avis de la CNIL.

Alex TÜRK