Conférence de presse
19 mai 2014

Présentation du 34ème rapport d'activité 2013

Chiffres clés de l'année 2013

Les particuliers et la CNIL

Près de 10 000 demandes individuelles adressées à la CNIL

- 5 640 plaintes
  - Dans **99% des cas**, l'intervention de la CNIL se traduit par une suite favorable pour le plaignant.
- 4 305 demandes de droit d'accès indirect (fichiers de police, de gendarmerie, de renseignement, FICOBA, etc.) **+ 105 % depuis 2011** (2099 demandes).

L'action de contrôle et de sanction

- 414 contrôles (dont 134 contrôles vidéoprotection)
  - **89% des organismes se mettent en conformité à la suite d'un contrôle**
- 57 mises en demeure
  - **86% des organismes se mettent en conformité à la suite d'une mise en demeure**
- 5 avertissements
- 7 sanctions financières
- 1 relaxe

L'encadrement et la mise en conformité des acteurs

- 13 000 organismes ont désigné un correspondant informatique et libertés (CIL) (+ 21 % par rapport à 2012)
- 29 labels ont été délivrés
- 2542 décisions et délibérations adoptées (+ 20% par rapport à 2012)
- 247 autorisations, dont 3 autorisations uniques
- 129 avis
- 3 recommandations
- 11 085 déclarations relatives à des systèmes de vidéosurveillance
- 5 514 déclarations relatives à des dispositifs de géolocalisation
- 416 autorisations de systèmes biométriques
- 160 interventions extérieures (formations, colloques, conférences nationales et internationales, séminaires)

Simplification des formalités pour les organismes

En 2013, la CNIL a traité 92 351 dossiers de formalités qui comprennent 51 000 engagements de conformité, c'est-à-dire des formalités allégées sur le plan administratif mais garantissant un niveau homogène de protection des données.

93 % des formalités sont effectuées en ligne. 93% des usagers sont satisfaits de l'accomplissement des formalités préalables (source : IFOP).

En 2013, la CNIL a délivré les récépissés **dans un délai moyen de 48h pour les déclarations simplifiées et de 5 jours calendaires pour les déclarations.**

Temps forts 2013-2014

Mars 2013

- Lancement, par la CNIL, d'un groupe de travail sur l'accès aux données personnelles des résidents européens par des autorités publiques étrangères dans le cadre de lois extraterritoriales ;

Avril 2013

- Présentation des résultats de l'étude Mobilitics menée avec Inria.

Mai 2013

- 1er Sweep day : journée d'audit en ligne en coopération avec 20 autres autorités de protection des données internationales.
- Publication du « décret transparence » sur les liens d'intérêt dans le secteur de la santé.

Juin 2013

- Présentation des propositions de la CNIL à la suite des contrôles des fichiers d'antécédents judiciaires.
- Premières révélations d'Edward Snowden sur l'existence du programme de surveillance PRISM mis en place par la NSA.
- La présidente de la CNIL met en demeure Google de se conformer, dans un délai de trois mois, à la loi Informatique et Libertés.

Juillet 2013

- Organisation d'un Workshop OpenCNIL sur l'Open Data.
- 28 organismes (50 fin 2013) officialisent la constitution d'un Collectif pour faire de l'éducation au numérique la grande cause nationale 2014.
- Publication de la lettre Innovation et Prospective sur le *quantified self*.

Août 2013

- Le G29 saisit la Commission Européenne et entame une évaluation indépendante du programme Prism.

Septembre 2013

- La CNIL engage une procédure formelle de sanction à l'encontre de Google, ainsi que 5 autres autorités européennes.

Octobre 2013

- La Commission LIBE (Libertés civiles, de la justice et des affaires intérieures) du Parlement Européen adopte sa position sur le projet de règlement européen.

Novembre2013

- Adoption d'une recommandation sur les coffres-forts électroniques.

Décembre 2013

- Publication de la lettre Innovation et Prospective sur les drones : vision prospective et enjeux pour les libertés.
- Publication de la recommandation sur les cookies / mise à disposition de l'outil de visualisation Cookieviz développé par la CNIL.
- Promulgation de la loi de programmation militaire : la CNIL fait part de sa position et déplore que la rédaction définitive du texte semble autoriser un accès aux données de contenu et non seulement aux données de connexion.

Janvier 2014

- Le 5ème Prix de thèse Informatique et Libertés est attribué à Francesca Musiani pour ses travaux sur les architectures pair-à-pair (P2P).
- Open Data et données personnelles : lancement d'une consultation en ligne des acteurs.
- La formation restreinte de la CNIL prononce une sanction pécuniaire de 150 000 € à l'encontre de la société GOOGLE Inc et l'enjoint de procéder à la publication d'un communiqué relatif à cette décision sur la page d'accueil de Google.fr, sous huit jours à compter de la notification de la décision.
- À l'occasion de la journée européenne de la protection des données, la CNIL met en ligne sur sa page Facebook des conseils pour mieux protéger ses données sur Facebook.

Février 2014

- Nouveau collège de la CNIL : élection du Président et des vice-présidents.
- Election d'Isabelle Falque-Pierrotin à la présidence du G29.
- Création d'un nouveau label pour les services de coffre-fort numérique.
- Publication de l'avis de la CNIL sur le projet de loi relatif à la géolocalisation.
- Adoption d'une nouvelle recommandation sur l'utilisation des cartes bancaires pour le paiement à distance.

Mars 2014

- Publication de 5 nouvelles fiches pratiques pour connaître ses droits et ses obligations en matière de commerce et de marketing.
- La loi du 17 mars 2014 relative à la consommation donne à la CNIL la possibilité de procéder à des contrôles en ligne.

Avril 2014

- Adoption de l'avis du G29 sur PRISM et la surveillance généralisée.

Bilan 2013 : la protection des données, une préoccupation croissante des particuliers

L'année 2013 a une fois encore montré une activité en forte croissance avec plus de 2500 décisions adoptées, 5640 plaintes (près de 2000 concernant l'e-réputation), 4305 demandes de droit d'accès indirect reçues (soit près de 10 000 demandes individuelles) et 414 contrôles réalisés. Ces chiffres illustrent la place prépondérante des données personnelles à l'ère numérique, et la sensibilité croissante des citoyens. Face à cette activité en pleine expansion, la CNIL poursuit une action efficace et accélère sa mutation pour gagner encore en réactivité.

_____

1. Une préoccupation croissante des citoyens, une intervention déterminante de la CNIL

En 2013, la CNIL a enregistré environ 5640 plaintes, ce qui correspond à une stabilisation des demandes. Ceci s'explique toutefois essentiellement par une meilleure orientation des demandes dès leur réception et par une mise en avant de contenus pratiques précisant davantage les cas dans lesquels la CNIL peut intervenir (les fiches pratiques sur les données personnelles au travail et sur la vidéosurveillance/vidéoprotection ont ainsi été téléchargées plus de 100 000 fois).

L'action de la CNIL
Dans **99% des cas**, l'intervention de la CNIL se traduit par une suite favorable pour le plaignant.

L'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de plaintes ainsi que l'exercice du droit d'accès.

L'année 2013 a parallèlement confirmé la tendance observée depuis 2011 quant au nombre important de plaintes relatives au secteur « internet/télécom » (34 % des plaintes reçues) et plus particulièrement aux **problématiques d'e-réputation**. **La CNIL a ainsi reçu 1 917 plaintes qui portent sur la suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne, la réutilisation de données publiquement accessibles sur internet, etc.**

Les autres motifs de plaintes sont, selon les secteurs concernés, les suivants :

- **Commerce** (19% des plaintes reçues) : radiation de fichiers publicitaires, conservation coordonnées bancaires, fichiers clients, opposition à recevoir des courriels publicitaires ;

- **Gestion des ressources humaines** (15% des plaintes reçues qui émanent de salariés ou de syndicats) : vidéosurveillance, géolocalisation, accès au dossier professionnel, cybersurveillance ;

- **Banque** (11% des plaintes reçues) : le motif principal de plainte est la contestation de l'inscription au FICP (fichier national des incidents de remboursement des crédits aux particuliers, ou au FCC (fichier central des chèques et des retraits de cartes bancaires).

- **Libertés publiques et collectivités locales** (7% des plaintes reçues) : élections présidentielles et législatives, presse en ligne, diffusion par les collectivités locales de documents publics sur internet.

Le devenir des données personnelles des personnes décédées sur les réseaux sociaux : une question nouvelle et de plus en plus fréquente.
Les personnes interrogent souvent la CNIL pour savoir s'il est possible d'accéder au compte Facebook d'un membre de leur famille décédé ou de faire fermer le compte. La procédure de demande de suppression de compte est réservée à la famille proche du défunt sur présentation d'un justificatif du lien de parenté. En revanche, la famille ne peut avoir accès aux données contenues sur le compte. Etant donné les nouvelles questions que posent ce concept de **« mort numérique »**, la CNIL a engagé une réflexion sur ce sujet en 2014.

2. Des demandes de droit d'accès indirect en forte croissance : FICOBA et les fichiers d'antécédents judiciaires ou de renseignement

En 2013, la CNIL a reçu **4305 demandes de droit d'accès indirect, soit une augmentation de 17% par rapport à 2012**. Ces demandes reçues représentent un total de 7148 vérifications à mener concernant par ordre d'importance : le fichier FICOBA de l'administration fiscale, les fichiers d'antécédents judicaires de la police et de la gendarmerie (fichier unique TAJ depuis le 1er janvier 2014) et les fichiers de renseignement.

Si on cumule les plaintes et les demandes de droit d'accès indirect, **ce sont donc près de 10 000 demandes individuelles qui ont été adressées à la CNIL en 2013**.

A cela se sont ajoutés 124 000 appels téléphoniques à la permanence juridique de la CNIL.

Ces chiffres témoignent donc de la sensibilité croissante des personnes concernées quant à la protection de leurs données personnelles dans un univers numérique marqué par la très forte circulation de ces données.

Gros plan sur FICOBA

Pourquoi cette augmentation des demandes d'accès à FICOBA ?

L'augmentation importante du nombre de demandes de droit d'accès indirect au fichier FICOBA dont la CNIL est désormais destinataire (**2167 demandes en 2013**), trouve son origine dans la reconnaissance par le Conseil d'Etat dans une décision du 29 juin 2011 du droit d'accès des héritiers en leur qualité « d'ayant droit du solde des comptes bancaires détenus par la personne décédée ».

Que contient FICOBA ?

Ce fichier, détenu par l'administration fiscale, permet à l'héritier d'avoir un recensement des comptes détenus par le défunt sur le territoire national (établissement, numéro et nature du compte, date d'ouverture, de modification ou de clôture), de nature à faciliter ses démarches aux fins de règlement de la succession. Il ne comporte aucune donnée concernant l'historique des opérations bancaires effectuées ou le solde des comptes à une date donnée.

Qui sont les demandeurs ?

Près de 80% des demandes reçues par la CNIL émanent soit des héritiers eux-mêmes soit, le plus fréquemment, des notaires en charge de la succession qu'ils ont mandatés en ce sens.

Pourquoi les délais sont-ils longs ?

Comme pour l'ensemble des fichiers relevant du régime de droit d'accès indirect, l'exercice d'un tel droit n'emporte pas un droit à communication systématique des données par l'intermédiaire de la CNIL. L'administration fiscale peut ainsi s'opposer à la communication pour des motifs liés au recouvrement des impositions ou à la lutte contre la fraude fiscale.

De tels éléments « de contexte » ne peuvent être issus du fichier FICOBA mais de données dont l'administration fiscale dispose par ailleurs et nécessitent, dès lors, une étude particulière de chacun des dossiers.

Le volume important de demandes, ainsi que cette phase de recherches préalables aux vérifications par un magistrat de la CNIL, expliquent qu'une réponse ne puisse être apportée dans de très brefs délais, même si tant la CNIL que ses interlocuteurs au sein de l'administration fiscale s'attachent à assurer un rythme de traitement soutenu. Actuellement, le délai moyen est de 6 mois.

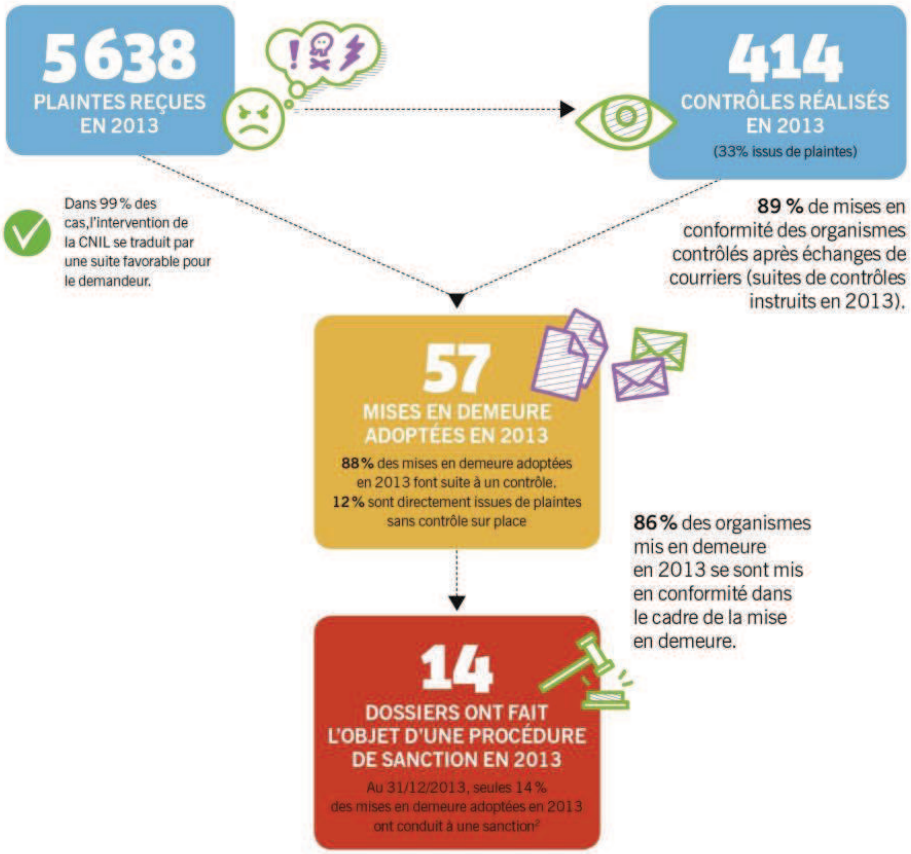
Vers une consultation de FICOBA par les notaires ?

Actuellement, les notaires ne disposent pas de la qualité de « tiers autorisé » qui leur donnerait la possibilité de solliciter directement l'administration fiscale pour obtenir les données issues de FICOBA qui leur sont nécessaires dans le cadre du règlement de successions. A la suite d'un rapport de la Cour des comptes de juillet 2013 et d'une mission d'information parlementaire, une proposition de loi a été déposée à l'Assemblée nationale visant à instaurer un droit mais aussi d'une obligation pour les notaires de consulter FICOBA.

3. Plaintes, contrôle, mise en demeure, sanction : une action suivie d'effet

La logique de la loi et son application par la CNIL visent avant tout la mise en conformité des organismes mis en cause. A chaque phase d'instruction d'une plainte et/ou d'un contrôle, ils ont donc la possibilité de suivre les mesures recommandées par la CNIL pour se mettre en conformité. C'est la raison pour laquelle « seulement » 14 sanctions ont été prononcées par la CNIL en 2013 pour un volume initial de quelques 6000 plaintes traitées.

En effet, **dans l'immense majorité des cas, la simple intervention de la CNIL se traduit par une mise en conformité de l'organisme et la satisfaction de la demande du plaignant.** Le prononcé de sanction par la CNIL permet ainsi de sanctionner des organismes qui persistent dans des comportements répréhensibles, et constitue donc un instrument de dissuasion important.



Piloter la conformité : objectif premier du régulateur

Dans un environnement technologiquement complexe, les acteurs publics ou privés sollicitent de plus en plus la CNIL pour s'assurer de la conformité de leurs traitements aux exigences légales. Pour les accompagner dans cette démarche, la CNIL leur propose différents outils pratiques et une approche sectorielle.

1. Les outils de la conformité

Pour la CNIL, accompagner la conformité signifie à la fois une nouvelle méthode de travail - associer pleinement les acteurs pour recueillir et comprendre leurs besoins - ainsi que de nouveaux outils - référentiels sectoriels et outils pratiques qui permettent de décliner, pour un secteur donné, les principes de la loi « informatique et libertés ». L'objectif de cette approche consiste à simplifier les formalités autant que possible sur le plan administratif moyennant le respect, par les organismes concernés, de bonnes pratiques régulièrement mises à jour.

La CNIL s'est donc engagée dans cette démarche d'accompagnement des professionnels en leur proposant des outils d'aide à la conformité tels que : les CIL (correspondants informatique et libertés), les labels, les règles internes d'entreprises (BCR) et la création de packs de conformité sectoriels.

Les correspondants « informatique et libertés », acteurs de la co-régulation

Chaque année, le CIL s'affirme un peu plus comme un acteur central de la mise en conformité. Fin 2013, **13 000 organismes avaient désigné un CIL**, contre 11 000 un an plus tôt. La richesse de la désignation d'un CIL s'apprécie particulièrement à l'occasion d'un nouveau projet impliquant un traitement de données personnelles grâce à ses conseils, lors de l'instruction d'une plainte ou d'un contrôle de la CNIL ou enfin dans la facilitation de l'exercice des droits d'accès ou d'opposition.
Appelé à prendre la suite du CIL avec des missions renforcées, le futur délégué à la protection des données sera au cœur du modèle proposé par le projet de Règlement européen.

Le label : un gage de confiance

La loi "informatique et libertés" permet à la CNIL de délivrer des labels "à des produits ou des procédures" (article 11).

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

A ce jour, trois référentiels ont été créés à la demande d'organisations professionnelles : le label « formations » et le label « audit de traitement », adoptés en 2012, et le 1er label produit adopté en 2014 pour les services de coffre-fort numérique.

Depuis 2012, ce sont **29 labels** qui ont été délivrés par la CNIL.

Les packs de conformité : une nouvelle approche sectorielle

Il est important de permettre aux entreprises d'un secteur d'accéder facilement à l'ensemble des outils et bonnes pratiques adaptés à leurs besoins pour protéger de manière optimale les données personnelles. C'est le sens des « packs de conformité »développés par la CNIL, qui contiennent des outils juridiques de simplification ou d'allégement des formalités ainsi que des bonnes pratiques spécialement adaptées au secteur professionnel. L'année 2013 a permis d'élaborer, à la suite d'une large concertation avec les professionnels concernés, différents packs sectoriels qui verront le jour en 2014 : le pack « assurance », le pack « logement social », le pack « compteurs communicants » et le pack « collectivités locales ».

Les recommandations

En 2013, la CNIL a élaboré 3 recommandations qui permettent de préciser aux professionnels les conditions de mise en œuvre pratiques de la loi. Ces recommandations ont porté respectivement sur les cookies et autres traceurs, la conservation des cartes bancaires par les commerçants et les coffres-forts numériques. A la suite de la recommandation sur les cookies, qui s'est accompagnée de la publication de nombreuses fiches pratiques, les principaux sites se sont mis en conformité.

2. Conseiller les pouvoirs publics

En 2013, la CNIL a rendu 74 avis sur des projets de décrets ou de loi. A titre d'exemple la CNIL a rendu un avis sur :

- Le projet de loi relative à la consommation avec des dispositions prévoyant la mise en place d'un registre national des crédits aux particuliers ;
- La transparence des liens d'intérêts dans le secteur de la santé ;
- La transparence de la vie politique ;
- La PNIJ (plateforme nationale des interceptions judiciaires): texte réglementaire pas encore publié ;
- Le Projet de loi relatif à l'utilisation de la géolocalisation dans le cadre des enquêtes judiciaires ;
- Le TAJ (traitement des antécédents judiciaires) ;
- Les téléservices publics locaux.

Par ailleurs, la CNIL met à disposition des parlementaires son expertise juridique et technologique et propose des actions d'information ou de sensibilisation. En 2013, elle a participé à plus d'une vingtaine de rendez-vous et d'événements avec des parlementaires (auditions, rendez-vous de travail, démonstration de l'outil Cookieviz).

3. Accompagner l'innovation

Dans le cadre de son activité d'innovation et de prospective, la CNIL renforce sa capacité d'écoute et de dialogue avec de très nombreux acteurs d'horizons divers. Cette démarche lui permet de mieux anticiper les évolutions technologiques et d'accompagner les nouveaux usages le plus en amont possible pour garantir une innovation durable, respectueuse des droits des utilisateurs. Pour ce faire, la CNIL peut mobiliser son équipe d'experts informatiques ainsi que 3 chargés d'études prospectives.

La CNIL s'est notamment dotée d'un laboratoire d'innovation en 2011, qui permet de tester des produits et applications innovants, de développer des outils mis à disposition du public tels que l'outil Cookieviz qui a été téléchargé 62 500 fois et enfin de mener à bien des projets de recherche et développement comme le projet Mobilitics en partenariat avec Inria.

Vidéoprotection : bilan de 3 ans de contrôles

Depuis la loi d'orientation et de programmation pour la performance et la sécurité intérieure du 14 mars 2011 (LOPPSI 2), la CNIL est compétente pour contrôler, sur place, les conditions de mise en œuvre des dispositifs de vidéoprotection. Après trois années de vérifications sur le terrain, il est, aujourd'hui, possible pour la CNIL de dégager les principales conclusions de l'ensemble de ces contrôles.

Après 3 ans de contrôles, la CNIL est devenue un acteur essentiel, et reconnu, de ce secteur. Cette reconnaissance est issue du résultat de l'investissement de la CNIL en matière de contrôle. En effet, depuis 2011, la CNIL a concentré près d'un tiers de ses contrôles sur ces systèmes, soit plus de 450 missions sur l'ensemble du territoire national. En particulier, au cours de l'année 2013, **elle a réalisé plus de 130 contrôles. En tout, ce sont ainsi plusieurs dizaines de milliers de caméras qui ont pu être contrôlées.**

La CNIL a développé une méthodologie précise des contrôles qu'elle effectue afin que les garanties essentielles prévues par la loi (information des personnes, durée de conservation, limitation des zones filmées, sécurité du système, etc.) soient précisément contrôlées, de manière uniforme sur l'ensemble du territoire. Cette expertise est d'ailleurs parfois sollicitée par les organismes eux-mêmes puisque, comme le leur permet la loi, certains d'entre eux demandent à la CNIL un contrôle du système qu'ils mettent en œuvre. Cette démarche de mise en conformité a été adoptée par des acteurs importants (SNCF, RATP, communes) et doit être encouragée.

Enfin, la CNIL est très fréquemment saisie par des salariés qui s'interrogent sur les conditions de mise en œuvre de dispositifs de vidéosurveillance par leur employeur (un peu plus de 300 plaintes).

Quels constats ?

Dans plus de la moitié des cas, les systèmes sont composés de plusieurs caméras et relèvent, pour partie, du code de la sécurité intérieure et, pour partie, de la loi "informatique et libertés". Si les obligations sont, dans le fond, globalement les mêmes, l'existence d'un double régime juridique est parfois source d'incompréhension pour les responsables concernés.

Une absence de formalités préalables

L'application de la loi "informatique et libertés" aux caméras filmant les lieux non ouverts au public est relativement ignorée des responsables de traitement, ce qui a conduit la CNIL à constater que près de la moitié des dispositifs n'ont pas fait l'objet de formalités préalables auprès d'elle.

En ce qui concerne les caméras filmant la voie publique ou les lieux ouverts au public, seuls 15% d'entre eux n'avaient pas été autorisés par le préfet territorialement compétent. Néanmoins, la CNIL a constaté à plusieurs reprises que certains des dispositifs n'ont pas fait l'objet d'une demande de renouvellement de leur autorisation préfectorale.

Une information des personnes à améliorer

L'information des personnes constitue une des garanties essentielles apportées par la loi, notamment en ce qu'elle permet aux personnes filmées d'exercer, si elles le souhaitent, leur droit d'accès aux images qui les concernent. **Or, dans plus de 30% des cas, la CNIL a pu constater que cette information était soit inexistante soit insuffisante** (par exemple, en ce qu'elle n'indique pas les coordonnées de la personne à contacter pour exercer le droit d'accès).

Des durées de conservation à améliorer

Environ 15% des contrôles ont démontré une durée de conservation des images supérieure à celle autorisée par le préfet pour les dispositifs de vidéoprotection, ou admise par la CNIL pour la vidéosurveillance. Ces résultats sont essentiellement dus à une absence de paramétrage des dispositifs d'enregistrement.

Des mesures de sécurité insatisfaisantes

Dans plus de 30% des cas, les contrôleurs de la CNIL ont relevé des manquements au regard de l'obligation de sécuriser les dispositifs vidéo (accès aux images en temps réel ou accès aux enregistrements). Ces manquements peuvent consister en une mauvaise gestion des mots de passe permettant l'accès au dispositif de visualisation ou d'enregistrement mais peuvent aussi se traduire par un mauvais paramétrage du système qui rend parfois les caméras concernées accessibles depuis internet.

Des dispositifs parfois trop intrusifs

En ce qui concerne les dispositifs de vidéoprotection, la CNIL vérifie que les zones filmées sont uniquement celles autorisées par l'arrêté préfectoral. Elle porte une attention toute particulière aux dispositifs mis en œuvre par les collectivités locales afin que ceux-ci « ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées » (article L. 251-3 du code de la sécurité intérieure). Au cours de l'année 2013, **la CNIL a ainsi mis en demeure 7 communes** pour ne pas avoir respecté cette disposition essentielle au regard de la protection de la vie privée des personnes vivant sur le territoire communal.

En ce qui concerne les dispositifs de vidéosurveillance, la CNIL exerce un contrôle plus poussé du dispositif qui doit répondre aux exigences de proportionnalité posées par la loi du 6 janvier 1978 modifiée. Ainsi, la CNIL a précisé, notamment dans des fiches pratiques diffusées sur son site internet, les conditions de mise en œuvre de ces dispositifs afin que ceux-ci ne portent pas atteinte à la vie privée des personnes filmées (les salariés ne doivent pas être filmés de manière permanente, interdiction de filmer l'entrée des habitations …).

Quelles suites ?

D'une manière générale, les organismes souhaitent se conformer aux préconisations qui sont adressées par la CNIL. En effet, les manquements relevés résultent le plus souvent d'une mauvaise connaissance du cadre légal plutôt que de la volonté de mettre en place un dispositif portant atteinte aux droits et libertés des personnes.

Ainsi, l'envoi d'un courrier d'observation est généralement suffisant pour obtenir une mise en conformité du dispositif contrôlé (94% des cas en 2013). Pour autant, en cas de manquement grave ou d'une absence de volonté de la part du responsable de se conformer à la loi, la CNIL peut prononcer une mise en demeure voire une sanction.

Ainsi, en 2013, la présidente de la CNIL a prononcé 8 mises en demeure portant sur les conditions de mise en œuvre de dispositifs de vidéoprotection et 8 mises en demeure concernant des dispositifs de vidéosurveillance. Les principaux manquements relevés sont relatifs à l'orientation des caméras, l'information des employés, la sécurité du système et la durée de conservation des images.
Enfin, la CNIL a développé des **outils d'information pédagogiques** sur le sujet. Elle a ainsi mis à disposition du public une série de fiches pratiques sur les conditions à respecter pour mettre en œuvre un dispositif de ce type. Ces fiches ont été téléchargées plusieurs dizaines de milliers de fois.

Une nécessaire harmonisation des conditions de mise en œuvre des dispositifs de vidéoprotection

La mise en œuvre d'un dispositif de vidéoprotection est soumise à l'accord préalable du préfet territorialement compétent, après avis d'une commission départementale. A l'occasion des contrôles, la CNIL a constaté des divergences entre préfectures concernant les conditions de mise en œuvre des dispositifs de vidéoprotection. La CNIL a donc alerté le ministère de l'intérieur sur la nécessité d'une application homogène des dispositions relatives à la vidéoprotection.

Une analyse des évolutions techniques des dispositifs vidéo et de leurs conséquences juridiques

Les contrôles effectués par la CNIL permettent également de constater les évolutions techniques de ces dispositifs qui, pour certaines d'entre elles, conduisent à réfléchir au cadre juridique applicable.
Les tendances :

- des dispositifs accessibles depuis des smartphones dont la sécurité de l'accès aux images et enregistrements n'est pas toujours assurée.
- des dispositifs vidéo composés de caméras permettant un enregistrement du son. Or, cette possibilité n'est ni prévue, ni interdite par le code de la sécurité intérieure bien qu'elle pose des questions au regard de la protection de la vie privée des personnes situées dans leur champ de visualisation et donc, d'enregistrement sonore.
- des dispositifs d'enregistrement vidéo embarqués dans l'habitacle de véhicules susceptibles d'être occupés par le public (taxi, ambulances), dont on peut questionner le caractère ouvert au public, ou non.
- déploiement de caméras « dômes » dotées d'une très forte capacité de zoom.

Ces caméras, qui sont capables de filmer à 360° avec une redoutable capacité de précision, défient la notion juridique de « proportionnalité », centrale en matière de protection des données à caractère personnel. Si une solution peut être trouvée par la mise en place de caches physiques ou numériques destinés à restreindre les zones filmées, ces protections se révèlent généralement insuffisantes.
L'ensemble de ces questions a conduit la CNIL à saisir le ministère de l'intérieur afin d'envisager les évolutions à apporter au cadre légal pour préserver l'équilibre entre la protection de la vie privée et la sécurité des biens et des personnes.

Une nouvelle organisation pour mieux répondre aux attentes des différents publics

La massification du traitement des données personnelles ainsi que la diversification de ses usages entrainent une croissance exceptionnelle de l'activité de la CNIL. Pour faire face à ce phénomène et à quelques mois de l'adoption du projet de règlement européen, la CNIL doit faire preuve d'initiative et d'innovation, aussi bien en termes de méthodes que d'outils de régulation. C'est précisément pour mieux répondre aux attentes de ses différents publics que la CNIL a procédé, en avril 2014, à la réorganisation de ses services.

Dans le cadre du plan d'orientation stratégique 2012-2015, la CNIL a développé une stratégie claire : s'adapter à un environnement numérique en constante évolution en développant une gamme élargie d'outils de régulation et en plaçant ses publics au cœur de ses préoccupations. C'est dans la logique de cette stratégie et pour accélérer sa mutation qu'une réorganisation des services a été décidée par la présidente de la CNIL. Les objectifs sont les suivants :

- **Gagner en réactivité et en agilité** en recentrant les directions sur leurs missions principales.
- **Accorder une place centrale à nos publics :** développer la concertation aves les professionnels ; adopter une approche plus sectorielle ; proposer de nouveaux services en ligne plus adaptés aux besoins du grand public, notamment un service de questions/réponses en ligne sur son site.
- **Promouvoir une gamme élargie d'outils de régulation**, dans une logique de simplification et d'accompagnement renforcé des acteurs.
- **Accompagner les acteurs dans le développement de projets innovants** et durables.

Les services sont désormais organisés en cinq directions : la direction de la conformité, la direction des relations avec les publics, la direction de la protection des droits et des sanctions, la direction des technologies et de l'innovation et la direction administrative et financière.

Projet de règlement européen : point d'étape

La proposition de règlement a fait en 2013 l'objet de débats intenses, au Parlement européen comme au Conseil de l'UE. Les enjeux importants, qui sont à la fois technologiques, politiques, économiques et internationaux, ont retardé l'adoption du règlement. Dans ce contexte, la CNIL s'attache à promouvoir un cadre juridique équilibré, efficace et protecteur des droits des citoyens.

_____

Présentée par la Commission européenne le 25 janvier 2012, la proposition de règlement de l'Union européenne (UE) sur la protection des données personnelles vise à uniformiser la législation des Etats membres en l'adaptant au nouveau contexte numérique. Pour que le règlement soit adopté, le Parlement européen et le Conseil de l'UE doivent définir leurs positions respectives avant de négocier un texte de compromis. Le Parlement européen a adopté le 12 mars 2014, à une forte majorité, sa position en première lecture. Jugée globalement positive par la CNIL, cette position servira de base de négociation avec le Conseil lorsque celui-ci aura défini sa propre position.

Déjà des axes de convergence se dessinent, préfigurant les futures orientations de la réforme, notamment :

- la confirmation d'un champ d'application territorial large du règlement ;
- un renforcement des droits des personnes ;
- un allégement des formalités préalables couplé à une responsabilisation des entreprises ;
- la création d'un statut légal pour les sous-traitants ;
- le développement de la certification et des codes de conduite européens ;
- une approche plus protectrice de l'encadrement des transferts de données hors de l'UE ;
- une harmonisation des pouvoirs des autorités de protection et des sanctions renforcées.

Les sujets de préoccupation

Le guichet unique pour les entreprises – La CNIL estime que s'il est légitime que les entreprises implantées dans plusieurs Etats membres puissent disposer d'un interlocuteur unique pour les traitements de données mis en œuvre dans ces pays, cette nécessité pratique ne doit pas pour autant remettre en cause la garantie d'une protection de proximité pour le citoyen, lui permettant d'exercer effectivement ses droits sur son territoire de résidence. La CNIL s'est donc attachée à promouvoir un modèle de gouvernance équilibré, dans l'intérêt de tous. Elle a donc conçu, en étroite collaboration avec le Gouvernement français, une solution alternative et crédible au modèle de guichet unique tel que proposé par la Commission.

Les données pseudonymes – La CNIL admet que la pseudonymisation des données, en tant que mesure de sécurité, peut justifier un régime d'obligations allégées pour les responsables de traitement dans le respect des exigences de proportionnalité ; elle met toutefois en garde contre la création d'un régime dérogatoire pour les données pseudonymes en tant

que telles. Le danger est double : d'une part, les capacités croissantes de croisement des données rendent la protection contre une identification du sujet toute relative ; d'autre part, dans l'économie numérique, des pseudonymes « numériques » sont de plus en plus utilisés comme forme alternative d'identification dans le but direct de cibler des individus.

L'approche par les risques – La CNIL admet que la mise en œuvre des obligations particulières pesant sur les responsables de traitement (et les sous traitants) puisse être modulée en fonction des risques pour les droits et libertés fondamentales pour la personne concernée ; elle considère toutefois que l'approche par le risque ne doit en aucun cas affecter les droits ni conduire à exonérer le responsable de traitement (ou le sous-traitant) de son obligation générale de conformité aux dispositions du règlement, ni même l'exonérer de certaines de ses obligations particulières.

Dans ce contexte, la CNIL continue de sensibiliser les pouvoirs publics à ses préoccupations. Elle s'attache aussi à défendre ses positions dans le cadre du Groupe de l'article 29, qui regroupe les « CNIL européennes ».

Propositions sur les évolutions de la loi informatique et libertés dans le cadre d'un projet de loi numérique

Le Gouvernement a annoncé, à l'occasion du séminaire sur le numérique de février 2013, son intention de déposer un projet de loi sur le numérique. Les ministères de la Justice et de l'économie numérique ont été chargés de préparer ce projet, qui pourrait être examiné par le Parlement début 2015. La CNIL formule plusieurs propositions d'évolution législative qui pourraient être envisagées dans la perspective de ce projet de loi. Elles devront bien sûr s'articuler avec le projet de règlement européen actuellement en discussion.

Ces propositions concernent les quatre principaux acteurs de l'écosystème « informatique et libertés » : les individus, les entreprises, les pouvoirs publics, et enfin la CNIL.

I. Le renforcement de l'effectivité des droits pour les personnes

Pour faire de l'univers numérique un espace de droits et de libertés, il est essentiel de renforcer les droits des personnes. Le futur règlement prévoit d'ailleurs de nouveaux droits au bénéfice de l'individu (droit à l'oubli, à la portabilité des données, etc.). Cependant, plusieurs propositions peuvent d'ores et déjà être retenues à cadre européen constant :

Un renforcement du droit d'accès

- Introduire **la possibilité pour les individus d'exercer les droits conférés par les articles 38 à 40 (opposition, accès, rectification) par voie électronique**.
- Introduire l'obligation du responsable de traitement de **transmettre aux personnes une preuve de l'exercice de leurs droits afin de faciliter le régime de la preuve** (par exemple, permettre aux individus, exerçant leur droit d'opposition via un lien de désabonnement, de recevoir un email prouvant l'exercice de ce droit, constitutif d'une preuve en cas de non-respect de celui-ci).

Une protection particulière pour les mineurs

La loi ne comporte aucune disposition propre aux mineurs, alors même que l'immense majorité d'entre eux utilise, notamment, les réseaux sociaux, et que les questions de e-réputation sont régulièrement liées à des données mises en ligne avant l'âge de la majorité.

- Introduire dans la loi la possibilité d'obtenir l'effacement, notamment en ligne, de données personnelles de mineurs, via l'exercice du droit d'opposition. L'exercice d'un tel droit devrait être inconditionnel s'agissant des données portant sur une personne mineure en supprimant l'exigence d'un « motif légitime », actuellement prévu.

II. La simplification des formalités pour les entreprises

Dans la logique du projet de règlement et des efforts engagés par la CNIL depuis déjà plusieurs mois (dispenses, normes simplifiées et autorisation uniques), il parait opportun d'alléger les formalités pesant sur les responsables de traitement.

- **Simplifier les formalités relatives aux transferts internationaux lorsque les entreprises s'engagent dans un régime de garanties substantielles avec des**

« BCR » (*binding corporate rules* ou règles d'entreprise contraignantes) **:** les demandes d'autorisation pour les transferts internationaux de données connaissent une forte croissance (près de 1500 autorisations en 2013).

Par ailleurs, sans qu'une modification des textes soit nécessaire, la CNIL a décidé d'engager un processus de simplification administrative en accélérant l'adopt*ion de dispenses de déc*laration, normes simplifiées ou autorisations uniques. Ces différents outils permettent en effet de limiter la charge des formalités administratives pour des traitements relativement « standards » tout en fixant, en amont, des règles claires, stables et homogènes pour l'ensemble des organismes concernés.

III. Des relations renforcées avec les pouvoirs publics

Les relations avec les pouvoirs publics et le contrôle des fichiers publics constitue l'un des enjeux de la loi sur le numérique. La CNIL propose ainsi de donner la possibilité, pour les présidents des deux assemblées parlementaires, **de la saisir pour avis sur les propositions de loi**.

IV. La nécessaire évolution des règles dans le domaine des fichiers dits de souveraineté

Dans le contexte « post-Prism », il est nécessaire de donner des garanties supplémentaires aux individus en matière de contrôle des fichiers de souveraineté. Ces fichiers (DCRI, DGSE, etc.) sont en effet les seuls, en France, à ne pouvoir faire l'objet d'aucun contrôle de la CNIL ou d'une autre autorité administrative indépendante.

- **Etendre le pouvoir de contrôle de la CNIL aux fichiers de renseignement** selon des modalités tenant compte de leurs spécificités. Ce contrôle ne porterait que sur le respect de la loi informatique et libertés, dans les conditions de mise en œuvre desdits fichiers, et en aucun cas sur l'activité des services de renseignement.
- **Permettre un accès direct aux données contenues dans les fichiers d'antécédents judiciaires pour les personnes non mises en cause à quelque titre que ce soit (victimes, plaignants)**. Cela permettrait de désengorger partiellement l'activité de la CNIL et des services de police et de gendarmerie en matière de droit d'accès indirect, et d'accroître la transparence de ces fichiers.

V. Renforcer l'efficacité et la crédibilité des sanctions

- **Augmenter le montant maximal des sanctions, qui est de 150 000 euros maximum aujourd'hui.** Ce montant pourrait être exprimé en valeur absolue et en pourcentage du chiffre d'affaires.
- **Accélérer le possible déclenchement d'une procédure de sanction pécuniaire.** Actuellement, lorsque la situation est particulièrement urgente ou que le manquement n'appelle plus de correction, le président de la CNIL peut décider de saisir directement la formation restreinte, sans mise en demeure préalable. Toutefois, cette formation ne peut alors prononcer qu'un avertissement. La CNIL propose donc de faire évoluer la législation sur ce point.

La notification des violations de données personnelles

En 2013, le règlement européen *data breach* a été adopté. Entré en vigueur le 25 août dernier, ce règlement définit notamment les délais, le contenu et les modalités de la notification aux autorités des failles de sécurité et de l'information faite aux personnes par les opérateurs de communications électroniques. En 2013, la CNIL a reçu 15 notifications à ce titre.

_____

Qu'est-ce qu'une violation de données à caractère personnel ?

Toute destruction, perte, altération, divulgation ou accès non autorisé à des données à caractère personnel est une violation de données à caractère personnel.
Une violation peut résulter d'un acte malveillant (par exemple, en cas de piratage informatique) ou se produire à la suite d'une erreur matérielle (par exemple, lorsqu'un salarié détruit ou divulgue le fichier clients de sa société par une fausse manipulation).

Le principe : une obligation de notification

Actuellement, sont seuls concernés par cette obligation de notification les opérateurs de communications électroniques (FAI, opérateurs de téléphonie fixe et mobile), lorsque la violation intervient dans le cadre de leur activité de fourniture de services de communications électroniques.

Une généralisation de cette obligation à tous les responsables de traitement est prévue dans le projet de règlement sur la protection des données. Dans l'intervalle, les responsables de traitement qui n'entrent pas dans le champ de l'article 34 bis de la loi du 6 janvier 1978 modifiée sont soumis à une obligation générale de sécurité et de confidentialité des données (article 34 de la loi).

Les modalités de la notification

Les opérateurs doivent notifier à la CNIL toute violation de données, et ce quel qu'en soit la gravité.
Ils doivent également informer les personnes concernées par la violation, sauf lorsque :

- la violation n'est pas susceptible de porter atteinte aux données ou à la vie privée des personnes concernées ;
- l'opérateur a mis en œuvre, en amont, des mesures de protection appropriées qui rendent les données incompréhensibles à toute personne non autorisée à y avoir accès.

- Nombre de notifications reçues par la Cnil

L'action de la CNIL

31 notifications ont été reçues par les services depuis 2011, dont 15 en 2013 et 2 en 2014.
En août 2013, une téléprocédure a été mise en place pour permettre aux opérateurs de procéder aux notifications de façon sécurisée, conformément au règlement européen. Cette téléprocédure est accessible à partir du site de la CNIL

En février 2014, constatant que les dispositions de la loi du 6 janvier 1978 modifiée et du règlement européen ne sont pas ou que partiellement respectées, la Commission a organisé

une réunion avec les principaux opérateurs. Cette réunion a été l'occasion de rappeler aux opérateurs leurs obligations et d'aborder les difficultés que ces derniers rencontrent (notamment le respect des délais de notification).

A la suite de cette réunion, la thématique des violations de données personnelles a été inscrite au programme annuel des contrôles de la CNIL. Ces contrôles peuvent être réalisés sur place ou, très prochainement, en ligne.

Tout manquement à l'article 34 bis constaté lors de ces contrôles pourra faire l'objet de sanctions administratives (avertissement, injonction de cesser le traitement et sanction pécuniaire de 150 000 euros) et pénales (300 000 euros et 5 ans d'emprisonnement).

La CNIL a déjà prononcé 10 mises en demeure relatives à des failles de sécurité et 8 sanctions.