Conférence de presse
23 avril 2013

Présentation du 33ème rapport d'activité 2012

Chiffres clés de l'année 2012

- 6017 plaintes (+ 4,9% par rapport à 2011)
- 3682 demandes de droit d'accès indirect (+ 75% par rapport à 2011), dont 1829 concernent l'accès au fichier FICOBA
- 458 contrôles (+19% par rapport à 2011)
- 173 contrôles vidéoprotection
- 10 709 organismes ont désigné un correspondant (+ 24 % par rapport à 2011)
- 16 Labels
- 160 interventions extérieures (formations, colloques, conférences nationales et internationales, séminaires)
- 43 mises en demeure
- 9 avertissements
- 4 sanctions financières
- 2 relaxes
- 2078 décisions et délibérations adoptées (+5,5% par rapport à 2011)
- 316 autorisations, dont 3 autorisations uniques
- 113 avis
- 3 dispenses
- 2 recommandations portant sur la communication politique et les compteurs communicants
- 8946 déclarations relatives à des systèmes de vidéosurveillance (+ 49,3% par rapport à 2011)
- 5483 déclarations relatives à des dispositifs de géolocalisation (+ 22,3 % par rapport à 2011)
- 795 autorisations de systèmes biométriques (+6,8 % par rapport à 2011)

Simplification des formalités pour les organismes
En 2012, la CNIL a traité 88 990 dossiers de formalités qui comprennent notamment 48 833 déclarations simplifiées, dont :

- 2255 engagements de conformité à un acte règlementaire unique
- 4720 engagements de conformité à une autorisation unique
- 255 engagements de conformité à la méthodologie de référence
- 319 engagements de conformité à une déclaration unique.

93% des formalités sont effectuées en ligne. 95% des usagers sont satisfaits de l'accomplissement des formalités préalables (source : IFOP).

En 2012, 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 2012-2013

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.

Septembre 2012

- Affaire du « bug Facebook ». La généralisation de la Timeline a créé une confusion de la part des utilisateurs qui ont eu l'impression que des messages privés anciens devenaient visibles.

Octobre 2012

- La CNIL et FIEEC ont organisé le 3 octobre 2012 une matinée de débat sur les nouveaux enjeux du développement des industries électriques, électroniques et de communication et de la vie privée.

- Après plusieurs mois d'enquête menée par la CNIL sur les nouvelles règles de confidentialité de Google entrées en vigueur le 1er mars dernier, les autorités de protection des données européennes publient leurs conclusions communes.

- Après consultation des acteurs concernés, l'autorisation unique n° AU-007 est modifiée et ne porte plus sur les contrôles d'horaires des salariés.

Novembre 2012

- Chercheurs, universitaires, professionnels du droit et représentants d'associations se réunissent le 30 novembre à l'occasion de la première journée d'études organisée par la CNIL. Publication du premier numéro des cahiers innovation & prospective. Ce numéro est consacré à la synthèse d'une réflexion prospective sur les enjeux de la vie privée, les libertés et les données.

- La CNIL et l'Institut Mines-Télécom partenaires pour sensibiliser la communauté scientifique à la protection des données.

Décembre 2012

- Publication des photos sur Internet : comment partager sans se sur-exposer ? La CNIL a demandé à TNS Sofres de mener une étude auprès des internautes afin de comprendre quelle place occupent aujourd'hui les photos dans la vie numérique.

Janvier 2013

- La CNIL salue le projet de rapport de M. Albrecht, rapporteur à la Commission Libertés civiles, justice et affaires intérieures du Parlement européen, publié le 8 janvier 2013, qui répond en grande partie à ses préoccupations sur le projet de règlement européen de protection des données personnelles.

- Compteurs communicants : premières recommandations de la CNIL

- Publication d'une série de fiches pratiques destinées à accompagner les salariés et les employeurs dans leur gestion des données personnelles au travail.

Février 2013

- A l'occasion de l'édition 2013 du *Safer Internet Day*, la CNIL et l'UNAF mettent en ligne un guide pour les parents pour un usage responsable d'Internet,

- Règles de confidentialité de Google : vers une action répressive et coordonnée des autorités européennes

- Le séminaire gouvernemental sur le numérique prévoir un renforcement des droits des citoyens et du rôle de la CNIL.

Mars 2013

- Open Data : la CNIL souhaite accompagner les acteurs publics et privés et lance une consultation des acteurs publics et privés concernés.

Avril 2013

La CNIL et Inria présentent l'expérience *Mobilitics*, un voyage au cœur des smartphones et des applications mobiles.

Bilan 2012 : une activité en hausse et un pilotage de la conformité au cœur du métier de la CNIL

L'année 2012 a une fois encore montré une activité en forte croissance avec plus de 2000 décisions adoptées, 6000 plaintes enregistrées, 458 contrôles réalisés (+19% par rapport à 2010), 3682 demandes de droit d'accès indirect (+75% par rapport à 2011) dont 1800 portant sur l'accès au fichier FICOBA (fichier des comptes bancaires). Au-delà de ces chiffres, cette année se caractérise par de nombreuses initiatives de la CNIL pour accompagner les acteurs dans leur démarche de conformité.

_____

1. Une préoccupation constante des citoyens

Le chiffre de 6017 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 (44% des plaintes ont été reçues via cnil.fr en 2012).

L'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de plaintes (46% des plaintes reçues).

Au-delà de ce volume important, l'année 2012 a confirmé la tendance observée en 2011 quant à au nombre important de plaintes relatives à internet/télécom (31 % des plaintes reçues) et plus particulièrement aux **problématiques de « droit à l'oubli numérique »**. La CNIL a reçu 1 050 plaintes qui portent sur la suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne, etc.

Les autres motifs de plaintes sont les suivants :

- **Commerce** (21% des plaintes reçues) : radiation de fichiers publicitaires, conservation coordonnées bancaires, fichiers clients ;

- **Gestion des ressources humaines** (15% des plaintes reçues) : vidéosurveillance, géolocalisation, accès au dossier professionnel ;

- **Banque** (10% des plaintes reçues) : inscription au FICP (fichier national des incidents de remboursement des crédits aux particuliers, FCC (fichier central des chèques et des retraits de cartes bancaires).

- **Libertés publiques et collectivités** (8% des plaintes reçues) **avec une augmentation significative de ces plaintes liée aux opérations électorales** : élections présidentielles et législatives, presse en ligne, diffusion par les collectivités locales de documents publics sur internet.

2. Les demandes d'accès au fichier FICOBA en forte augmentation

En 2012, la CNIL a reçu 1829 demandes d'accès au fichier FICOBA.

Pourquoi cette augmentation des demandes ?
L'augmentation importante du nombre de demandes de droit d'accès indirect au fichier FICOBA dont la CNIL est désormais destinataire, 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.
Les attentes en ce domaine sont amplifiées par le fait que les notaires ne se sont pas vus reconnaître, à la différence d'autres professions (ex : huissiers de justice munis d'un titre exécutoire), le statut de « tiers légalement autorisé » à accéder aux données de ce fichier directement auprès de l'administration fiscale.

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 (moyenne de 250/300 par mois), 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.

Comment améliorer la situation ?
Cette situation n'est pas satisfaisante, notamment pour les demandeurs. C'est pourquoi différentes pistes de réflexion sont à l'étude, y compris au sein de l'administration fiscale, pour améliorer le dispositif.

3. Un accompagnement des acteurs dans leur démarche de conformité

Dans un contexte d'évolutions technologiques et économiques extrêmement rapides, les organismes souhaitent s'assurer de la conformité permanente de leurs traitements aux exigences légales et aux bonnes pratiques.

De nouveaux outils pratiques et pédagogiques

La CNIL s'est donc engagée dans la mise en œuvre de véritables outils d'accompagnement des acteurs publics ou privés dans cette dynamique de mise en conformité. Elle a élaboré de nouveaux outils tels que :

- **5 fiches pratiques sur les données personnelles au travail**, mises en ligne en janvier 2013, qui ont fait l'objet de plus de 30 000 téléchargements ;
- **le guide de la sécurité informatique** comprenant une méthode et un catalogue de mesures pour aider les organismes à gérer les risques sur la vie privée. Ces outils opérationnels doivent faciliter l'intégration de la protection de la vie privée grâce à une approche pragmatique et rationnelle. Une version anglaise est également disponible. Ces guides ont été téléchargés 8000 fois.
- un « **pack de conformité** » spécialement conçu pour les acteurs du logement social et après les avoir consultés sera très prochainement disponible.

Les labels

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.

Pour obtenir un label CNIL, les entreprises doivent :

- Se conformer aux exigences d'un référentiel établi par la CNIL.
- Justifier la conformité de la procédure ou du produit labellisé à travers un dossier de candidature
- Fournir les éléments de justification (référentiel d'audit, procédures internes, contrats types...).

A ce jour, deux labels CNIL ont été créés à la demande d'organisations professionnelles : le label « formations » et le label « audit de traitement ».
La CNIL a délivré ses premiers labels en juin 2012. Depuis, ce sont 16 labels qui ont été délivrés. 11 pour les formations et 5 pour les audits de traitement.

Les correspondants « informatique et libertés »

Chaque année, le CIL s'affirme un peu plus comme un acteur central de la mise en conformité. En 2012, la barre des 10 000 organismes ayant désigné un CIL a été franchie. Aujourd'hui, on compte plus de 11 000 organismes dotés d'un CIL et 3 700 correspondants.

Consacré par le projet de Règlement européen, le CIL devient un pilier de la conformité à la protection des données dans les organismes.
Alors que la désignation d'un CIL est actuellement optionnelle et constitue encore un élément accessoire des actions de mise en conformité, le futur délégué à la protection des données sera au cœur du modèle proposé par le projet de Règlement européen.
En effet, bientôt obligatoire pour certains organismes, le futur délégué veillera à instaurer des procédures pour s'assurer de l'effectivité de la conformité à la protection des données personnelles de la structure qui l'aura désigné.

La CNIL aux côtés des acteurs publics

La numérisation croissante et la dématérialisation des données concernent de plus en plus le secteur public, et participent souvent de l'amélioration du service public. La CNIL encadre l'action publique et accompagne les acteurs en mettant à leur disposition des outils pratiques de mise en conformité, en faisant la promotion des correspondants et en mettant en place des partenariats.

_____

Une action en amont

La CNIL intervient en amont de la mise en place de traitements de données à caractère personnel par le biais des autorisations, des demandes d'avis ou encore des demandes de conseil. Elle peut aussi définir un cadre commun d'exigences à remplir pour la mise en œuvre de services.
Par ailleurs, la CNIL met à disposition des parlementaires son expertise juridique et technique et propose des actions d'information ou de sensibilisation. En 2012, elle a participé à plus d'une vingtaine de rendez-vous et d'événements avec des parlementaires (auditions, rendez-vous de travail).

A titre d'exemple, la CNIL a ainsi, en 2012, fixé le cadre de la mise en ligne des **archives publiques** (autorisation unique) après une concertation approfondie avec les services publics compétents.

Le secteur public représente une part importante de l'activité de la CNIL :

86 % des demandes d'avis reçues par la CNIL concernent le secteur public
22% des demandes d'autorisation reçues par la CNIL concernent le secteur public
28% des demandes de conseil reçues par la CNIL concernent le secteur public

Un accompagnement permanent : la mise en place d'outils pratiques

Plusieurs outils pratiques ont été développés pour accompagner les collectivités ou entreprises publiques dans leur démarche de mise en conformité. En 2012, la CNIL a tout particulièrement fait porter son action sur la vidéoprotection avec l'élaboration :

- **d'un vadémécum avec l'AMF** (Association des Maires de France) rappelant aux collectivités locales les 10 points pour assurer la sécurité collective dans le respect des libertés individuelles ;
- **de 6 fiches pratiques thématiques sur la vidéoprotection** / vidéosurveillance téléchargeables gratuitement depuis son site. Ces fiches ont été mises en ligne en juin 2012, et ont d'ores et déjà été téléchargées plus de 40 000 fois sur notre site.

En 2013, la CNIL a également conclu une convention avec la SNCF sur la vidéoprotection dans les gares.

Promotion et accompagnement des CIL (correspondants informatique et libertés)

Les « correspondants informatique et libertés » sont de véritables acteurs de la mise en conformité. La CNIL promeut donc leur désignation au sein des organismes publics. Ainsi :

- 1599 organismes du secteur public sont dotés d'un CIL et bénéficient de conseils au quotidien de la part de la CNIL ;

- Le **nombre de CIL dans les collectivités locales a presque doublé entre 2011 et 2012**. Ils sont passés de 244 CIL en 2011 à 486 en 2012.
- le Centre National de la Fonction Publique Territoriale (CNFPT) a inscrit le CIL au sein du Répertoire des Métiers Territoriaux qui regroupe les métiers de la fonction publique territoriale ;
- la CNIL mène une collaboration étroite avec les réseaux de CIL du secteur public (SUPCIL réseau des CIL de l'enseignement supérieur – APRONET réseau des CIL de la fonction publique territoriale).

Partenariats et convention

La mise en place des partenariats permet de diffuser la culture informatique et libertés, organiser des actions de sensibilisation et de formation sur la protection des données et mettre en œuvre des actions de conformité par secteur.

Les principales conventions **signées ou en cours en 2012** avec le secteur public sont les suivantes :

- Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) – (transmission de signalements, actions de formation, actions de communications communes) ;
- Association des Maires de France (volet vidéoprotection) ;
- Conférence des Présidents d'Université (CPU) ;
- Conférence de Grandes Ecoles (CGE) ;
- Institut national de recherche en informatique et automatique (INRIA);
- Institut Mines télécom ;
- DGCCRF (transmission de signalements, actions de formation, actions de communications communes).
-

Contrôles

La réalisation de vérifications sur place est un vecteur important de mise en conformité. **93** contrôles ont été réalisés dans le secteur public**. 57** pour la loi "informatique et libertés" (contre 228 dans le secteur privé) et **36** pour les contrôles vidéoprotection (contre 137 dans le privé).

Les contrôles emblématiques dans le secteur public en 2012 :

- les fichiers d'antécédents judiciaires (STIC –JUDEX) ;
- les données de santé (les groupes hospitaliers d'importance nationale) ;
- la délivrance des visas (contrôle dans des consulats sur les conditions de recueil et de traitement des données biométriques) ;
- les fichiers « sociaux » détenus par les collectivités locales et les CCAS.

A titre d'exemple, un contrôle a été réalisé dans un établissement hospitalier où une faille de sécurité avait été relevée. A la suite de ce contrôle, le groupe hospitalier auquel cet établissement appartient a revu ses mesures de sécurité, rappelé à l'ensemble des praticiens et des cadres les principes « informatique et libertés », et leur demandé de recenser les traitements « locaux » mis en œuvre.

Accompagner l'innovation : une activité centrale pour la CNIL

Nous assistons depuis plusieurs années à un véritable changement d'ère du fait du numérique. Avec la dématérialisation croissante des industries et des services, nous sommes passés d'un monde de fichiers à un univers de données dans lequel le numérique est devenu ambiant. Face à ce nouvel écosystème, la CNIL renforce sa capacité d'écoute et de dialogue avec de très nombreux acteurs pour mieux anticiper les évolutions technologiques et accompagner les usages innovants le plus en amont possible.

_____

Une organisation adaptée

Afin d'accompagner l'innovation, la CNIL a structuré son organisation interne.
En effet, la CNIL dispose aujourd'hui **d'une équipe de 10 experts informatiques**, ce qui lui confère une solide capacité d'analyse des technologies numériques. C'est à ce titre qu'elle a été mandatée pas ses homologues européens pour mener l'audit portant sur les règles de confidentialité de Google. Elle est donc parfaitement en capacité de discuter avec les grands acteurs de l'internet. Par ailleurs, elle participe activement aux travaux européens menés par le G29 sur les puces RFID, la publicité comportementale, les technologies sans contact, les objets communicants et elle pilote les travaux de normalisation (ISO/IEC 27001).

Une direction des études, de l'innovation et de la prospective a été créée en 2011. Elle fait appel à **un comité de la prospective** comprenant 6 personnalités extérieures. Ce comité joue un rôle de conseil dans le choix des études qui sont menées par la CNIL. Il constitue aussi un espace d'échanges et de réflexion sur les enjeux « informatique et libertés ». Il a par exemple participé à la préparation et l'animation de la journée d'études « vie privée 2020 » organisée en novembre 2012 et à la publication du premier Cahier IP.

Un laboratoire d'innovation a été créé en 2011. Il permet à la CNIL de disposer, en son sein, de moyens informatiques dédiés pour tester et expérimenter, en réel, des produits et applications innovants. Le laboratoire porte également des projets d'analyse, d'expérimentation et de « Recherche & Développement ». C'est le cas par exemple du projet *Mobilitics*, en partenariat avec Inria qui a permis d'analyser *in vivo*, pendant 3 mois, tous les échanges de données entre des smartphones et des applications mobiles. Ce projet a été présenté en avril 2013.

Afin de développer sa coopération avec le monde académique, la CNIL a signé **des conventions de partenariat avec le monde de la recherche** (Institut Mines-Télécom, Inria). Elle participe par ailleurs au projet Mes Infos mené par la FING.

Une doctrine pragmatique et évolutive grâce à un dialogue avec les acteurs

La CNIL cherche à confronter sa doctrine à la réalité des acteurs. C'est pourquoi elle a engagé avec eux une démarche d'ouverture pour s'assurer que ses positions correspondent à leurs attentes et sont suffisamment opérationnelles. Cette démarche est mise en œuvre systématiquement avant l'élaboration de nouvelles recommandations ou à l'occasion de la révision de normes existantes qui ne sont plus adaptées à la réalité des pratiques.

Par exemple, la CNIL a :

- lancé une consultation publique sur le ***cloud computing***, avant de proposer des recommandations pratiques permettant aux entreprises de fixer les conditions

optimales de protection des données personnelles qu'elles souhaitent voir héberger ;

- modifié **l'autorisation unique sur les dispositifs biométriques** après avoir consulté les principaux acteurs du secteur, notamment les organisations syndicales et patronales, ce qui a abouti au retrait du contrôle des horaires des salariés du champ de cette autorisation ;
- consulté les professionnels afin d'élaborer des **premières recommandations relatives aux compteurs communicants**. La CNIL participe à un groupe de travail au sein de la FIECC ;

La CNIL à l'initiative du débat public

Aujourd'hui, les données personnelles sont au cœur des questions économiques et sociétales. Des sujets tels que le big data, l'open data ou le droit à l'oubli suscitent de nombreuses questions. La CNIL, en tant que régulateur des données personnelles, est tout à fait légitime pour jouer un rôle de « catalyseur » du débat public. Elle a organisé en mars 2012 le premier PrivacyCamp à la Cantine, en association avec des acteurs du numérique (Mozilla, Owni, Silicon Sentier). Elle a réuni 160 personnes à l'occasion de la journée d'études « vie privée 2020 » en novembre 2012. Elle va lancer une consultation publique sur le droit à l'oubli. Enfin, elle souhaite organiser prochainement un débat public sur l'ensemble de ces sujets afin d'orienter les choix individuels et collectifs.

Projet de règlement européen : un enjeu majeur pour la France

La protection de la vie privée et des données personnelles représente un enjeu majeur de politique publique en France et partout en Europe. L'essor du numérique et le contexte de globalisation rendent nécessaire la révision du cadre juridique européen existant. La directive européenne de 1995 est ainsi appelée à être remplacée par un règlement européen d'application directe dans l'ensemble des États membres de l'Union européenne. Il devrait notamment permettre une meilleure harmonisation et renforcer l'effectivité des règles de protection des données personnelles. Le texte définitif devrait être adopté fin 2013 et entrer en vigueur deux ans plus tard. Ce moment est historique et il faut en prendre la pleine mesure car il dessinera le nouveau paysage de la protection des données du XXIème siècle en Europe.

La Commission européenne a rendu public, le 25 janvier 2012, un projet de règlement relatif à la protection des données personnelles. Le texte est actuellement en cours de discussion au Parlement européen, où il fait l'objet d'amples débats (le pré-rapport présenté en janvier 2013 par M. Albrecht, rapporteur à la Commission Libertés civiles, justice et affaires intérieures du Parlement européen, a ainsi fait l'objet de plusieurs milliers de propositions d'amendements). La Commission européenne a prévu une adoption fin 2013.

Ce projet a pour double objectif de renforcer les droits des citoyens et de moderniser le cadre existant pour tenir compte des nouveaux défis liés au développement des nouvelles technologies et à la mondialisation.

La CNIL souscrit aux objectifs poursuivis par cette réforme, notamment quant au renforcement du consentement des personnes dont les données sont traitées, la reconnaissance d'un droit à la « portabilité » des données, mais aussi la simplification des démarches administratives pour les entreprises. Plus généralement, elle partage la volonté de développer la responsabilisation des entreprises selon un processus de mise en conformité permanent.

Le projet de texte soulève cependant de sérieuses interrogations quant à l'effectivité de la protection des droits des personnes.

Le projet prévoit ainsi de donner une **compétence** exclusive à la « CNIL » du pays de l'établissement principal de l'entreprise responsable du traitement pour prendre l'ensemble des décisions applicables (y compris les contrôles et sanctions éventuelles). Un tel mécanisme aurait pour conséquence d'obliger les citoyens à faire valoir leurs droits dans un pays autre que celui de leur résidence, celui de l'établissement principal, leur CNIL nationale devenant une simple « boîte aux lettres ». De plus, les entreprises seraient incitées à choisir leur lieu d'établissement principal en fonction des contraintes locales, encourageant les risques de concurrence intra-communautaire en la matière. La CNIL a donc, depuis un an, proposé un mode de gouvernance à la fois intégré et décentralisé : intégré, parce que les autorités de contrôle doivent pouvoir prendre conjointement des décisions à l'égard des traitements transnationaux ; décentralisée, parce que chaque CNIL doit rester compétente pour les résidents de son territoire.

Le débat porte également sur les conditions dans lesquelles peuvent intervenir les **transferts de données hors UE, certains préconisant que de tels transferts puissent avoir lieu sur la base d'une simple « autoévaluation » de la part du responsable de traitement. Un tel mécanisme affaiblirait considérablement le niveau de protection des citoyens européens. La CNIL préconise donc de maintenir un contrôle sur ces transferts, dans le cadre d'instruments juridiques pertinents.**

Enfin, la CNIL continue à promouvoir l'introduction dans le règlement d'un véritable **droit au déréférencement** de la part des moteurs de recherche. Le droit au déréférencement n'est, pour la personne qui remplit les conditions pour demander l'effacement de ses données personnelles, que le corollaire du droit d'effacement : il s'agit de pouvoir demander au moteur de recherche d'effacer totalement de ses résultats la donnée dont l'effacement a été obtenu, ainsi que ses répliques.

Dans ce contexte, la CNIL invite l'ensemble des pouvoirs publics nationaux à se mobiliser et à promouvoir une vision humaniste de la protection des données personnelles, qui définisse un juste équilibre entre droits fondamentaux et innovation technologique.

L'éducation au numérique : un chantier prioritaire

La CNIL s'est engagée depuis plusieurs années dans de nombreuses actions pédagogiques pour sensibiliser les jeunes, les enseignants et les chefs d'établissements aux nouveaux usages numériques. Elle souhaite aujourd'hui contribuer plus fortement à l'éducation au numérique, en concertation avec les acteurs concernés.

_____

48 % des 8-17 ans sont connectés à Facebook et 18 % des moins de 13 ans y ont leur propre compte.*
90 % des 15-17 ans possédant un smartphone l'utilisent pour prendre des photos ou des vidéos.**
Si l'usage de ces outils se généralise, leur appropriation implique une prise de conscience individuelle et collective sur les enjeux, les risques et les bonnes pratiques en la matière. Soucieuse d'informer et de sensibiliser les citoyens, notamment les plus jeunes, sur la protection des données personnelles et de la vie privée, la CNIL a mené, depuis plusieurs années, de nombreuses actions pédagogiques.

Elle a ainsi créé un site dédié, www.jeunes.cnil.fr, sur lequel les internautes peuvent trouver des vidéos, comme la vidéo interactive "Share the party", les éditions spéciales de Mon Quotidien et l'Actu, le quiz des Incollables sur la protection des données personnelles, etc… Le même site comprend également un espace "parents", avec des tutoriels vidéo sur "Comment créer des listes d'amis sur Facebook ?" et "Sécuriser son smartphone". Enfin, une vingtaine de fiches pédagogiques sont disponibles dans l'espace "enseignants". Un serious game sur les réseaux sociaux et les traces a été réalisé en partenariat avec Internet sans crainte.

Par ailleurs, la CNIL délivre un label pour les "formations informatique et libertés". Dans le cadre de la francophonie, elle accompagne la mise en place de nouvelles autorités de protection des données grâce à des actions de formation.

Aujourd'hui, la CNIL souhaite renforcer son action avec l'élaboration de nouveaux outils et l'élargissement de leur diffusion. Cette action a vocation à s'articuler avec celle des autres acteurs concernés, publics comme le ministère de l'éducation nationale, pour la mise en place d'une véritable éducation au numérique et aussi privés.

La CNIL a ainsi mis en place un poste de responsable de l'éducation au numérique. Depuis, différentes initiatives ont été engagées à destination notamment des formateurs (association CLCV, chambres de commerce et d'industries, UFC Que Choisir). Enfin, la CNIL souhaite fédérer les acteurs publics et privés intéressés autour de l'objectif de la reconnaissance de l'éducation au numérique comme « grande cause nationale » pour 2014.

***Etude réalisée par TNS Sofres pour l'UNAF, la CNIL et Action innocence du 10 au 17 juin 2011 par téléphone, auprès d'un échantillon national représentatif de 1200 enfants et adolescents, âgés de 8 à 17 ans.*
***Enquête en ligne réalisée par Médiamétrie du 4 au 14 novembre 2011 auprès de 2315 utilisateurs de smartphones âgés de 15 ans et plus.*

La notification des violations de données personnelles : une nouvelle mission

A l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées. Cette obligation a été transposée en droit français à l'article 34 bis de la loi « Informatique et Libertés » par l'ordonnance du 24 août 2011. Le législateur a donc confié la CNIL d'une nouvelle mission. Elle accompagnera ainsi les fournisseurs de services de communications électroniques dans la mise en œuvre de mesures de protection efficaces contre toute violation de données. Elle peut enfin, en fonction de la gravité de cette violation, imposer aux fournisseurs l'information des personnes concernées.

_____

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, l'obligation de notification des violations s'impose uniquement aux fournisseurs de services de communications électroniques devant être déclarés auprès de l'ARCEP (fournisseurs d'accès à internet, de téléphonie fixe ou mobile), et lorsque la violation intervient dans le cadre de leur activité de fourniture de services de communications électroniques. A titre d'illustration, l'intrusion dans la base clients d'un FAI devra être considérée comme une violation de données soumise à notification, mais pas le piratage du fichier des ressources humaines de ce même FAI.

Dès qu'il constate une violation de données, le responsable de traitement doit sans délai en informer la CNIL. Il doit également informer les personnes dont les données ont fait l'objet de la violation, sauf s'il a mis en œuvre en amont des mesures techniques qui rendent les données incompréhensibles à toute personne non autorisée à y avoir accès. La CNIL peut cependant, si elle estime que la gravité de la violation le justifie, mettre en demeure le fournisseur d'informer les intéressés.

Le défaut de notification à la CNIL et aux personnes concernées est sanctionné à l'article 226-17-1 du Code pénal (cinq ans d'emprisonnement et 300 000 € d'amende).

Le projet de règlement européen relatif à la protection des données prévoit, à ce stade, la généralisation de cette obligation de notification à l'ensemble des responsables de traitement. Actuellement, les responsables de traitement qui n'entrent pas dans le champ de l'article 34 bis de la loi « Informatique et Libertés » sont cependant soumis à une obligation générale de sécurité et de confidentialité des données (article 34).

L'action de la CNIL

A ce jour, la CNIL a reçu **18 notifications de violation de données personnelles**. Ce faible nombre de notifications s'explique par le fait que les modalités de mise en œuvre de cette nouvelle obligation n'ont été que récemment fixées. En effet, au niveau national, un décret d'application a été publié en mars 2012. Un règlement européen visant à harmoniser les procédures de notification des violations aux autorités de protection des données personnelles est sur le point d'être adopté. Il définit notamment le contenu et les délais de notification aux autorités de protection des données et impose à ces dernières de mettre à disposition des déclarants un moyen électronique sécurisé de notification.

Dans les années à venir, cette nouvelle mission aura des conséquences sensibles sur l'activité de la CNIL qui devra non seulement traiter les notifications des fournisseurs de services de communications électroniques, mais également accompagner ces derniers dans l'appréciation de la gravité des failles et la mise en œuvre de mesures de protection efficaces. A cet égard, la CNIL participe aux travaux menés par le G29 pour aider les responsables de traitement à évaluer le niveau de gravité des violations subies.

De manière plus générale, ces nouvelles obligations s'inscrivent dans un processus de responsabilisation accrue des acteurs en charge des données personnelles. Elles permettront à la CNIL d'avoir une meilleure vision du niveau de sécurité mis en œuvre et d'offrir ainsi un meilleur accompagnement des entreprises et une meilleure protection des personnes.

Avant-propos d'Isabelle Falque-Pierrotin
Rapport d'activité 2012

Une année pleine d'audace

Interrogée à mi-année sur le mot qui décrivait le mieux l'état d'esprit qui devait guider la CNIL en 2012, j'avais parlé d'audace. C'est cette audace qui devait nous permettre d'innover, de repenser la régulation, de renouveler notre action et nos outils pour faire face aux différentes mutations structurelles liées au développement du numérique.

Pour réaliser cet objectif, un plan stratégique triennal a été adopté en juillet 2012. Il inscrit l'action quotidienne de notre institution autour de trois directions : celle de l'ouverture et de la concertation avec les acteurs car le régulateur ne peut plus travailler et réfléchir seul ; celle de la conformité à travers laquelle nous responsabilisons ceux qui traitent des données personnelles et, en particulier les entreprises et construisons avec eux des outils concrets de mise en œuvre des principes informatiques et libertés ; celle enfin du respect de la régulation via une politique répressive plus ciblée et plus efficiente. Ce dessein représente un effort considérable pour notre institution. Grâce au travail des équipes et des membres de la CNIL, il est en train d'être mis en œuvre et nous sommes en chemin vers cette nouvelle CNIL ; une e-cnil, plus réactive, plus agile, plus ancrée dans le réel. Il est rendu d'autant plus complexe qu'il s'inscrit dans un environnement qui, en ce début d'année 2013, est marqué par de fortes tensions.

Pour commencer, évoquons la compétition économique croissante autour des données personnelles.
Ce constat dépasse le cadre d'internet puisque le numérique est présent dans tous les secteurs économiques traditionnels et constitue le socle des innovations et des services de demain dans la banque, l'assurance, l'énergie, l'automobile, la santé, etc.
Les formules utilisées pour illustrer la richesse et le caractère central des données personnelles dans l'économie ont fleuri dans les médias : « pétrole du numérique », « matière première », « ruée vers l'or », « eldorado », etc.

Cette ressource est un peu particulière car elle est, pour partie, produite par les individus eux-mêmes.
On aurait donc tort d'ignorer ou de minorer cette dimension humaine. L'économie se construit désormais à partir de l'individu ; c'est de plus en plus lui qui est le produit, la ressource-clé. Or, le citoyen/consommateur numérique a mûri. S'il veut profiter pleinement des services qui sont à sa disposition, il demande en contrepartie des garanties par rapport à ses données personnelles car il s'inquiète de plus en plus par-rapport à l'utilisation de celles-ci (79% des Français se disent inquiets de l'utilisation qui peut être faite de leurs données personnelles à des fins de marketing direct ou de publicité en ligne). Il veut donc avoir une vie en ligne mais aussi plus de transparence et plus de maîtrise sur ses données. On a vu la confusion et la méfiance suscitées par le « bug Facebook » en septembre 2012. Faux bug informatique mais vrai bug psychologique ! Quelques semaines plus tard, c'est Instagram qui a dû faire machine arrière après le tollé provoqué par l'annonce de ses nouvelles conditions générales qui le rendait propriétaire des photos de ses clients.

Les acteurs économiques doivent réaliser qu'en procédant à marche forcée, ils installent un inconfort, un déficit de sécurité dans l'esprit de leurs clients qui peuvent se retourner contre eux de façon brutale. L'innovation impose souvent la rupture, ou au moins de rompre avec des règles établies. Mais un modèle économique fondé sur l'innovation doit reposer sur la confiance et la transparence. Lorsque la confiance est rompue, le modèle économique se fragilise. On le voit, la protection des données personnelles est en train de rentrer dans le débat concurrentiel ; loin d'être un frein, la protection des données peut aujourd'hui être considérée et présentée comme un atout commercial. Opposer l'innovation et la protection des données est dès lors une vue simpliste et à très court terme qui ne reflète pas la complexité de l'écosystème numérique et les attentes du consommateur.

Au même moment, une autre bataille a lieu sur le terrain géostratégique.
A Bruxelles, les différents blocs géographiques se font face et s'affrontent pour élaborer le cadre juridique européen de la protection des données du XXIème siècle. S'il en était besoin, l'importance des enjeux stratégiques peut se mesurer aux 3000 amendements déposés sur le projet de règlement. De même, par le déploiement d'une armée de lobbys qui, de mémoire de parlementaires européens, n'avait jamais envahie Bruxelles à ce point. Pour l'Europe, le moment est en effet historique et le défi est grand. Elle doit moderniser son modèle et le rendre compétitif, par-rapport aux initiatives étrangères comparables, tout en réaffirmant la protection des données personnelles en tant que droit fondamental. Elle doit concilier croissance économique et libertés.
Dans cette bataille, la CNIL, aux côtés de ses homologues européens, ne ménage pas ses efforts. Elle a mobilisé les parlementaires, le gouvernement, ses homologues pour expliquer, convaincre et proposer des alternatives allant dans le sens d'une gouvernance européenne décentralisée reposant sur des autorités puissantes évoluant à armes égales et coopérant fortement entre elles. L'année 2013 sera déterminante car le texte européen pourrait être adopté tout comme les cadres du Conseil de l'Europe, de l'OCDE et de l'APEC.

Au-delà de ces affrontements, des questions fondamentales se posent et la CNIL souhaite lancer le débat.
Depuis quelques semaines en effet se multiplient dans les journaux français et internationaux des analyses sur le rôle croissant des données dans le développement de l'économie numérique et notamment du Big data et, face à ces belles promesses économiques, le débat public se noue sur le meilleur cadre de régulation souhaitable, le plus à même d'assurer le développement de celles-ci.
Pour certains, une régulation excessive des données personnelles handicaperait les acteurs français dans l'élaboration de nouveaux services alors même que nos concitoyens ne s'inquiètent pas outre mesure de la protection de leur vie privée. Nous devrions au contraire « libérer » les données, et ainsi favoriser la croissance.

D'autres estiment que l'encadrement des données est nécessaire mais que les institutions publiques ne peuvent plus être vraiment efficaces dans un univers aussi évolutif que le numérique. Aussi renvoient-ils vers l'individu tout le poids de la régulation : c'est à celui-ci de garder la maitrise de ses données, de faire le choix de les échanger ou de les négocier. Aucun tabou collectif n'existerait ; seule la volonté individuelle primerait.

Ce débat sur la régulation, sa nécessité et son ancrage pertinent n'est pas nouveau concernant internet et le numérique. Nous en parlons depuis 10 ans ! Les données

personnelles succèdent ainsi à la protection de l'enfance ou à la propriété intellectuelle. Ces questions, quoique différentes peuvent nous aider à construire une action de régulation efficace et légitime en matière de protection des données personnelles.

D'abord, compte tenu du rôle central de l'utilisateur et de ses usages dans le numérique, il est naturel de rendre à l'individu la maitrise de ses données. La question est de savoir comment le faire effectivement et jusqu'où. Faut-il aller vers une privatisation des données, faisant de chacun d'entre nous un négociateur, propriétaire de son identité comme certains le proposent ou doit-on privilégier une approche plus collective ?

Par ailleurs, dès lors que nous faisons face à un déluge de données, répliquées de façon intensive, il faut réfléchir à leurs utilisations. Beaucoup d'entre elles ne posent aucun problème au régulateur. Mais certaines semblent revenir telles des boomerangs vers l'individu mettant en cause ses libertés. L'individu doit-il consentir et si oui, comment, à de nouvelles utilisations de ses données ? Mais comment lui faire consentir a priori a des usages futurs qu'il ne connait pas ?

Enfin, concernant l'Etat, il est clair que celui-ci a une action singulière à mener en termes de protection des données personnelles. Il doit veiller à ce que sa politique d'ouverture des données, parfaitement légitime, ne se retourne pas contre les citoyens en leur imposant une transparence excessive. Une réflexion spécifique doit donc être engagée sur l'articulation entre Open data et vie privée afin de construire une modernisation exemplaire, respectueuse des citoyens.

Nous avons besoin d'innover, de créer de nouveaux usages et services. Notre croissance et notre rayonnement international en dépendent. Fixer le cadre de cette innovation, les responsabilités respectives de l'Etat, des entreprises et des citoyens n'est pas superfétatoire. **En réalité, protection des données et innovation sont les deux faces d'une même médaille. L'une sans l'autre et nous risquons une crise de confiance généralisée.**
La CNIL, consciente de cette ambivalence, souhaite qu'un débat ouvert et constructif se mette en place afin de fixer les contours de nos choix individuels et collectifs. Elle a lancé celui-ci début 2013 et veut y associer l'ensemble des parties prenantes concernées.

La CNIL est donc en marche. Elle est déterminée à prendre le virage du numérique et à se positionner comme une autorité de régulation crédible.
Les mesures annoncées par le Premier ministre, à l'issue du séminaire gouvernemental sur le numérique le 28 février 2013, constituent par ailleurs une étape importante vers le renforcement des droits numériques de nos concitoyens. Elles confortent également le rôle de la CNIL en lui accordant une place et des pouvoirs plus importants.
L'ensemble de ces mesures, tout comme la constitutionnalisation de la protection des données personnelles que la CNIL appelle de ses vœux, contribueront ainsi à construire un environnement de confiance, élément indispensable pour accompagner le développement d'une innovation durable. Dans ce contexte de bouleversement permanent, la CNIL doit, plus que jamais, faire preuve d'inventivité, d'écoute, et surtout d'audace. **L'audace, c'est affirmer une identité forte, tout en évoluant et tenant compte de la complexité du monde** dans lequel ces initiatives s'inscrivent. Nous n'en manquons pas cette année comme dans les années à venir.

*Source : Commission européenne, Eurobaromètre *Attitudes on Data Protection and Electronic Identity in the European Union*, juin 2011.