

COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

31^e RAPPORT
D'ACTIVITÉ
2010



En application de la loi du 11 mars 1957 (article 41) et du Code de la propriété intellectuelle du 1^{er} juillet 1992, toute reproduction partielle ou totale à usage collectif de la présente publication est strictement interdite sans autorisation expresse de l'éditeur. Il est rappelé à cet égard que l'usage abusif et collectif de la photocopie met en danger l'équilibre économique des circuits du livre.

© Direction de l'information légale et administrative – Paris, 2011
ISBN: 978-2-11-008684-6

COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

31^e RAPPORT
D'ACTIVITÉ
2010



prévu par l'article 11 de la loi du 6 janvier 1978,
modifiée par la loi du 6 août 2004

Sommaire

AVANT-PROPOS	7
Les chiffres de l'année 2010	13
Protéger	14
Informers	16
Conseiller et proposer	18
Contrôler	20
Sanctionner	22
Anticiper	24
Simplifier et réglementer	25
LES TEMPS FORTS	27
Notre priorité : sensibiliser les jeunes et les professionnels de l'éducation aux bonnes pratiques sur internet afin de favoriser une instruction « civico-numérique »	31
La révision du cadre juridique européen : quel futur pour la vie privée ?	36
Les nouveaux pouvoirs de contrôle de la vidéoprotection	40
Prospective et innovation : une priorité stratégique pour la CNIL	43
ANNEXES	47
Les membres de la CNIL	49
Les services de la CNIL au 4 mai 2011	50
Les moyens de la CNIL	52
Liste des organismes contrôlés en 2010	54
Liste des sanctions prononcées en 2010	58

Avant-propos



À l'occasion de la publication du 31^e rapport annuel de notre commission, je relève tout d'abord deux éléments purement formels.

Le lecteur remarquera en effet, d'une part, que nous avons procédé à un « remaniement » de ce rapport de façon à faciliter davantage encore sa lecture. D'autre part, dans le souci de « coller à la réalité », nous avons fait en sorte que le rapport publié en 2011 couvre l'ensemble de la période écoulée depuis le rapport précédent plutôt que l'année civile 2010. Ceci nous évitera quelques contorsions et présentations parfois surréalistes lorsqu'il s'agissait, par exemple, de feindre d'ignorer, dans la relation des faits survenus fin 2009, leur conclusion survenue début 2010 !

Quant à l'exercice constitué par le présent éditorial, rien ne change ; il s'agit comme chaque fois de résumer, en quelques lignes, les milliers d'heures consacrées par les commissaires, et l'ensemble de l'équipe de la CNIL, à la protection des données de leurs concitoyens !

Mais puisqu'il faut choisir... Retenons une très vive préoccupation, une interrogation récurrente et une vraie belle satisfaction.

Comment, en effet, ne pas être préoccupé face au déferlement des nouvelles applications technologiques qui, peu à peu, installe dans ce que l'on appelle notre « société numérique », un appareil de traçage de l'ensemble des citoyens : maillage de fichiers « traditionnels », vidéoprotection (ou vidéosurveillance), biométrie, géolocalisation, usages d'internet ?

Comment ne pas s'interroger sur les conséquences à terme du fossé existant entre les conceptions européenne et américaine en matière de protection des données ? L'Europe aura-t-elle le courage politique de poser « les questions qui fâchent » quant à l'application sur son territoire – évidemment indispensable – du droit européen aux activités des sociétés américaines de l'internet ? Profitera-t-elle de la perspective d'une révision de fond de la directive européenne pour adapter nos législations aux défis qui nous attendent ?

Enfin, pourquoi ne pas se féliciter de l'adoption, récemment, de dispositions législatives qui donnent à notre Commission la possibilité (tant attendue) de pouvoir contrôler, sur l'ensemble du territoire, les dispositifs de vidéoprotection, quels que soient les régimes juridiques qui les régissent ? Il y a là une évolution majeure et, disons-le aussi, un hommage rendu par les pouvoirs publics à notre institution, à ses compétences et à sa réputation.

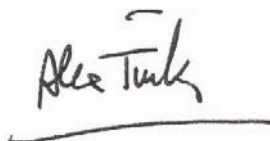
La mission première de notre Commission est de relever l'ensemble de ces défis. Elle en a la volonté et les capacités.

Que l'on me permette, pour conclure, un mot personnel.

Représentant élu du Sénat au sein de la CNIL depuis 1992, j'en assume la présidence, depuis mon élection par mes pairs, en février 2004. Mon mandat s'achèvera en septembre prochain et ne se renouvellera pas, conformément à la nouvelle législation.

Je voudrais exprimer ici mes remerciements les plus chaleureux à l'ensemble du personnel de la Commission ainsi qu'à mes collègues commissaires qui m'ont donné la chance de vivre à leurs côtés une expérience – une aventure – exaltante et passionnante au service de la protection de la vie privée et des libertés individuelles.

Je suis convaincu que notre Commission sera à la hauteur des attentes de nos concitoyens qui souhaitent pleinement profiter des avantages que procurent les technologies numériques dans le domaine de la connaissance, du dialogue entre les personnes et de l'accès à la démocratie, et en même temps être assurés que l'exercice de leurs libertés individuelles et de la protection de leur vie privée sont garantis.

A handwritten signature in black ink that reads "Alex Türk". The signature is written in a cursive style and is positioned above a horizontal line.

Alex TÜRK
Président de la Commission nationale
de l'informatique et des libertés

Le mot du secrétaire général



L'amélioration du service rendu à l'utilisateur : voici, à mon sens, la tendance la plus marquante de l'année 2010 pour notre Commission.

Grâce à la réduction des délais tout d'abord, puisque les récépissés délivrés aux organismes qui déclarent leurs fichiers à la CNIL le sont en 5 jours depuis le 1^{er} décembre 2010. Ils l'étaient en 13 mois en 2006. De même, les autorisations préalables délivrées par la CNIL aux entreprises qui souhaitent transférer des données hors de l'Union européenne, parce qu'elles externalisent certaines activités, le sont en 25 jours depuis le 1^{er} trimestre 2011. Elles l'étaient en 180 jours en 2009.

Cette performance résulte d'un triple phénomène. Juridique en premier lieu. La loi du 13 mai 2009 a délégué au président ou au vice-président la compétence pour autoriser ces transferts. Auparavant, ces derniers faisaient l'objet d'un vote à la majorité qualifiée en séance plénière de notre Commission. Ce nouveau système de délégation permet ainsi de traiter davantage de demandes, en un temps réduit. Tel était précisément l'objectif poursuivi par le législateur. En effet, plus le nombre des autorisations de transfert délivrées est élevé, plus leur délai moyen d'instruction par les services, mécaniquement, se réduit. Pour s'en convaincre, il suffit de rappeler que le nombre d'autorisations de transferts adoptées par la séance plénière de notre Commission en 2009, avant cette réforme législative, était de 80 en 2007, 215 en 2008 et 314 en 2009. Ce nombre a atteint 543 décisions déléguées en 2010.

Organisationnel en second lieu. La réduction importante des délais a été rendue possible grâce à une profonde réorganisation interne menée depuis 2007. Ainsi, un véritable *front office* a-t-il été mis en place au profit du service d'accueil et de renseignement du public, permettant de traiter, dès le premier appel, un grand nombre de demandes et toutes les déclarations.

Managérial enfin. Notre Commission a décidé de mettre en œuvre une prime de performance adossée, pour partie, à l'atteinte de résultats chiffrés, ce qui témoigne de la motivation des équipes et est, par ailleurs, suffisamment novateur dans l'administration pour devoir être souligné ici.

Au-delà de ces chiffres, la Commission a mis à la disposition des usagers des services variés leur permettant d'effectuer, depuis le 14 juin 2010, leurs formalités

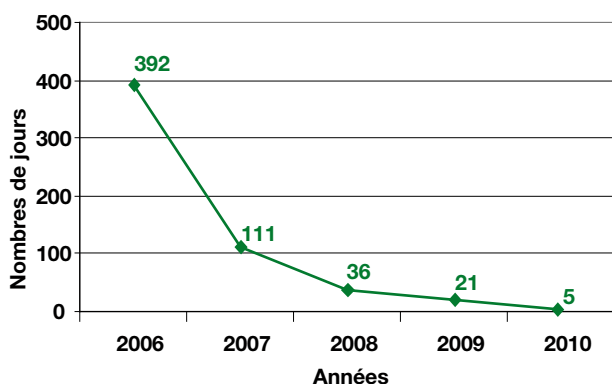
préalables (demandes d'avis et d'autorisation préalable pour les fichiers les plus sensibles, déclarations) ou encore de déposer une plainte directement en ligne. Aujourd'hui, près de 20% des plaintes sont ainsi adressées à la CNIL sous forme dématérialisée.

Ce bref panorama serait incomplet s'il n'était fait mention de la campagne de communication que la CNIL a engagée en direction des mineurs. Aujourd'hui, 70% des moins de 11 ans utilisent internet et 49% des 11-12 ans possèdent leur propre téléphone portable grâce auquel, pour la plupart, ils accèdent à internet et aux réseaux sociaux. La précocité de ces usages exige, en contrepartie, qu'une pédagogie adaptée soit engagée afin de promouvoir les bonnes pratiques et sensibiliser ces jeunes utilisateurs aux risques induits par un dévoilement excessif de soi sur les réseaux. C'est pourquoi la CNIL a entrepris un effort de sensibilisation sans précédent en leur direction en consacrant plus de 500 000 euros à une opération impliquant, notamment, la réalisation de deux éditions spéciales des journaux *Mon Quotidien* (pour les 10-14 ans) et *l'actu* (pour les 14-18 ans) consacrés à la question de la protection de la vie privée sur internet.

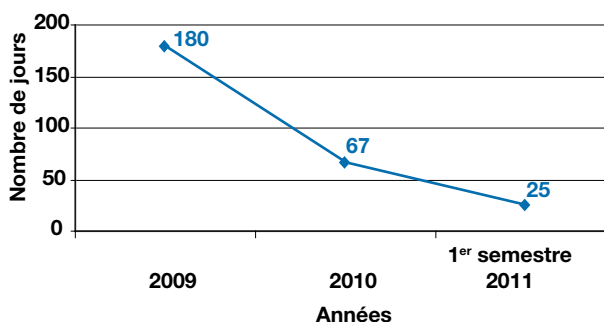
Puisque ce qui est sur le réseau un jour peut l'être pour toujours, parce que l'action réparatrice d'une plainte ou d'une sanction n'effacera jamais le dommage subi par l'intéressé, il importait à nos yeux de s'adresser directement, et dans un langage adapté, à ces jeunes utilisateurs. Ce faisant, il s'agit bien, comme le prévoit l'article 1^{er} de notre loi, de faire en sorte que l'informatique soit « au service de chaque citoyen », y compris ceux de demain.

Yann PADOVA

**Délais moyens de délivrance
des récépissés des déclarations normales**



**Délais moyens de traitement
d'une autorisation de transfert hors UE**



LA CNIL EN ACTION





LES CHIFFRES DE L'ANNÉE 2010

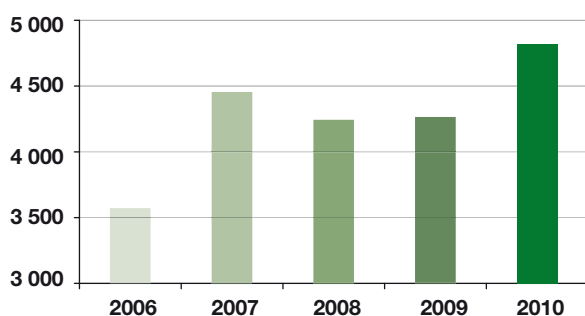
- **71 410** traitements de données personnelles enregistrés
- **68 262** récépissés envoyés par la CNIL
- **48 heures** de délais pour recevoir un récépissé pour une déclaration simplifiée et 5 jours pour une déclaration (contre 13 mois en 2006)
- **88 %** des déclarations sont faites en ligne
- Les membres de la CNIL se sont réunis **33** fois en séance plénière
- Les membres de la formation contentieuse se sont réunis **12** fois
- **2 905** transferts hors de l'Union européenne contre 2 860 en 2009
- **706** autorisations relatives à des systèmes biométriques et 3 refus
- **258** autorisations
- **8** avis sur des projets de loi ou de décret
- **78** avis portant notamment sur des traitements mis en œuvre pour le compte de l'État
- **4 376** déclarations relatives à des systèmes de vidéosurveillance
- **10 000** appels téléphoniques
- **28 490** courriers reçus
- **1 569** décisions et délibérations adoptées
- **4 821** plaintes
- **1 877** demandes de droit d'accès indirect aux fichiers de police et de renseignement
- **308** contrôles
- **111** mises en demeure
- **3** avertissements
- **5** sanctions financières
- **7 300** organismes ont désigné un correspondant
- **254** actualités mises en lignes sur www.cnil.fr
- **33 000** abonnés à la lettre InfoCNIL
- **600 000** exemplaires de l'édition spéciale de *Mon Quotidien* envoyés à toutes les classes de CM2
- **200 000** exemplaires de l'édition spéciale de *l'actu* envoyés dans les collèges
- **18** auditions devant le Parlement
- **11** délégations étrangères reçues

PROTÉGER

Nette hausse des plaintes reçues

En 2010, la CNIL a reçu un nombre record de plaintes (4 821) pour non-respect de la loi « Informatique et Libertés ». Ce chiffre représente une hausse de 13 % par rapport à 2009.

Évolution du nombre de plaintes reçues par la CNIL



Si tous les secteurs sont concernés par cette augmentation, les questions liées au « droit à l'oubli sur internet » (pour demander la suppression de contenus – textes, photographies, vidéos – qui apparaissent sur des sites ou des blogs) et à la vidéosurveillance sont en particulière progression. La CNIL continue également à recevoir un nombre important de plaintes concernant les secteurs de la banque et du crédit, du travail (notamment sur les questions de surveillance des salariés) et du commerce (gestion des fichiers de clients ou d'envoi de publicité).

Le lancement, en juin 2010, du service de « plainte en ligne » permet également d'expliquer ces chiffres. En effet, près de 20 % des plaignants utilisent aujourd'hui internet (www.cnil.fr) pour adresser une plainte à la CNIL ; ils n'étaient que 8 % à le faire en septembre 2010.

Comment la CNIL traite-t-elle les plaintes ?

Dans près de 20 % des cas, le service des plaintes est en mesure de répondre directement au plaignant (pour lui préciser ses droits et les démarches à accomplir auprès du responsable du fichier, pour lui indiquer – après analyse juridique – que le responsable du fichier n'est pas en faute ou encore que la CNIL n'est pas compétente sur la question posée).

Dans 80 % des cas, il y a en revanche nécessité d'intervenir auprès du responsable du fichier concerné par la plainte. Cette intervention, par un échange de courriers, est généralement suffisante pour obtenir ou s'assurer du respect de la loi « Informatique et Libertés ». Si nécessaire, la CNIL peut faire usage de ses pouvoirs de contrôle sur place (environ 2 % des dossiers, 19 % des contrôles ont été effectués dans le cadre de l'instruction de plaintes) et, dans les cas les plus graves, elle peut mettre en demeure le responsable du fichier de se conformer à la loi (également 2 % des dossiers).

Les délais d'instruction des plaintes varient de quelques jours à plusieurs mois en fonction de la complexité de la plainte, de la qualité des réponses apportées par le responsable du fichier ou encore des actions entreprises pour instruire le dossier (contrôle, mise en demeure, procédure de sanction...).

Le droit d'accès indirect aux fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique

En 2010, la CNIL a reçu **1 877** demandes de droit d'accès indirect. Le plus souvent, ces demandes sont engagées à la suite de décisions défavorables en matière d'accès à des emplois publics ou privés relevant du domaine de la sécurité ou de la défense. En effet, l'accès à ce type d'emplois donne lieu à des enquêtes administratives préalables à l'occasion desquelles les préfets consultent ces fichiers. Le STIC peut être consulté à l'occasion du recrutement, de l'agrément ou de l'habilitation des personnels de professions très diverses : personnels de surveillance et de gardiennage, personnes souhaitant travailler dans les zones aéroportuaires, agents de police municipale, gardes champêtres, préfets, ambassadeurs, directeurs et chefs de cabinets des préfets, magistrats, etc. **Au total, la consultation du STIC à des fins d'enquête administrative est susceptible de concerner plus d'un million d'emplois.**

Une demande d'accès indirect concerne généralement plusieurs fichiers. Par exemple pour les fichiers de police judiciaire, les magistrats de la CNIL effectuent des vérifica-

tions dans le fichier STIC, dans les fichiers de la sécurité publique des commissariats et dans le fichier JUDEX de la gendarmerie nationale. Les demandes ont donné lieu à **4 185** vérifications qui ont permis de clôturer **1 838** dossiers. **60% des vérifications effectuées en 2010 ont concerné les fichiers de police judiciaire**, avec les résultats suivants :

Fichiers de police judiciaire	STIC	JUDEX
Nombre de vérifications effectuées	1 155	1 372
Nombre de fiches « mis en cause » vérifiées	662	254
Fiches exactes	21 %	52 %
Fiches modifiées pour tenir compte, notamment, des suites judiciaires réservées aux infractions enregistrées	59 %	23 %
Fiches supprimées	20 %	25 %

Le nombre des demandes d'exercice du droit d'accès indirect adressées à la CNIL en 2010 permet de constater une baisse par rapport aux années antérieures. Une hausse sensible avait notamment été enregistrée au cours de l'année 2008, marquée par une augmentation significative du nombre de demandes. Cette hausse, qui s'est poursuivie de manière plus modérée en 2009, était essentiellement imputable au large débat et à la mobilisation suscités par

la création du fichier EDVIGE liée à la nouvelle architecture des services de renseignements du ministère de l'Intérieur. La CNIL avait alors reçu de nombreuses demandes d'accès aux fichiers de renseignement.

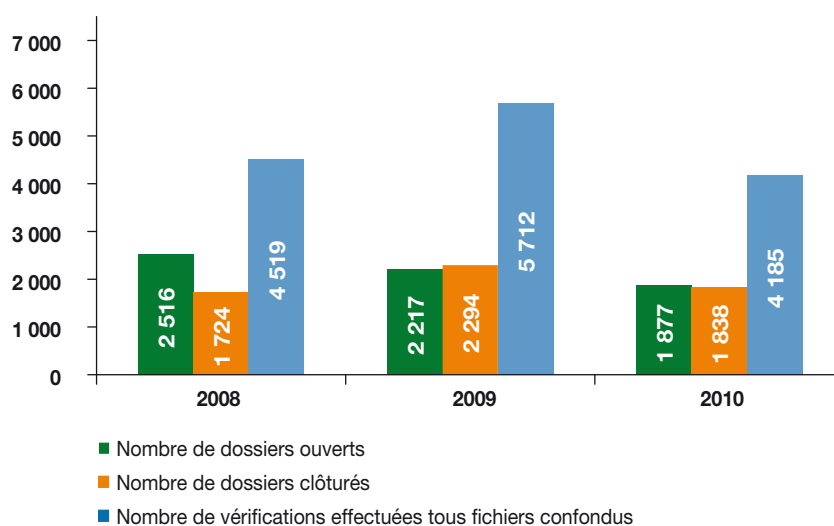
Comment ça marche ?

En application de l'article 41 de la loi « Informatique et Libertés », toute personne peut demander à la CNIL de vérifier les informations qui la concernent susceptibles de figurer dans les fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique.

Un magistrat de la CNIL appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes est alors désigné pour mener les investigations utiles dans les fichiers concernés et faire procéder aux modifications nécessaires.

Les principaux fichiers concernés par cette procédure sont les fichiers de police judiciaire de la police et de la gendarmerie nationales (STIC et JUDEX), les fichiers des services de renseignements ainsi que le système d'information Schengen (SIS).

Évolution des demandes de droit d'accès indirect depuis 2008



INFORMER

La CNIL vous informe au quotidien

Sensibiliser les collégiens, les enseignants et les chefs d'établissement aux bonnes pratiques sur internet: notre priorité

À la suite des actions menées en 2010, la CNIL a confirmé en 2011 son engagement pour promouvoir les bons usages chez les jeunes utilisateurs d'internet. Après les élèves et enseignants de primaire, elle s'est adressée avec des supports adaptés, aux collégiens, aux enseignants ainsi qu'aux chefs d'établissement du second degré. Toutes ces actions de sensibilisation sont développées au chapitre deux de ce rapport.

Partenariat France Info

Le partenariat débuté en 2007 a été renouvelé. Chaque vendredi, la CNIL intervient dans l'émission «Le droit d'info» présentée par Karine DUCHOCHOIS pour répondre à une question pratique en lien avec la protection de la vie privée. Ce partenariat contribue à mieux faire connaître les droits «Informatique et Libertés» et à dispenser des conseils pour une meilleure protection de sa vie privée au quotidien. Les 50 chroniques diffusées portaient sur des sujets tels que : l'e-réputation, les enquêtes INSEE, les coffres-forts électroniques, le cyber-harcèlement, le décrochage scolaire, etc.

Le Prix de thèse «Informatique et Libertés»

Le Prix de thèse «Informatique et Libertés» incite au développement des recherches universitaires concernant la protection de la vie privée et des données personnelles. Ce prix concerne aussi bien les sciences humaines, le droit, les sciences politiques, l'économie que les disciplines techniques. Un montant de 7 000 euros est alloué au lauréat, afin de faciliter la publication de sa thèse.

Le jury, présidé par Jean-Marie COTTERET, membre de la CNIL, professeur émérite des Universités, a décerné le Prix de thèse 2010 à monsieur Nicolas LECHOPIER pour sa thèse intitulée «Éthique dans la recherche et démarcation. La scientificité de l'épidémiologie à l'épreuve des normes de confidentialité», philosophie, Université Paris I, Panthéon-Sorbonne. L'ouvrage paraîtra en septembre aux éditions Michalon.

Le site internet www.cnil.fr

En 2010 et 2011, le site a augmenté de façon tout à fait significative le nombre d'actualités mises en ligne. Elles sont en effet passées de 73 en 2008 et 113 en 2009 à 254 en 2010. Cette accélération met en évidence une meilleure réactivité de la CNIL à l'actualité qui informe plus souvent et plus simplement les citoyens. Le service offert aux professionnels s'est aussi amélioré puisqu'il est possible désormais d'effectuer l'ensemble des formalités en ligne. Autre nouveauté, le service de plainte en ligne ouvert en juin 2010.

Les réseaux sociaux

L'année 2010 marque l'entrée de la CNIL sur les réseaux sociaux. Elle est présente sur Facebook, Twitter, Dailymotion et les réseaux professionnels Viadeo et LinkedIn.



L'image de la CNIL

Comme les années précédentes, une étude portant sur la perception et l'image de la CNIL a été menée en décembre 2010 par l'Ifop sur un échantillon de 1 000 personnes représentatives de la population française.

La notoriété de la CNIL

Question :

Connaissez-vous, ne serait-ce que de nom, la CNIL ?

	Juin 2004	Décembre 2010	Évolution 2004/2010
Oui	32	47	+ 15
Non	68	53	
	100%	100%	

Le niveau d'information sur les droits

Question :

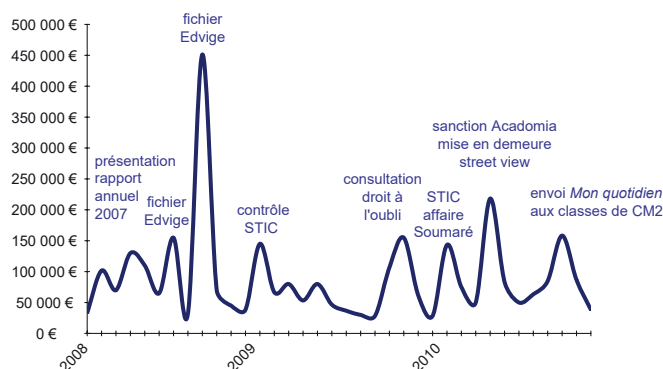
Vous-même, avez-vous le sentiment d'être suffisamment informé à propos de vos droits en matière de protection des données personnelles vous concernant ?

	2004	2010	Évolution 2004/2010
Oui, tout à fait	3	10	
Oui, plutôt	18	24	
Sous-total oui	21	34	+ 13
Non, plutôt pas	39	34	
Non, pas du tout	39	28	
Sous-total non	78	62	
Sans opinion	1	4	
	100%	100%	

On constate entre 2004 et 2010 une progression de la notoriété qui tend aujourd'hui à se stabiliser autour de 47%. La connaissance des droits est passée de 21% en 2004 à 34% en 2010. La présence hebdomadaire de la CNIL sur France Info, la reprise par les médias de sujets touchant le grand public (cours à domicile, collecte des adresses WiFi), ainsi que les nombreuses actions de sensibilisation des jeunes aux bons usages d'internet permettent d'expliquer ces taux de notoriété et de connaissance des droits.

Afin d'évaluer l'impact des retombées presse et notamment audiovisuelles, la CNIL dispose d'un outil mesurant l'équivalence publicitaire audiovisuelle. Celle-ci est calculée en fonction de deux critères : le coût moyen de la publicité (à la seconde) et la surface rédactionnelle (la durée de la séquence). En 2008, l'équivalence publicitaire de la présence de la CNIL dans la presse audiovisuelle représentait 1,3 millions d'euros, 889 000 euros en 2009 et 1,14 million d'euros en 2010.

Équivalence publicitaire audiovisuelle



Source : Press Index.

La CNIL vous répond au quotidien

C'est le service d'orientation et de renseignement du public (SORP) qui est en première ligne pour répondre aux usagers, qu'ils soient des professionnels ou des particuliers : c'est lui qui reçoit les courriers, les déclarations, les appels téléphoniques (10 000 appels par mois).

Les courriers

2008	2009	2010
24 225	24 880	28 490

Les déclarations

2008	2009	2010
71 990	68 185	70 797

Depuis mars 2010, toutes les formalités auprès de la CNIL peuvent être réalisées en ligne sur le site internet de la CNIL. Désormais, un formulaire spécifique est proposé pour chacune des procédures prévues par la loi « Informatique et Libertés », alors qu'auparavant, la dématérialisation ne concernait que les déclarations. La dématérialisation des procédures connaît un grand succès puisque **88%** des formalités sont effectuées en ligne.

- **45 173** déclarations simplifiées (**42 188** en ligne et **2 985** sur support papier, soit environ 94% des déclarations simplifiées en ligne).
- **23 690** déclarations normales (**18 449** en ligne et **5 241** sur support papier, soit environ 78% en ligne).
- **800** demandes d'autorisation (**604** en ligne et **196** sur support papier, soit 76% effectuées en ligne).
- **642** demandes d'autorisation de recherche médicale (**415** en ligne et **227** sur support papier, soit 65% en ligne).
- **152** demandes d'autorisation évaluation des soins (**72** en ligne et **80** sur support papier, soit 48% en ligne).
- **340** demandes d'avis (**101** en ligne et **239** sur support papier, soit 30% en ligne).

Dématérialisée, la procédure est accélérée. Depuis le 1^{er} décembre 2010, **le délai moyen de délivrance du récépissé est de 48h pour une déclaration simplifiée, et de 5 jours calendaires pour les déclarations normales.** Ces délais étaient de 13 mois en 2006 et 3 semaines en 2009.

CONSEILLER ET PROPOSER

La CNIL informe les pouvoirs publics

La multiplication des travaux parlementaires auxquels notre Commission a été associée en 2010, comme en attestent les 18 auditions auxquelles elle a participé, souligne l'intérêt grandissant des députés et sénateurs de tous groupes pour les questions relatives à la protection de la vie privée. Elle traduit également leur volonté de se saisir de ces thématiques nouvelles.

La multiplication des initiatives législatives intéressant notre Commission a confirmé en 2010, peut-être plus que les années précédentes, l'absolue nécessité pour elle d'être présente, tous les jours, aux côtés des parlementaires et des administrateurs des assemblées, pour les accompagner dans leurs travaux, et leur apporter son expertise.

Les initiatives législatives intéressant la CNIL

- Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.
- Adoption le 23 mars 2010 par le Sénat, en première lecture, de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique.
- Suite de l'examen de la proposition de loi de simplification et d'amélioration de la qualité du droit (devenue loi n° 2011-525 du 17 mai 2011).
- Remise, le 28 octobre 2010, du rapport d'information (n° 2925) du Comité d'évaluation et de contrôle des politiques publiques de l'Assemblée nationale sur les autorités administratives indépendantes.
- Dépôt dans chacune des chambres de propositions de résolution similaires (n° 2837 et n° 168) appelant à l'adoption de standards internationaux dans le domaine de la protection des données personnelles.
- Suite de l'examen du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (devenu loi n° 2011-267 du 14 mars 2011).
- Début de l'examen des projets de loi ordinaire et organique relatifs au Défenseur des droits (devenus loi n° 2011-334 et loi organique n° 2011-333 du 29 mars 2011).

Faciliter la recherche dans le domaine de la santé

La CNIL a été alertée, à de nombreuses reprises, des difficultés juridiques et techniques que rencontrent les chercheurs et les autorités sanitaires en France pour mener à bien certaines études, faute de pouvoir utiliser le NIR (numéro de sécurité sociale). Ces acteurs ne sont pas toujours en mesure de fournir aux pouvoirs publics des indicateurs statistiques fiables, pourtant indispensables à la définition et à l'évaluation des politiques de santé publique et à la surveillance sanitaire de la population.

Soucieuse de faciliter la recherche médicale et les études de santé publique, tout en garantissant la protection des données personnelles et de la vie privée, notre Commission a pris l'initiative de proposer aux ministres concernés qu'un décret en Conseil d'État prévoit et détermine une politique d'accès au NIR à des fins de recherche et d'études de santé publique.

Améliorer la sécurité juridique en développant le correspondant informatique et libertés (CIL)

La CNIL a accentué ses démarches de sensibilisation à la loi « Informatique et Libertés » en direction des collectivités locales et des entreprises. Elle a ainsi signé en 2010 quatre nouvelles conventions de partenariat, qui ont principalement pour objectif de diffuser la culture « Informatique et Libertés » et de favoriser la désignation de correspondants informatique et libertés (CIL). Ces conventions ont été signées avec une association de maires (Association des maires de Meurthe-et-Moselle), un incubateur de sociétés innovantes (incubateur national Belle de Mai à Marseille), le Conseil national des barreaux (CNB) et le Conseil supérieur du notariat (CSN).

Le CIL apparaît aujourd'hui comme un acteur incontournable de la protection des données. La proposition de loi visant à mieux garantir le droit à la vie privée à l'heure

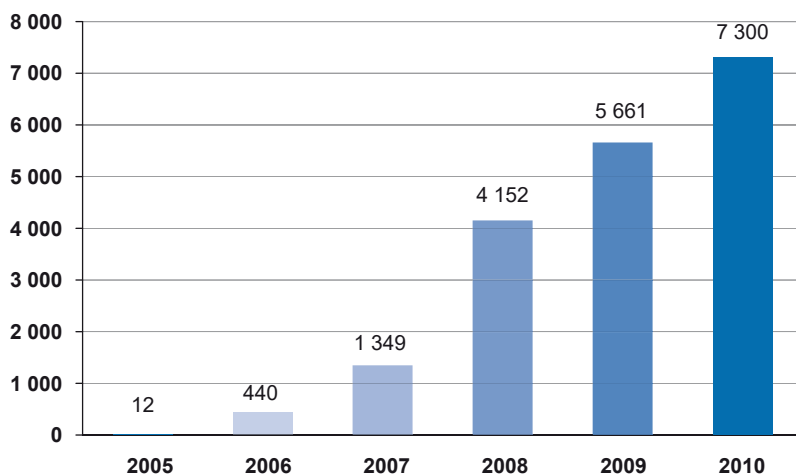
du numérique, adoptée au Sénat en première lecture en mars 2010, pourrait le rendre obligatoire. Un choix similaire pourrait également être fait par la Commission européenne à l'occasion de la révision de la directive européenne sur la protection des données.

La CNIL a mis en place un service exclusivement dédié à l'accompagnement des CIL dont le nombre est en progression constante depuis 2005. Elle a organisé 25 ateliers de

formation (généralistes ou thématiques) qui ont réuni 530 participants. L'exercice de cette fonction s'affirme comme un métier à part entière. C'est pourquoi, la CNIL souhaite sa reconnaissance par une inscription dans les répertoires de métiers gérés notamment par Pôle emploi ou le Centre national de la fonction publique territoriale (CNFPT).

Pour la première fois, la CNIL a réuni les correspondants à l'occasion d'une convention organisée le 8 avril 2011.

Nombre d'organismes ayant désigné un CIL



CONTRÔLER

La Commission s'était fixé des objectifs ambitieux en termes de contrôles pour l'année 2010. Ceux-ci ont été atteints et confirment ainsi la place prépondérante de l'activité de contrôle sur place de la CNIL.

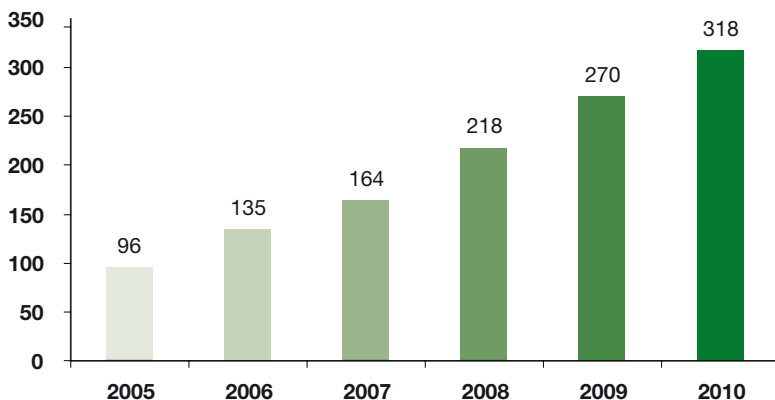
Ainsi, **308 contrôles** ont été effectués au cours de l'année 2010, soit **une augmentation de 14%** par rapport à l'année 2009. Cette progression s'inscrit dans le processus continu, depuis 2004, de l'augmentation du nombre de contrôles.

L'année 2010 aura également permis à la CNIL d'assurer une présence en termes de contrôles sur l'ensemble du territoire, comme le montre la carte ci-dessous.

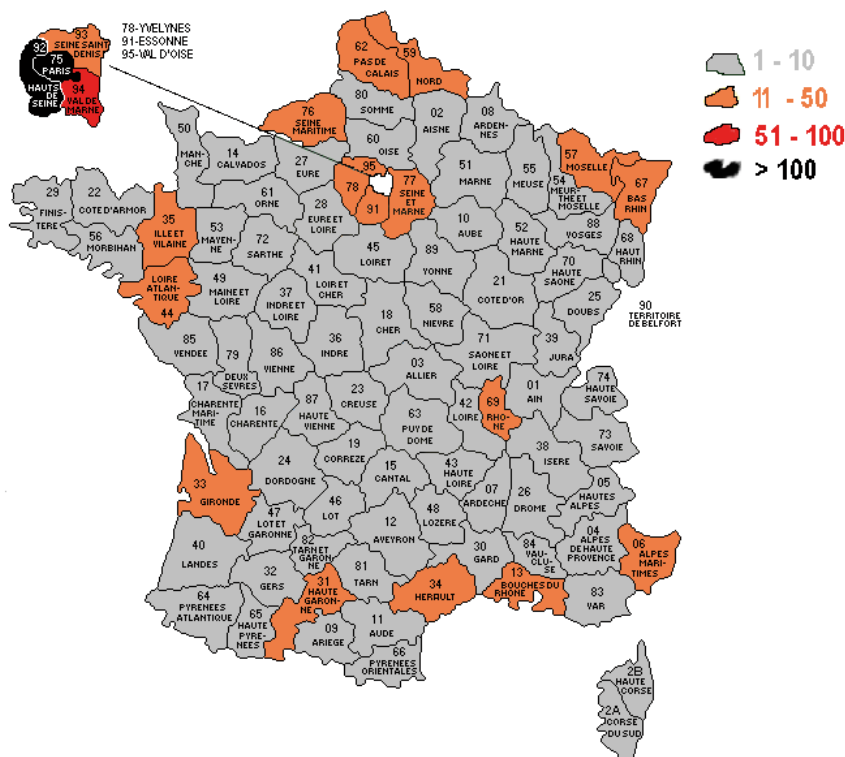
Concernant les organismes contrôlés au cours de cette année, on peut mentionner les chiffres suivants :

- 80% des organismes appartiennent au secteur privé ;
- 20% relèvent de la sphère publique ;
- et 95% des organismes contrôlés n'avaient pas désigné de correspondant Informatique et Libertés au moment du contrôle.

Nombre de contrôles réalisés



Répartition géographique des contrôles



Les contrôles significatifs

On peut citer les contrôles effectués en octobre 2010 auprès **de la gendarmerie nationale** dans le cadre du dossier dit « MENS » qui ont permis à la Commission d'adresser rapidement un rapport complet au Premier ministre sur cette question. On peut aussi évoquer les contrôles effectués à la suite **des révélations sur les prétendus antécédents judiciaires de M. Soumaré**. Ils ont permis, d'une part, d'identifier l'origine de la fuite des informations concernant le candidat aux élections régionales et, d'autre part, d'attirer l'attention de la Chancellerie sur l'absence de traçabilité des accès à l'application de la nouvelle chaîne pénale. Enfin, on peut parler des nombreux contrôles réalisés auprès de **la société Google Inc. dans le cadre du dispositif « Streetview »**.

Le programme des contrôles pour l'année 2010 a été intégralement réalisé.

Des contrôles ont été effectués sur la thématique du **voyage aérien** (contrôles d'aéroports, de compagnies aériennes, de sociétés de sécurité privée, de postes de police et de douanes, etc.), de **la protection des données de mineurs** (conseils généraux, établissements scolaires, associations, mairies et entreprises de cours à domicile) et **du droit au logement** (agences immobilières, offices HLM, etc.).

La CNIL a également mené un certain nombre de contrôles pour vérifier le respect des normes juridiques qu'elle adopte (normes simplifiées, autorisations uniques, etc.) et des normes techniques qu'elle impose (mesures de sécurité entourant les traitements les plus sensibles).

Enfin, on doit relever que **19% des contrôles ont été effectués dans le cadre de l'instruction de plaintes et 11% dans le cadre des suites des décisions de la formation restreinte**. Par exemple, à la suite d'une mise en demeure, des contrôles peuvent être effectués de façon à vérifier la mise en conformité des systèmes ou dispositifs.

Les coopérations

La CNIL a multiplié les **coopérations** avec d'autres autorités publiques :

- un protocole a ainsi été signé le 6 janvier 2011 avec la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) afin que celle-ci puisse transmettre à la CNIL les noms des principaux sites web sur lesquels des manquements à la loi « Informatique et Libertés » auraient été constatés;
- la CNIL est par ailleurs de plus en plus régulièrement saisie de demandes de contrôle venant de l'inspection du travail;
- la CNIL a adhéré à un mécanisme de coopération internationale en matière de contrôle *a posteriori* sur les questions de vie privée : le GPEN (*Global Privacy Enforcement Network*).

SANCTIONNER

La réforme de la formation contentieuse

À la suite de la publication des lois organique et ordinaire relatives au Défenseur des droits le 30 mars 2011, l'organisation et le fonctionnement de la formation contentieuse de la Commission ont été profondément modifiés.

Le législateur a formellement consacré par cette réforme les règles du procès équitable en exigeant une stricte séparation des phases d'enquête et d'instruction d'une part, et de jugement, d'autre part. Ainsi, la composition de la formation restreinte est modifiée : les membres du bureau (Président et Vice-présidents) ne peuvent plus en faire partie. Celle-ci est désormais composée d'un président distinct de celui de la formation plénière et de cinq autres membres élus par les dix-sept membres du collège.

En application de ces dispositions, la Commission a procédé à l'élection des six membres de la formation restreinte lors de sa séance plénière du jeudi 5 mai 2011. Elle a ensuite procédé à l'élection du président de la formation.

Les membres élus de la formation restreinte

Claire DAVAL, Présidente ;
Jean-François CARREZ ;
Jean-Marie COTTERET ;
Claude DOMEIZEL ;
Sébastien HUYGHE ;
Dominique RICHARD.

Afin de répondre également aux exigences de l'article 6-1 de la CEDH (Cour européenne des droits de l'homme), les mises en demeure sont désormais décidées par le seul président de la CNIL.

Enfin, grâce à cette réforme, la Commission dispose d'une plus grande liberté de publicité de ses décisions : le bureau peut désormais, sur demande du Président, décider de la publicité des mises en demeure, et la formation restreinte dispose, elle, d'une plus grande liberté pour la publication des sanctions qui ne sont désormais plus soumises à la condition de mauvaise foi pour insertion dans la presse.

Zoom

Google « Street View » : la CNIL a prononcé une amende de 100 000 euros

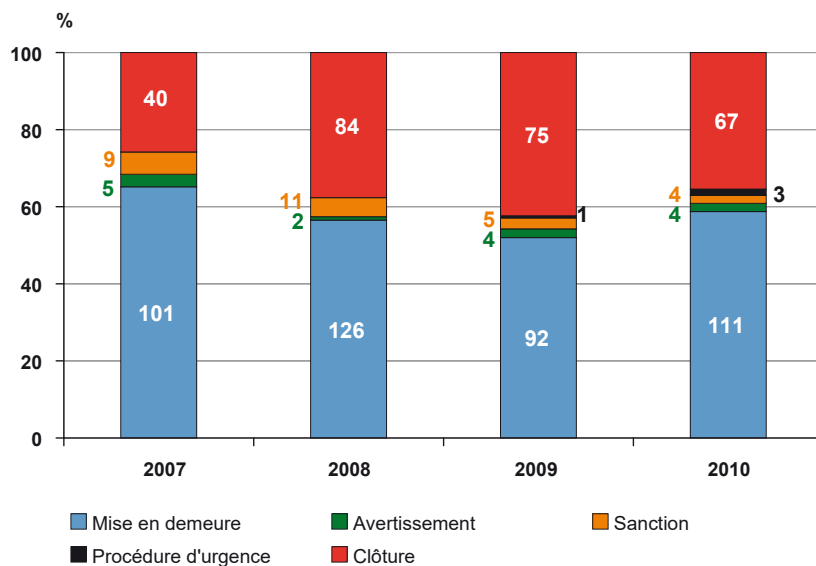
La société Google procède depuis plusieurs années à la collecte massive de données techniques sur les réseaux Wi-Fi, aux fins d'offrir des services de géolocalisation, notamment les services Google Maps, Street View et Latitude. La Commission a mené une série de contrôles sur place afin de vérifier la conformité de ces traitements à la loi « Informatique et Libertés ».

Ces contrôles ont révélé divers manquements comme la collecte de données Wi-Fi à l'insu des personnes concernées et la captation de données dite « de contenu » (identifiants, mot de passe, données de connexion, échanges de courriels). La CNIL a donc mis en demeure la société Google en mai 2010, de régulariser sa situation. Estimant que Google n'avait pas répondu à ses demandes dans les délais impartis, la formation contentieuse de la CNIL a prononcé à l'encontre de la société, le 17 mars 2011, une amende de 100 000 euros.

Un tableau recensant toutes les sanctions adoptées en 2010 est disponible en annexe de ce rapport.

Les procédures engagées devant la formation contentieuse sont en évolution constante depuis l'année 2007, malgré un ralentissement de l'activité en 2009 (ayant pour origine les conséquences de deux décisions du Conseil d'État du 6 novembre 2009 relatives à la notification du droit d'opposition lors des missions de contrôles de la Commission). Le bilan de l'année 2010 est marqué par une activité importante et par l'adoption pour la première fois de décisions d'interruption de traitements de données à caractère personnel. À l'instar des autres années, le taux de mise en conformité suite aux mises en demeure et le taux de décisions de clôture particulièrement élevé, démontrent le caractère pédagogique et l'efficacité de la procédure de mise en demeure.

Décisions de sanction



ANTICIPER

La CNIL doit permettre à notre société de faire face aux nouveaux défis technologiques. Pour remplir cette mission, elle s'est dotée d'un service de l'expertise informatique composé d'ingénieurs spécialisés qui analysent le fonctionnement des nouvelles technologies dans un grand nombre de domaines allant d'internet à la biométrie, en passant par les RFID et le vote électronique. Leur travail consiste non seulement à estimer les risques d'atteinte à la vie privée liés à une technologie mais aussi à évaluer les mesures de sécurité qui peuvent être mises en œuvre en réponse à ces risques. Dans un monde technologique de plus en plus complexe, cette expertise est devenue incontournable pour dialoguer avec les acteurs du monde numérique et permettre de mener une réflexion sur l'innovation.

À court terme, l'enjeu principal sera de parvenir à préserver nos libertés fondamentales, notamment d'expression et d'aller et venir, dans un contexte de développement technologique accéléré et de traçabilité. Les menaces se matérialisent plus précisément dans les capacités de communication des objets de notre quotidien, en particulier de nos smartphones, qui peuvent être géolocalisés en permanence. Ainsi, de nouveaux usages sont régulièrement inventés tels que le paiement sans contact ou les multiples applications reposant sur l'internet mobile.

Des utilisations inconscientes du mobile font aussi leur apparition. Il s'agit des dispositifs de mesure d'audience qui permettent, dans les centres commerciaux ou les aéroports, de suivre le parcours d'une personne ou de mesurer le temps qu'elle passe dans une file d'attente.

Dans un autre domaine, les compteurs intelligents permettent de connaître très précisément la consommation électrique d'un foyer. Chaque équipement ayant une signature électrique qui lui est propre, une fréquence de mesure élevée permet de savoir quel équipement est utilisé à quel moment. Un profilage des habitudes de consommation, à l'intérieur même de la maison, devient alors possible.

Enfin, le développement des objets communicants annonce l'avènement de « l'internet des objets », dont on commence à peine à percevoir la complexité en termes de gouvernance, de protection des données, d'usages et de sécurité.

Pour faire face à ces défis, il paraît nécessaire non seulement de bien comprendre les enjeux technologiques d'aujourd'hui mais également d'anticiper ceux de demain. À cet effet, la Commission s'appuie sur une forte expertise en interne ainsi que sur la création en janvier 2011 d'une nouvelle direction entièrement dédiée à la prospective et l'innovation (voir chapitre II du rapport). Cette nouvelle direction permettra de mener une réflexion faisant non seulement intervenir des juristes et des experts informatiques mais aussi des sociologues, des politiques et des économistes, car ces enjeux concernent tous les secteurs de notre société. En parallèle, la Commission échange et développe sa capacité d'influence auprès de ses homologues, de groupes d'experts ou des agences en charge de la sécurité informatique, tant au niveau national qu'europpéen. Elle met également en place des conventions de partenariat avec des organismes de recherche publique.

La CNIL agit ensuite à plusieurs niveaux :

- par la pédagogie, en rédigeant des bonnes pratiques dans le domaine de la sécurité comme le *Guide sécurité* paru en 2010, ou encore en analysant minutieusement les risques générés par les nouvelles technologies et en décrivant sur son site comment s'en prémunir ;
- en développant le *Privacy by Design*, c'est-à-dire en aidant les industriels à intégrer la protection des données dès la conception de leurs produits, ou en soutenant les solutions techniques permettant de juguler les problèmes créés par la technologie ;
- en adoptant des décisions juridiques ancrées dans la réalité et la complexité technique ; c'est ainsi, par exemple, que la recommandation de la CNIL sur le vote électronique a été révisée en octobre 2010.

Enfin, la CNIL développe son pouvoir de labellisation. Il constituera un levier de régulation économique incitant les entreprises et les personnes à favoriser les procédures ou les produits respectueux de la vie privée. Les premiers labels seront délivrés au cours du second semestre 2011.

SIMPLIFIER ET RÉGLEMENTER

La CNIL poursuit ses efforts pour simplifier les formalités par le biais d'exonération de déclaration, de déclaration simplifiée ou d'autorisation unique.

Au titre de la simplification des formalités préalables, la CNIL a adopté en 2010 :

– **4 autorisations uniques** : par exemple, autorisation unique relative aux éthylotests anti-démarrage dans les véhicules affectés aux transports de personnes du 28 janvier 2010, modification de l'autorisation unique relative aux alertes professionnelles du 14 octobre 2010 ;

– **2 normes simplifiées** : norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France (MICEN) du 9 septembre 2010, modification de la norme simplifiée concernant la durée de conservation et le versement aux archives publiques des données issues de la matrice cadastrale du 11 février 2010,

– **1 dispense** : mise à jour de la dispense relative aux traitements mis en œuvre par les associations et organismes à but non lucratifs du 10 juin 2010 ;

– **2 avis sur acte réglementaire unique** : téléservice « guichet-entreprise. fr » du 28 janvier 2010, téléservice demandes d'acte civil du 25 mai 2010 ;

– **3 recommandations** : recommandation relative à la sécurité des systèmes de vote électronique du 21 octobre 2010, recommandation relative à la réutilisation des données à caractère personnel contenues dans des documents d'archives publiques du 9 décembre 2010, recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules du 8 avril 2010.

Zoom

Éthylotests anti-démarrage : adoption d'une autorisation unique

Depuis le 1^{er} janvier 2010, les autocars neufs affectés aux transports en commun d'enfants sont obligatoirement équipés d'un système de mesure du taux d'alcoolémie au démarrage (EAD). Afin de faciliter les démarches des sociétés de transports, la CNIL a adopté une autorisation unique encadrant ces dispositifs.

En cas de taux d'alcoolémie égal ou supérieur à un taux prédéfini, le démarrage du véhicule est bloqué, un voyant rouge s'allume, sans que le taux d'alcoolémie ne s'affiche. Un nouvel essai est alors possible au bout d'une minute. Si le souffle reste positif, l'EAD bloque le démarrage pendant trente minutes. Le véhicule peut toutefois démarrer sans qu'il soit nécessaire de souffler dans l'EAD, notamment au moyen d'une clé détenue par le chauffeur ou par un code détenu par l'employeur. Tout démarrage sans utilisation de l'EAD est enregistré.

L'EAD fonctionne à partir d'un boîtier numéroté installé dans le véhicule. Le fait qu'il soit possible, à partir du numéro de l'EAD, d'identifier un conducteur en particulier, y compris de manière indirecte, permet de considérer qu'il s'agit d'un traitement de données à caractère personnel, puisqu'il est possible, à partir du numéro de l'EAD, d'identifier le conducteur concerné (horodatage des données associées au numéro de l'EAD).

Un nombre important d'organismes sont d'ores et déjà concernés par la mise en place des EAD et ce dispositif a vocation à s'étendre à tous les transports en commun à partir de 2015. Au vu du nombre de sociétés potentiellement concernées, la CNIL a adopté une autorisation unique. Cette mesure de simplification permet désormais aux sociétés de transports d'effectuer, directement en ligne, un engagement de conformité à cette norme. En 2010, environ 400 engagements de conformité à l'autorisation unique EAD (AU n° 26) ont été effectués.

LES TEMPS FORTS





LES FAITS MARQUANTS

15 janvier 2010

- Le premier prix de thèse Informatique et Libertés a été décerné à madame Marie-Charlotte ROQUES BONNET.

28 janvier 2010

- Ouverture des comptes Facebook, Twitter et Dailymotion de la CNIL.
- Publication d'une édition spéciale de *Mon Quotidien* « protège ta vie privée sur internet ».
- Lancement du clip « jepubliejeréfléchis » avec internet sans crainte.

9 février 2010

- La CNIL parraine le 1^{er} épisode du serious game 2025 ex-machina consacré aux réseaux sociaux.

10 février 2010

- Rejet de l'accord SWIFT par le Parlement européen.

11 février 2010

- Signature d'une convention de partenariat avec le Conseil national des barreaux (CNB).
- Autorisation d'une expérimentation d'un dispositif biométrique pour contrôler l'identité de patients pris en charge en radiothérapie.

25 février 2010

- La CNIL demande des explications sur l'origine des informations concernant M. Ali Soumaré.

Mars 2010

- Toutes les formalités préalables (demande d'avis, d'autorisation, déclaration) peuvent se faire en ligne sur le site de la CNIL.

18 mars 2010

- La CNIL ordonne, pour la première fois, l'interruption en urgence d'un traitement (contrôle d'accès biométrique illicite).

30 et 31 mars 2010

- Rencontres régionales en Bourgogne.

1^{er} avril 2010

- Autorisation d'une expérimentation d'un système de paiement reposant sur l'authentification du réseau veineux du doigt.

8 avril 2010

- Refonte de la recommandation relative aux nouveaux services de géolocalisation (*Pay as you drive*, lutte contre le vol).

13 avril 2010

- Signature d'une convention de partenariat avec l'Association des maires de Meurthe-et-Moselle.

20 avril 2010

- 10 autorités de protection des données (Canada, France, Allemagne, Irlande, Israël, Italie, Pays-Bas, Nouvelle-Zélande, Espagne, Royaume Uni) demandent à Google des explications à propos du lancement de son service Google Buzz.

22 avril 2010

- La CNIL ordonne l'interruption en urgence d'un système de vidéosurveillance permanente des salariés.
- Avertissement public prononcé à l'encontre d'AlS2 (Academia) pour des commentaires excessifs dans ses fichiers.

18 mai 2010

- Un rapport du Conseil national de la consommation propose de mieux défendre les droits Informatique et Libertés des consommateurs.

26 mai 2010

- Mise en demeure de Google en raison de la collecte de données Wi-Fi par les véhicules Street View.

14 juin 2010

- Ouverture du service de plainte en ligne sur www.cnil.fr

17 juin 2010

- Amende de 15 000 euros prononcée à l'encontre d'une société récidiviste (envoi de fax publicitaires non sollicités par la société JPSM).

22 et 23 juin 2010

- Rencontres régionales en Auvergne.

1^{er} juillet 2010

- La loi portant réforme du crédit à la consommation crée un comité de préfiguration du futur registre national des crédits aux particuliers auquel la CNIL est invitée à participer.

7 juillet 2010

- Le Parlement européen approuve le nouvel accord SWIFT.

12 juillet 2010

- La loi dite « Grenelle II » soumet à l'autorisation préalable de la CNIL les panneaux publicitaires de mesure d'audience.

17 septembre 2010

- Signature d'une convention de partenariat avec le Conseil supérieur du notariat (CSN).

7 octobre 2010

- Publication sur le site de la CNIL du *Guide sécurité des données personnelles*.

14 octobre 2010

- La CNIL publie ses premières conclusions à la suite des contrôles effectués à la gendarmerie nationale pour vérifier l'existence d'un fichier dénommé « MENS ».
- Adoption des recommandations pour la mise en œuvre des compteurs électriques intelligents (dits *Smart grids*).
- Modification du champ d'application de l'autorisation unique relative aux alertes professionnelles, suite à l'arrêt de la Cour de cassation de décembre 2009.

21 octobre 2010

- Mise à jour de la recommandation sur le vote électronique.

29 octobre 2010

- La conférence internationale des commissaires à la protection des données et de la vie privée se tenant à Jérusalem appelle les pouvoirs publics nationaux à se mobiliser pour adopter une convention internationale.

4 novembre 2010

- La Commission européenne dévoile ses orientations stratégiques pour la révision de la directive de 1995 sur la protection des données et de la vie privée.

17 et 18 novembre 2010

- Rencontres régionales en Haute-Normandie.

25 novembre 2010

- La CNIL adresse une édition spéciale de *Mon Quotidien* à toutes les classes de CM2.

2 décembre 2010

- Autorisation du déploiement du DMP (dossier médical personnel) sur l'ensemble du territoire.

15 décembre 2010

- Ouvertures des comptes Viadéo et LinkedIn de la CNIL.

1^{er} janvier 2011

- Création d'une nouvelle direction chargée des études, de l'innovation et de la prospective.

4 janvier 2011

- Envoi d'une édition spéciale du journal l'ACTU dans les classes de 4^e des collèges.

- Envoi du Guide sur l'enseignement à tous les chefs d'établissement du second degré.

- Ouverture d'un espace dédié aux enseignants sur www.jeunes.cnil.fr.

6 janvier 2011

- Signature d'un protocole de coopération avec la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes).

Janvier 2011

- La CNIL demande à ce que le NIR (numéro de sécurité sociale), puisse être employé pour faciliter la recherche médicale.

14 janvier 2011

- La CNIL décerne son second Prix de thèse à monsieur Nicolas LECHOPIER.

24 au 28 janvier 2011

- Rencontres régionales en Guyane, Martinique et Guadeloupe.

28 janvier 2011

- Lancement de l'application CNIL pour apprendre à rester net sur le web à l'occasion de la journée européenne de protection des données.

3 mars 2011

- Publication de l'avis sur le décret relatif à la conservation d'informations par les hébergeurs et les FAI.
- Autorisation de deux dispositifs d'alertes professionnelles dédiés au traitement des plaintes en matière de discriminations et s'inscrivant dans le cadre du label « Diversité ».

14 mars 2011

- Promulgation de la LOPPSI qui donne à la CNIL un pouvoir de contrôle des systèmes de vidéoprotection installés sur la voie publique.

21 mars 2011

- 100000 euros d'amende pour Google et son service Street View.

31 mars 2011

- Publication de la loi sur le Défenseur des droits qui modifie l'organisation de la CNIL et notamment la composition de la formation contentieuse. Cette loi précise : « La fonction de président de la Commission est incompatible avec toute activité professionnelle, tout mandat électif national, tout autre emploi public et toute détention, directe ou indirecte, d'intérêts dans une entreprise du secteur des communications électroniques ou de l'informatique. »

NOTRE PRIORITÉ : sensibiliser les jeunes et les professionnels de l'éducation aux bonnes pratiques sur internet afin de favoriser une instruction « civico-numérique »

Aujourd'hui, 70% des moins de 11 ans utilisent internet, et 49% des 11-12 ans possèdent leurs propres téléphones portables qui permettent pour la plupart un accès illimité aux réseaux sociaux Twitter ou Facebook alors même que ce dernier est théoriquement interdit aux moins de 13 ans (source : étude IPSOS/e-enfance, décembre 2008). Parallèlement, de plus en plus d'établissements scolaires ont recours à des systèmes de vidéoprotection, et pour plus de 400 d'entre eux à des systèmes de reconnaissance biométrique à l'entrée des cantines.

Force est de constater que la conception de la vie privée est en train de changer face à la percée des nouvelles technologies dans notre vie quotidienne. Les jeunes générations vivent avec une informatique ambiante, « au bout de leur doigts », d'un maniement naturel et spontané. Ils revendiquent le droit à la transparence, à la liberté d'expression, souvent au détriment de leur intimité.

Si la Commission n'a aucun jugement *a priori* à porter sur les technologies liées au numérique et ne conteste pas la nécessité d'en utiliser certaines, il faut être conscient qu'en ce domaine, la combinaison de certaines technologies aboutit à des dispositifs ultra-performants de traçage des personnes. Il faut dès lors réfléchir à leur usage : telle est la première mission, aujourd'hui, de la Commission.

La pression de ces nouvelles technologies sur le monde de l'éducation exige que soit traitée, de façon prioritaire, la question de la protection de la vie privée. La Commission a donc décidé de lancer en 2010 et 2011 un plan d'urgence, massif, de sensibilisation des acteurs à ces questions, afin d'inciter les jeunes à adopter de bonnes pratiques quant à l'utilisation d'internet et la protection de leur vie privée. Ces actions entendent accompagner toute la communauté éducative pour que les élèves puissent, tout à la fois, profiter de ce qu'apporte le réseau en termes de dialogue et d'accès à la connaissance, et assurer la préservation de leur identité et de leur intimité.

La première réponse qui doit être apportée à la communauté éducative doit reposer sur la pédagogie. Il s'agit non seulement de veiller à l'application de la loi « Informatique et Libertés » mais également de sensibiliser

aussi bien les parents, les élèves, les professeurs et les chefs d'établissements aux règles à mettre en œuvre pour encadrer la création de fichiers et empêcher que les capacités de stockage et de recherche qu'offre l'informatique ne soient utilisées pour porter atteinte aux libertés.

Vers une instruction civico-numérique

La Commission est extrêmement favorable à une instruction civique résolument moderne, visant à apprendre aux élèves à préserver les valeurs essentielles que sont l'identité et l'intimité.

Elle se félicite que l'article L. 312-15 du Code de l'éducation nationale vienne d'être complété et prévoit désormais que : « Dans le cadre de l'enseignement d'éducation civique, les élèves sont formés afin de développer une attitude critique et réfléchie vis-à-vis de l'information disponible et d'acquiescer un comportement responsable dans l'utilisation des outils interactifs lors de leur usage des services de communication au public en ligne. Ils sont informés des moyens de maîtriser leur image publique, des dangers de l'exposition de soi et d'autrui, des droits d'opposition, de suppression, d'accès et de rectification prévus par la loi n° 78-17 du 6 janvier 1978 relative à

l'informatique, aux fichiers et aux libertés, ainsi que des missions de la Commission nationale de l'informatique et des libertés.»

La solution n'est pas seulement de consacrer un module de formation, parmi d'autres, à ces questions. Il convient surtout de teinter toutes les disciplines de la préoccupation « Informatique et Libertés ». Cette instruction civique résolument moderne, devra être fondée sur les valeurs d'identité et d'intimité.

Les nouvelles générations doivent en effet se réapproprier les notions d'identité, de personnalité, de vie privée, d'intimité et en percevoir toutes les nuances. Il semble se dégager de l'utilisation faite par les jeunes du réseau une confusion entre intimité et innocence. Ils n'hésitent pas à livrer sur internet des informations personnelles, dès lors que, disent-ils, « ils n'ont rien à se reprocher ». Or, ce raisonnement peut être dangereux.

En effet, aujourd'hui aucun utilisateur d'internet ne peut avoir la certitude absolue, lorsqu'il quitte le réseau, de ne pas y laisser des informations, sans parler de celles qui ont été confiées à son insu par quelqu'un d'autre. Il faut être conscient du fait que s'il est porté atteinte à l'intimité, cette dernière, ne se reconstitue pas.

Il faut également repenser les relations au sein de la communauté éducative, dans la mesure où le réseau abolit les frontières de la classe. En effet, l'espace numérique de travail (ENT) est l'illustration parfaite de cette dématérialisation de la classe et donc des relations au sein d'un établissement scolaire. Les contenus et supports de cours sont désormais accessibles en continu, la classe au sens matériel du terme n'a plus le même sens, ni la même réalité temporelle. Désormais le professeur peut, s'il le souhaite, communiquer en dehors des horaires de classe avec ses élèves, avec les parents ou ses collègues. L'abolition de ces frontières pose la question de l'articulation entre le droit de regard du chef d'établissement et la liberté pédagogique des professeurs.

Un nouveau cadre doit être défini, afin de protéger les professeurs, ainsi que les élèves les uns par rapport aux autres. Il est inconcevable que de jeunes enseignants d'université ou des étudiants puissent avoir le sentiment que leur vie est brisée, en raison du harcèlement dont ils font l'objet sur le réseau.

Une nouvelle forme de harcèlement scolaire : le harcèlement numérique

Suite à l'ensemble des plaintes et des événements relevés en 2010, le ministère de l'Éducation nationale, de la Jeunesse et de la Vie associative a développé en 2011 une réflexion majeure sur le harcèlement à l'école.

En avril 2011, le rapport rendu par É. DEBARBIEUX au ministre chargé de l'Éducation nationale, de la Jeunesse et de la Vie associative identifiait les nouvelles formes de harcèlement, mettant ainsi en relief que « *les développements des technologies de la communication changent le problème du harcèlement à l'École, en abolissant la distinction entre harcèlement à l'École et poursuite de ce harcèlement hors l'École* »¹.

Outre-Atlantique, le *Cyberbullying research center* propose une définition du cyberharcèlement, ou *cyberbullying* qui a été reprise dans les travaux rendus au ministère : le harcèlement numérique serait le fait de se moquer de manière répétée d'une autre personne en ligne, de la harceler par courrier électronique ou bien de poster sur internet un contenu préjudiciable à une autre personne.

Bien qu'inédites, ces pratiques connaissent une croissance exponentielle. Le constat dressé est alarmant : à l'école élémentaire, le nombre de victimes de harcèlement verbal ou symbolique peut être estimé à environ 14% des élèves, dont 8% d'élèves victimes d'un harcèlement sévère (insultes, atteintes physiques, dénigrement public et répété par un ou plusieurs individus) et 6% d'élèves d'un harcèlement « modéré » (actes ponctuels de dénigrement, médisance, indiscretion)².

Concernant les nouvelles formes de harcèlement, l'enquête réalisée en 2010 sur un échantillon de 1 000 enfants âgés de 9 à 16 ans³ établit que 25% des 9-10 ans sont inscrits sur Facebook, généralement avec l'accord des parents, bien que cela soit interdit jusqu'à l'âge de 13 ans. Or, cette entrée très précoce sur les réseaux sociaux génère nombre d'expériences douloureuses, étroitement liées à l'environnement scolaire de l'enfant.

En France, au collège, 7,5% des élèves ont été confrontés à une intimidation sur internet, contre une moyenne de 6% à 15% d'élèves harcelés (les *bullied*) à l'étranger⁴.

5% d'entre eux ont été victimes de « *happy slapping* » (lynchage collectif filmé *via* un téléphone mobile, et souvent mis à disposition en ligne sur des sites tels que

1. DEBARBIEUX É., *Refuser l'oppression quotidienne : la prévention du harcèlement à l'École*, Rapport au ministre de l'Éducation nationale, de la Jeunesse et de la Vie associative, Observatoire international de la violence à l'école – Université Bordeaux Segalen, 12 avril 2011, p. 9.

2. Enquête en école élémentaire réalisée sur un échantillon de 12 326 élèves dans 157 écoles.

3. Enquête de D. PASQUIER, du Laboratoire traitement et communication de l'information (CNRS/Télécom Paris Tech) réalisée à domicile entre mai et août 2010 sur un échantillon de 25 140 enfants de 9 à 16 ans utilisateurs d'internet et un de leurs parents.

4. Le nombre d'élèves harcelés peut atteindre 20% de victimes et d'agresseurs en Espagne ou au Portugal et en Corée.

Youtube ou Dailymotion), dont 2,8% plusieurs fois⁵. Une autre enquête locale a démontré que plus de 6% des collégiens sont confrontés de manière répétée à des moqueries sur internet, et 5% à des rumeurs propagées par SMS⁶.

Certes, le nombre de plaintes reste assez faible, mais la CNIL a constaté une progression des cas de harcèlement ou de lynchages sur internet, en particulier sur les réseaux sociaux comme Facebook. En 2010, tous publics confondus, la CNIL a reçu 30 plaintes par mois relatives au cyberharcèlement.

Pour l'heure, il convient de remarquer que l'ensemble de ces indicateurs sont fragiles : l'extension du phénomène interdit toute généralisation de ces chiffres, d'autant plus que nombre de victimes ne déclarent pas les actes de harcèlement dont elles ont souffert.

Néanmoins, à l'unisson avec les équipes mobiles de sécurité, le ministère de l'Éducation nationale et le rapport de M. DEBARBIEUX⁷, la CNIL observe que le cyberharcèlement « devient un des problèmes majeurs dans le déclenchement des faits de violence collective (bagarres collectives naissant de rumeurs sur le web, sur Twitter ou par SMS par exemple) ».

Ce type de harcèlement ne touche pas seulement les élèves, mais nuit également à un nombre croissant d'enseignants et de personnels administratifs. La gravité de ces pratiques est telle qu'elle conduit certains à cesser leur activité de manière temporaire ou définitive.

C'est pourquoi, dès 2010, la CNIL a souhaité sensibiliser tous les publics à l'ensemble des droits protégés par la loi « Informatique et Libertés » modifiée, et invocables par les victimes d'actes de cyberharcèlement.

Tout d'abord, la Commission a souhaité rappeler l'ensemble des droits qu'une personne tient de la loi qui correspond notamment au droit au respect de la vie privée (art. 1^{er} de la loi), du droit à l'information préalable (art. 32), au droit de consentir ou non à la mise à disposition de ses données personnelles (art. 7), ainsi qu'aux droits d'accès à ses données (art. 39), de rectification et de suppression de ses données (art. 40) et d'opposition (art. 38).

5. Enquête effectuée dans l'académie de Bordeaux en 2009 par l'Observatoire international de la violence à l'école, auprès de 462 collégiens.

6. Enquête inédite menée par É. DEBARBIEUX en Aveyron en 2010 sur un échantillon de 1 061 collégiens issus de cinq collèges différents.

7. Parmi les 14 propositions du rapport, 2 visaient directement le harcèlement numérique : la responsabilisation des médias et des opérateurs de téléphonie mobile et fournisseurs d'accès à internet et le lancement d'une campagne nationale de sensibilisation en population générale (proposition n° 3) ; promotion d'une utilisation proactive des réseaux sociaux (proposition n° 12).

Elle a mis en avant le droit, pour toute personne victime de harcèlement, de porter plainte auprès de la CNIL (art. 11-2-c de la loi). Cette plainte pourra être adressée soit par voie postale, soit directement en ligne.

La compétence de la CNIL reste néanmoins limitée au droit d'opposition (art. 38 de la loi), sur le fondement duquel le retrait des contenus illicites pourra être exigé.

La Commission a également sensibilisé les jeunes publics à la possibilité de dénoncer des contenus contraires à l'ordre public par le biais du portail internet-signalement.gouv.fr.

Ce portail permet de transmettre les signalements effectués de manière nominative ou anonyme par des policiers et gendarmes affectés à la Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), qui est intégrée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), ce service appartenant aux services de la Police nationale.

En 2010, ce portail a permis le signalement de 78 000 contenus illicites (contre 53 000 en 2009, pour un internet plus sûr).

La CNIL a rappelé l'applicabilité en ligne de l'article L. 232-33-2 du code pénal : « Le fait de harceler autrui par des agissements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel, est puni d'un an d'emprisonnement et de 15 000 euros d'amende. »

Dès lors, le *cyberbullying* revêtant un caractère illégal, la Commission recommande aux victimes des actes de harcèlement numérique d'effectuer un dépôt de plainte auprès de l'autorité judiciaire (art. L. 226-16 et suivants du Code pénal).

La CNIL poursuivra cette action avec le ministère de l'Éducation nationale, conformément au souhait exprimé par le ministre chargé de l'Éducation, Luc CHATEL, lors de son discours de clôture des assises nationales sur le harcèlement scolaire ouvertes les 2 et 3 mai 2011 à Paris.

Rassemblant des professeurs, parents, psychologues et spécialistes afin de proposer des mesures concrètes pour lutter contre le harcèlement à l'École, ces assises ont donné lieu à l'identification d'axes d'intervention, auxquels s'associe la CNIL.

Il s'agira, en partenariat avec la CNIL et l'association e-enfance (association reconnue d'utilité publique, créée en 2005), de mettre en œuvre la formation de formateurs et de mettre à disposition les ressources pédagogiques de la CNIL afin de sensibiliser les conseillers principaux d'éducation, les chefs d'établissement, les professeurs ou les personnels administratifs et parascolaires à ces nouvelles problématiques.

Il s'agira également de traiter les cas avérés de harcèlement, et particulièrement les cas de *cyberbullying*. Cette mesure concerne en premier lieu le harcèlement sur internet. Elle a pour ambition de faire cesser les brimades, les humiliations et les persécutions qui rendent le quotidien de certains élèves invivable. Elle vise à créer une nouvelle sanction disciplinaire d'intérêt général : la suspension du profil Facebook des élèves « harceleurs ».

Associée à la réflexion du ministère, Facebook a admis le principe d'un partenariat avec l'institution scolaire pour mettre en œuvre une suppression des pages personnelles appartenant aux cyberharceleurs, notamment par le biais du Centre de sécurité de Facebook (Facebook Safety Center : www.facebook.com/safety.com) et par celui du système de signalement d'abus disponible via des liens sur le site de Facebook.

Néanmoins, à ce jour, les conditions de mise en œuvre de cette suppression restent à préciser.

Pour les cas les plus graves, les familles des élèves victimes bénéficieront d'un accompagnement adapté pour déposer plainte, via un partenariat avec l'Office central de lutte contre la cyber-criminalité.

La Commission reste néanmoins convaincue qu'une pédagogie nouvelle, construite en partenariat et en réseau avec le ministre de l'Éducation nationale, les recteurs, les inspecteurs d'académie, les chefs d'établissement, les parents d'élèves et surtout avec les jeunes fournira les points

de repère qui manquent aujourd'hui pour éradiquer le harcèlement numérique et encourager un usage civilisé de l'internet, que ce soit au sein de l'École, ou bien en dehors.

Les actions de sensibilisation

La CNIL a initié de nombreuses actions de sensibilisation en 2010 et 2011 qui ont représenté un investissement budgétaire de 500 000 euros, sans précédent à la CNIL. Elle a d'abord choisi de s'adresser aux enfants de CM2 en leur adressant, à tous, un exemplaire de l'édition spéciale de *Mon Quotidien* (le journal des 10-14 ans édité par Play Bac) intitulé « Protège ta vie privée sur internet ». L'objectif étant de leur rappeler que la vigilance s'impose dès aujourd'hui, en particulier lorsqu'il s'agit de diffuser des informations à caractère politique, sexuel, médical ou religieux. C'est bien avant de publier qu'il faut réfléchir car, une fois en ligne, il est difficile de supprimer les informations qui peuvent les suivre toute leur vie.

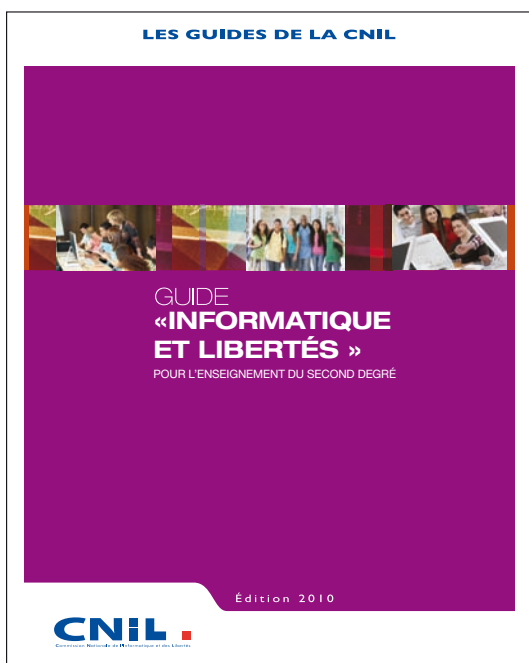
La CNIL s'est ensuite adressé aux collégiens ainsi qu'à leurs enseignants en leur adressant un numéro spécial de *l'actu* (le journal des 14-18 ans). Les CDI (centres de documentation et d'information) ont aussi été destinataires de ces supports. Cet envoi était accompagné d'un poster présentant les « 10 conseils de la CNIL pour rester net sur le web ».

La CNIL s'est également associée à internet sans crainte pour proposer un clip vidéo sur la problématique des traces laissées sur internet. Cette vidéo d'abord consultable sur internet a ensuite été diffusée sur 34 chaînes de télévision grâce à l'aide du CSA. L'équivalent budgétaire de cette diffusion est estimé à 340 564 € (HT).

La CNIL a parrainé un *Serious Game* (jeu éducatif) produit par internet sans crainte et lancé le 9 février 2010 à l'occasion du mois de l'internet sans crainte. Ce « thriller » éducatif et interactif évoque les questions de publication et de gestion de son image en ligne sur les réseaux sociaux. Il propose de se projeter dans l'avenir pour voir comment les actions d'aujourd'hui peuvent modifier l'identité numérique de demain.

Enfin, une application disponible sur Iphone et lancée le 28 janvier 2011 à l'occasion de la journée européenne de protection des données, s'adressant aux enfants de 6 à 14 ans, leur propose de découvrir les règles de protection de la vie privée sur internet à travers trois univers : quiz, conseils et dictionnaire d'internet.

La CNIL a aussi souhaité s'adresser spécifiquement aux enseignants et personnels éducatifs en mettant à leur disposition sur le site www.jeunes.cnil.fr un espace dédié comprenant 20 fiches pédagogiques pour animer des ateliers ou proposer des idées de débats ou d'exposés. Qu'est-ce qu'un ami sur un réseau social ? / Téléphone mobile, géolocalisation et publicité ciblée / Partager ses photos / S'inscrire sur un réseau social / Exercer ses droits).



Au-delà de la sensibilisation des jeunes et des enseignants, la CNIL a souhaité rappeler aux chefs d'établissements les règles à respecter lors de la création de fichiers ou de dispositifs de surveillance tels que la biométrie dans les cantines scolaires ou la vidéosurveillance. Un guide « Informatique et Libertés » a donc été envoyé à tous les chefs d'établissement du second degré (collèges et lycées) ainsi qu'aux académies.

Pour accompagner et présenter le lancement de toutes ces actions, la CNIL a participé à de nombreuses conférences ou ateliers de sensibilisation dans les établissements scolaires et dans les académies. Lors de cette vingtaine d'interventions, elle a rencontré les jeunes, les enseignants, les parents d'élèves, les personnels administratifs et les chefs d'établissement. Elle a également conclu des partenariats avec certaines académies afin de former les membres du corps enseignant mais aussi les chefs d'établissement aux problématiques « Informatique et Libertés » et aux responsabilités qui en découlent. Certains de ces partenariats se sont traduits par la création de Commissions locales Informatique et Libertés (CLIL).

LA RÉVISION DU CADRE JURIDIQUE EUROPÉEN : QUEL FUTUR POUR LA VIE PRIVÉE ?

Zoom

La protection des données personnelles : un cadre juridique défini au niveau européen

Le 24 octobre 1995, l'Union européenne a adopté la directive 95/46/CE destinée à harmoniser, au sein des États membres de l'Union, la protection assurée à toute personne de ses données à caractère personnel, quel que soit le lieu où sont opérés les traitements. En France, la loi du 6 janvier 1978 a été largement remaniée par la loi n° 2004-801 du 6 août 2004 transposant en droit français les exigences de cette directive européenne.

À ce jour, les 27 États membres de l'Union, ainsi que les pays de l'Espace économique européen (Islande, Liechtenstein, Norvège), disposent d'une loi « Informatique et Libertés » et d'une autorité de contrôle indépendante. Ces autorités indépendantes se réunissent régulièrement à Bruxelles au sein du « groupe de l'article 29 » dit G29, par référence à l'article de la directive qui l'institue. Le Président de la CNIL, M. Alex Türk, a présidé le G29 de février 2008 à février 2010.

Les défis sont toutefois de plus en plus nombreux et complexes. Ainsi, le cadre juridique européen, s'il reste largement valable, mérite d'être adapté pour prendre en compte certaines évolutions. Il en va ainsi, entre autres :

- du développement fulgurant d'internet et des nouvelles technologies (publicité ciblée, nanotechnologies, puces RFID, dispositif de géolocalisation, informatique en nuages, etc.) et de l'apparition d'un Web participatif dit « Web 2.0 » ;
- de la nécessité de renforcer la responsabilité des entreprises, tout en évitant les lourdeurs administratives ;
- de la nécessité de faciliter les flux transfrontières de données personnelles hors Union européenne, tout en maintenant un haut niveau de protection ;
- de la prise en compte de l'entrée en vigueur du Traité de Lisbonne et de l'intégration des secteurs de la police et de la justice dans un instrument juridique européen.

La révision de la Directive constitue une des priorités stratégiques de la nouvelle Commission européenne, sous l'impulsion de sa vice-présidente, M^{me} Viviane Reding, commissaire en charge de la justice, des droits fondamentaux et de la citoyenneté.

En janvier 2010, M^{me} Reding a annoncé son désir de mettre en place un calendrier ambitieux mais plusieurs membres du G29 ont manifesté leur inquiétude à ce sujet.

La révision du cadre juridique européen : une priorité stratégique de la Commission européenne

Comme le souligne l'article 1^{er} de la loi « Informatique et Libertés », « l'informatique doit respecter l'identité humaine, les droits de l'homme, la vie privée et les libertés ».

Alors même que la majorité des États du monde sont encore totalement dépourvus de cadre juridique pour la protection des données personnelles, l'Union européenne est aujourd'hui à la pointe du combat en faveur d'une protection exigeante et effective de la vie privée des individus. Elle doit le rester et œuvrer pour la promotion de ce droit dans le monde entier.

Zoom

Les diverses initiatives ayant mené à la révision de la directive

Ces dernières années, la CNIL a constaté une augmentation du nombre de projets liés, directement ou indirectement, à la révision de la directive européenne.

Fin 2008, un groupe d'experts avait été constitué par la Commission européenne afin de proposer des mesures permettant de répondre aux nouveaux défis de la protection des données en Europe. Du fait de la composition de ce groupe représentant majoritairement des sociétés américaines, M. Jacques Barrot, alors Vice-président de la Commission européenne, a mis fin à ses activités.

Ce dernier a ensuite organisé une conférence réunissant les grands acteurs de la protection des données, puis a initié une large consultation publique sur les nouveaux défis en matière de protection des données personnelles.

Tenant compte de cette inquiétude, la Commission européenne a décidé d'agir en deux temps : elle a publié une communication sur ses orientations stratégiques en novembre 2010 et elle publiera, d'ici à la fin de l'année 2011, une proposition de cadre législatif européen.

Ce projet de texte sera ensuite examiné par le Parlement européen et le Conseil de l'Union. Ce processus pourrait prendre plusieurs années avant l'adoption finale d'un nouveau texte européen.

Quel(s) instrument(s) juridique(s) ?

La directive européenne définit un cadre pour le rapprochement des législations nationales des États membres, et ce pour avoir un niveau de protection équivalent dans tous les pays. Elle laisse néanmoins une marge d'appréciation aux États membres quant à la manière d'y parvenir. Il apparaît ainsi que de profondes divergences subsistent entre les législations des différents États membres et dans la pratique des diverses autorités de protection des données.

Aussi, comme le propose la Commission européenne, il conviendrait d'harmoniser davantage, à un haut niveau de protection, les règles de protection des données à l'échelon européen.

Il serait ainsi envisagé de s'orienter vers une directive européenne plus précise et détaillée ou alors vers un règlement communautaire, voire vers une combinaison de ces deux instruments.

Par ailleurs, pour prendre en compte l'entrée en vigueur du traité de Lisbonne, il importe de soutenir l'adoption d'un

instrument juridique global, applicable également aux traitements mis en œuvre à des fins répressives, et ce sous réserve de dérogations strictement limitées et appropriées à ce secteur.

Les défis à relever pour le futur de la vie privée

La Commission européenne a publié, le 4 novembre 2010, une communication sur ses orientations stratégiques pour la révision du cadre juridique européen en matière de protection des données.

La CNIL accueille favorablement les grandes orientations de ce document stratégique. Les discussions sur ces différentes orientations et leur traduction en termes juridiques concrets vont certainement susciter d'importantes discussions. Il est toutefois d'ores et déjà possible de mettre en avant un certain nombre de points fondamentaux.

À l'heure de la mondialisation, quel droit appliquer ?

Les critères actuels de détermination du droit applicable, axés sur le lieu d'établissement du responsable de traitement et sur le recours à des moyens de traitement, ne sont pas pleinement satisfaisants. En effet, l'application du droit européen aux grands acteurs de l'internet, délivrant leurs services à des millions de citoyens européens, est parfois contestée. À l'inverse, certains responsables de traitement sont soumis au droit européen, alors même que leur activité ne présente que des liens extrêmement ténus avec le territoire et/ou le public européen.

La Commission européenne va donc proposer de réviser et de clarifier les dispositions existantes.

La Commission souhaite tout d'abord protéger les citoyens européens, dès lors que leurs données personnelles sont traitées, et ce, y compris lorsque les entreprises traitant ces données sont établies uniquement hors Union européenne.

Par ailleurs, au niveau intracommunautaire, il est indispensable de simplifier les règles existantes pour éviter, autant que possible, l'application cumulative de 27 droits nationaux à une même situation. Il convient donc d'être extrêmement vigilant au regard des risques de « forum shopping ». Certaines entreprises et acteurs de l'internet pourraient engager une course au « moins disant » et seraient encouragés à s'implanter dans les pays de l'Union offrant le niveau de protection le plus faible.

Afin d'assurer à la fois la protection des droits fondamentaux des individus et de mettre en place un environnement réglementaire compétitif pour les entreprises, il est fondamental, pour l'avenir, de trouver des solutions raisonnables

et efficaces, préservant certaines compétences nationales. Ainsi, il ne serait pas envisageable qu'une entreprise ciblant spécifiquement des millions de citoyens français ne soit pas soumise au droit français.

Comment renforcer les droits des individus ?

La directive prévoit des principes généraux et des « règles d'or » pour le traitement des données personnelles, ainsi que des droits (accès, opposition, rectification, etc.) qui constituent des garanties pour les individus. Il est toutefois de plus en plus difficile pour les personnes concernées, notamment sur internet, de faire respecter pleinement ces droits.

Aussi, la Commission européenne souhaite-t-elle mettre en avant différentes propositions. Il s'agirait par exemple d'introduire un principe général de transparence pour le traitement des données, impliquant notamment une information des personnes qui soit plus simple, adaptée et accessible. De même, les droits des personnes devraient être gratuits et pouvoir être exercés plus aisément en ligne.

Les règles relatives au consentement des personnes devraient être largement clarifiées et renforcées, afin que les individus puissent garder, de façon effective, le contrôle sur leurs données personnelles.

La notion de donnée sensible pourrait également être élargie, par exemple pour inclure les données génétiques.

La CNIL est, en outre, largement favorable à l'introduction, dans la proposition législative, d'un « droit à l'oubli », qui permettrait une plus grande effectivité dans l'exercice des droits de la personne et une meilleure prise en compte de la réalité d'une « mémoire numérique infaillible », qui, progressivement, remplace une « mémoire humaine limitée dans le temps ». Un tel droit à l'oubli impliquerait notamment de limiter strictement la durée de conservation des données à la réalisation des finalités initialement envisagées. Le droit à l'oubli supposerait d'obtenir la suppression des données personnelles, voire d'en demander la restitution, notamment dans le contexte des moteurs de recherche ou des réseaux sociaux.

Déplacer la protection des données au « cœur » de l'organisme traitant les données personnelles

On constate trop souvent que les entreprises ne mettent pas en œuvre les principes relatifs à la protection des données du fait d'une méconnaissance de leurs obligations.

Il est envisagé d'introduire une obligation générale, pour les responsables de traitement, de prendre les mesures appropriées pour mettre en œuvre les principes relatifs

à la protection des données. Les organismes devront démontrer, à la demande de l'autorité, que ces mesures appropriées ont effectivement été prises. C'est le principe d'*accountability*.

La Commission européenne envisage de rendre les correspondants Informatique et Libertés (CIL) obligatoires, sans toutefois faire peser de charges superflues, notamment sur les petites et moyennes entreprises.

Elle évalue par ailleurs la nécessité de promouvoir certains concepts comme le principe de prise en compte de la vie privée dès la conception (*privacy by design*) ou le principe de vie privée par défaut.

De même, il serait opportun d'introduire une responsabilité des concepteurs et producteurs de technologies et des industriels, afin de les responsabiliser quant aux produits qu'ils mettent en circulation sur le marché. Il faudrait également renforcer et harmoniser la responsabilité du sous-traitant en précisant davantage les obligations qui lui incombent.

Simplifier les formalités administratives

En ce qui concerne la réduction de la charge administrative, la Commission européenne indique vouloir simplifier et harmoniser le système actuel de notification.

Du point de vue de la CNIL, le régime de la déclaration, pour les traitements les plus courants ou posant peu de risques pour la vie privée, devrait ainsi progressivement être abandonné. En revanche, il est indispensable de conserver un régime de contrôle préalable fort, c'est-à-dire un régime d'autorisation, pour les traitements dits « à risques » comme par exemple pour le traitement des données se rapportant au corps humain, aux fichiers de sécurité publique, à certaines données sensibles, etc.

D'un point de vue plus pratique, il serait également souhaitable d'encourager l'accomplissement des formalités en ligne et surtout, dans une optique d'harmonisation, d'encourager la mise en place d'un formulaire d'enregistrement uniforme, valable dans toute l'Union. La mise en place d'un « guichet unique » pour toute l'Union pour l'accomplissement de ces formalités serait également une évolution positive.

Favoriser les transferts internationaux dans le respect des principes de protection des données

La Commission européenne veut améliorer et rationaliser les règles concernant les transferts de données en dehors de l'Union européenne. Il apparaît ainsi souhaitable de mettre pleinement en œuvre les outils existants (adéquation, *Safe Harbor*, clauses contractuelles, etc.) pour faciliter, sans baisser d'aucune manière le niveau de protection des individus.

La CNIL propose également d'intégrer, dans la proposition législative, les BCR (*Binding Corporate Rules*, qui sont

des codes de conduite applicables aux sociétés d'une multinationale), afin qu'ils deviennent un outil d'encadrement des transferts reconnu formellement, et ce suivant un mécanisme de reconnaissance mutuelle entre autorités européennes.

Au niveau mondial, la CNIL estime également qu'il est fondamental de déployer tous les efforts utiles pour élaborer un instrument juridique international contraignant dans le domaine de la protection des données, et ce pour pallier l'absence de cadre juridique dans la majorité des États du monde. À cet égard, les initiatives de la Conférence internationale des commissaires à la protection des données, définissant dans leur résolution de Madrid un corpus de principes communs applicables dans le monde entier, doivent être soutenues. Il en va de même des initiatives visant à moderniser la Convention 108 du Conseil de l'Europe, notamment pour la faire émerger comme un instrument mondial.

Zoom

Pour en savoir plus sur la révision de la directive 95/46/CE

La CNIL est pleinement investie sur ce dossier majeur de la révision de la directive. Elle a notamment été largement associée, dans le cadre du G29 et de façon bilatérale, aux diverses phases de consultation menées par la Commission européenne.

Ainsi, divers documents ont été préparés et permettent d'avoir davantage d'éléments sur la position de la CNIL et du G29 :

- l'avis du G29 sur le futur de la vie privée (WP168);
- l'avis du G29 (3/2010) sur le principe de responsabilité (*accountability principle*) (WP173);
- l'avis du G29 (8/2010) sur le droit national applicable (WP179);
- la lettre du G29 en date du 14 janvier 2011 adressée à M^{me} Reding sur les orientations stratégiques de la Commission européenne.

Par ailleurs, le G29 a adopté trois documents de travail sur les données sensibles, les formalités préalables et la coopération entre autorités. Un avis sur la notion de consentement est en préparation.

L'ensemble de la documentation disponible se trouve sur la page pertinente du site Europa : http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

Renforcer le rôle des autorités nationales de protection des données personnelles et du groupe des CNIL européennes (G29)

La Commission européenne souhaite renforcer, clarifier et harmoniser le statut et les pouvoirs des autorités de protection des données, y compris pour préciser plus avant les exigences en termes d'indépendance des autorités. Par ailleurs, elle voudrait améliorer la coopération et la coordination entre autorités, en particulier sur les sujets ayant une dimension transfrontière.

Il est en outre essentiel que les États membres fournissent des moyens suffisants aux autorités afin d'accomplir les missions qui leur sont confiées ou d'harmoniser « vers le haut » les compétences et pouvoirs de ces autorités.

Par ailleurs, le rôle du groupe de travail de l'article 29 (G29) doit être renforcé, afin que ce dernier puisse véritablement jouer son rôle de pilote de la vie privée en Europe, voire dans le monde. En tout état de cause, il apparaît indispensable de garantir l'impartialité et la transparence des activités du G29, qui doit disposer d'une autonomie juridique, administrative et financière.

De quoi s'agit-il ?

Le G29

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail des 27 CNIL européennes. Il a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ. Environ 15 sous-groupes composés des collaborateurs des CNIL européennes se réunissent régulièrement à pour alimenter les réflexions des membres du G29 en séance plénière et rédiger les avis qui leur seront ensuite soumis pour adoption.

LES NOUVEAUX POUVOIRS DE CONTRÔLE DE LA VIDÉOPROTECTION

Les constats relevés grâce aux contrôles

Dans le cadre de son programme annuel pour l'année 2010, la CNIL avait inscrit le contrôle des dispositifs de vidéosurveillance relevant de la loi « Informatique et Libertés ». Elle a ainsi effectué plus de 55 contrôles concernant ces dispositifs.

Ces contrôles ont majoritairement été réalisés dans le cadre de l'instruction de plaintes et ont permis à la formation contentieuse de dégager une première orientation en matière de proportionnalité de dispositifs de vidéosurveillance filmant des salariés sur leur lieu de travail.

Les constats effectués à l'occasion de ces contrôles peuvent se résumer par les chiffres suivants.

Nombre de contrôles	55
Absence de déclaration CNIL ou déclaration incomplète	23
Dispositif disproportionné (surveillance permanente des salariés concernés)	27
Durée excessive de conservation des images	10
Défaut d'information des personnes	38
Défaut de sécurité	14

Comment peut-on analyser ces chiffres ?

- En premier lieu, on relève que l'ensemble des finalités constatées a pour objet la sécurité des personnes et des biens.

Sur 27 dispositifs jugés excessifs, 6 (soit 10% des contrôles effectués) étaient délibérément orientés sur des salariés. Or, la mise en œuvre d'un dispositif de vidéosurveillance ne peut pas avoir pour seule finalité la surveillance des salariés.

Dans les 21 autres cas (soit 38% des contrôles effectués), les dispositifs avaient pour finalité d'assurer la sécurité des biens (marchandise, etc.) mais filmaient également des postes de travail de salariés qui n'étaient pas en contact avec la marchandise à protéger.

Avec ces décisions, la CNIL a établi une doctrine en matière de mise en œuvre de dispositifs de vidéosurveillance sur les lieux de travail. **La mise en œuvre de dispositifs de vidéosurveillance destinés à lutter contre le vol est acceptable, sous certaines conditions :**

- les zones sans rapport avec la finalité de lutte contre le vol ne doivent pas être filmées. Il peut s'agir notamment des zones de repos, des zones de travail sans présence de la marchandise. La marchandise peut être filmée – éventuellement les salariés qui la manipulent – mais pas les salariés en tant que tels ;
- la CNIL apprécie également la légitimité du dispositif : la lutte contre le vol ne doit viser que les marchandises en lien avec l'activité de l'entreprise concernée (ce qui permet d'éviter une lutte trop « générique » : lutte contre le vol de papiers, de crayons, etc.) ;
- enfin, si des moyens alternatifs existent déjà (armoires fortes, sécurité des locaux), le recours à des dispositifs de vidéosurveillance ne paraît plus indispensable.

- En deuxième lieu, les manquements aux obligations liées aux formalités déclaratives concernent 49% des organismes contrôlés.

Ce chiffre s'explique par la réalisation de contrôles auprès d'établissements mettant en œuvre des dispositifs filmant, pour partie, la voie publique ou les zones ouvertes au public relevant de la loi du 21 janvier 1995 et, pour partie, des lieux privés (entrepôts, salles réservées au personnel, etc.) qui, eux, relèvent de la loi « Informatique et Libertés ». La dualité de régime juridique, et la confusion en résultant, est le plus souvent la cause de ce manquement car il n'est pas toujours aisé d'apprécier quel est le régime applicable.

- En troisième lieu, le manquement à l'information des personnes a été relevé dans 69% des cas. Celui-ci s'explique dans la majeure partie des cas par la méconnaissance de cette obligation, conséquence de l'absence de formalités préalables, ou par des informations délivrées non conformes ou incomplètes (exemple : présence de pictogrammes dépourvus des mentions d'informations prévues par la loi).

- En quatrième lieu, le manquement à la nécessité de définir des durées de conservation limitées a été constaté dans 18% des établissements contrôlés. Ce chiffre, satisfaisant au demeurant, s'explique davantage par des raisons techniques de capacité de stockage d'images en base, permettant rarement une durée de conservation supérieure à 30 jours, que par une réelle politique de purge des données.

Enfin, il apparaît que 32% des organismes, pour l'essentiel des grandes surfaces commerciales, filmaient les aires de stationnement et leurs stations services. Ces dispositifs, dotés de caméras mobiles à agrandissement,

ont la faculté de filmer à 360 degrés autour du magasin, englobant ainsi la voie publique et les habitations avoisnantes dès lors qu'aucun masquage ou floutage n'est mis en œuvre.

Le bilan 2010 des contrôles « vidéosurveillance » se traduit par l'adoption de 14 mises en demeure (25,5%), la rédaction de 20 courriers de clôture (36,5%) et de 21 courriers d'observation (38%).

La CNIL précise les règles permettant la mise en œuvre de la vidéosurveillance dans les établissements scolaires

Certains établissements scolaires utilisent maintenant depuis de nombreuses années la vidéoprotection afin de renforcer la sécurité de leurs abords. Ces dispositifs, parce qu'ils filment la voie publique, doivent être autorisés par le préfet.

La CNIL a reçu, au cours de l'année 2011, des plaintes d'associations de parents d'élèves ou d'enseignants concernant l'installation de caméras au sein même des établissements scolaires et non plus seulement sur la voie publique.

Lors de ses contrôles auprès de certains des établissements mis en cause, la CNIL a constaté que ces caméras - qui peuvent être installées pour protéger les biens ou les personnes, lutter contre la fugue ou le tabagisme - filment les lieux de vie de ces établissements tels que les cours de récréation, les préaux, les jardins ou les foyers des élèves.

La CNIL n'a pas d'opposition de principe à l'installation de caméras dans les établissements scolaires. En effet,

celles-ci sont destinées avant tout à assurer la sécurité des élèves.

Cependant les contrôles ont montré que l'orientation de certaines caméras était inadéquate notamment lorsqu'elles filment en permanence « les lieux de vie » permettant une surveillance permanente des personnes qui s'y trouvent, qu'il s'agisse des élèves ou des enseignants.

Cette collecte excessive de données a conduit le président de la CNIL à mettre en demeure cinq de ces établissements de modifier leur système qui, tel qu'il est conçu, porte atteinte aux libertés des élèves et personnels de l'établissement scolaire, en les filmant en continu (article 6.3° de la loi « Informatique et Libertés »).

En effet, la sécurisation des biens et des personnes peut être obtenue par la mise en œuvre de moyens moins intrusifs : sécurisation renforcée des accès par exemple, ou configuration du dispositif de vidéosurveillance qui peut être limité aux seuls accès de l'établissement.

Seules des circonstances exceptionnelles – établissements scolaires victimes d'actes de malveillance fréquents et répétés – peuvent justifier que des élèves et des enseignants soient filmés en continu.

La Commission a également vérifié si les élèves, leurs parents et les personnels étaient bien informés de l'existence de ces dispositifs et de leur finalité, ce qui n'était pas toujours le cas.

Un pouvoir de contrôle étendu

La loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), promulguée le 14 mars 2011, confie dorénavant à la CNIL un pouvoir de contrôle de tous les dispositifs de vidéoprotection installés sur le territoire national, y compris ceux installés sur la voie publique, qui relèvent de la loi du 21 janvier 1995.

Il est rapidement apparu à notre Commission que le mécanisme d'autorisation préfectorale préalable créé en 1995 n'était pas suffisant : d'une part, parce qu'il ne concerne que les dispositifs dont le préfet a connaissance et, d'autre part, parce que les dispositifs effectivement en place peuvent ne pas respecter, volontairement ou non, le cadre fixé par l'autorisation préfectorale.

À l'issue d'un contrôle, la CNIL peut mettre en demeure les responsables de ces systèmes, si elle constate des manquements aux obligations qui s'imposent à eux (information du public, respect de la durée de conservation des enregistrements, limitation des destinataires des images, etc.). Elle peut enfin proposer au préfet d'ordonner des mesures de suspension ou de suppression du système contrôlé.

Ces nouvelles compétences étaient réclamées par le Parlement. Ainsi, le rapport des sénateurs COURTOIS et GAUTIER prônait, depuis 2008, dans un souci d'efficacité, la compétence de la CNIL en matière de vidéosurveillance.

La position de la CNIL quant aux conditions de développement des dispositifs de vidéoprotection est pragmatique et met en avant le critère de proportionnalité : s'il appartient aux pouvoirs publics compétents de décider le déploiement ou non de caméras, celui-ci doit impérativement s'effectuer dans le respect des droits et libertés de nos concitoyens.

Cette position a été confirmée par une étude, réalisée à la demande de la CNIL, qui avait montré que si 71 % des Français étaient favorables au développement des dispositifs de vidéoprotection, 79 % d'entre eux ne l'étaient qu'à la condition que l'on garantisse leurs droits individuels.

La CNIL réunit différents atouts qui sont essentiels pour exercer ce type de contrôles. En effet, elle jouit de réelles garanties d'indépendance, bénéficie d'une longue pratique des problématiques liées à la vidéoprotection et dispose d'un corps de contrôleurs de métier (juristes, informaticiens et ingénieurs).

La CNIL se félicite donc de l'extension de ses pouvoirs de contrôle par le législateur et entend assumer pleinement la responsabilité qui lui a été confiée.

Le programme de contrôles

La CNIL se mobilise déjà pour faire pleine application de ces nouvelles dispositions, puisque **150 contrôles ont été programmés, pour la seule année 2011 et sur l'ensemble du territoire national**, sur les dispositifs de vidéoprotection. Ils permettront d'avoir une vision générale des modalités de mise en œuvre de ces systèmes.

Les contrôles réalisés par les équipes de la CNIL porteront principalement sur les destinataires des images, leur durée de conservation ainsi que sur la sécurité du système. Ces contrôles permettront également de s'assurer que la configuration du dispositif est en adéquation avec l'autorisation obtenue afin de vérifier, notamment, que des parties privatives (intérieur de maisons, jardins, etc.) ne sont pas illégalement filmées. Enfin, une attention toute particulière sera portée à la vérification d'une correcte information des personnes, gage de transparence.

Les contrôles qui seront effectués par la CNIL sur l'ensemble du territoire national permettront également de garantir un niveau uniforme de protection des libertés individuelles et publiques, quelle que soit la situation géographique de nos concitoyens. Ces contrôles seront d'autant plus efficaces et pertinents que notre Commission pourra être saisie par toute personne s'estimant victime d'une difficulté tenant au fonctionnement d'un système de vidéoprotection.

Relevons que notre Commission est investie par la loi « Informatique et libertés » d'une mission de vigilance et d'alerte quant à l'évolution des technologies de l'information et des conséquences qui en résultent pour l'exercice des droits et libertés. Le contrôle des dispositifs de vidéoprotection lui permettra d'observer de façon privilégiée le développement des technologies relatives au traitement de l'image des personnes (biométrie, reconnaissance faciale, etc.) afin, le cas échéant, d'émettre des recommandations.

S'il est en effet illusoire de vouloir contrôler l'ensemble des dispositifs de vidéoprotection, il conviendra néanmoins que la CNIL puisse contrôler un pourcentage raisonnable de ceux-ci. Cet objectif est à mettre en perspective avec les 400 000 caméras installées en France qui relèvent du régime de la loi de 1995, dont environ 33 000 sur la voie publique (avec un objectif de 45 000 fin 2011, selon le ministre de l'Intérieur). Et ces chiffres sont en constante augmentation...

Afin que la CNIL puisse mener à bien cette mission confiée par le législateur, notre Commission souhaite que cette extension de compétence s'accompagne d'un accroissement de ses moyens.

PROSPECTIVE ET INNOVATION : UNE PRIORITÉ STRATÉGIQUE POUR LA CNIL

La création, en janvier 2011, de la Direction des études, de l'innovation et de la prospective (DEIP) répond à une orientation stratégique nouvelle de notre institution. La CNIL poursuit une démarche innovante et originale puisqu'elle est ainsi la première autorité de protection des données en Europe à se doter en propre d'une direction de la prospective. Cette direction dispose d'un budget spécifique pour commander et conduire des études notamment dans les domaines des sciences humaines et de l'économie et également d'un laboratoire de tests. Parmi les autorités de protection des données, seul le Commissariat à la vie privée du Canada (*cf. gros plan*) dispose d'une structure analogue.

Comme l'a expliqué le Président de la CNIL, « il s'agit de faire face aux nouvelles responsabilités qui nous incombent dans un contexte de développement massif et accéléré des nouvelles technologies et de leurs applications, susceptibles d'avoir des incidences sur le régime de nos libertés individuelles et sur la protection des données personnelles. C'est un projet prioritaire et enthousiasmant car cette nouvelle direction sera le fer de lance de la deuxième impulsion que je souhaite donner à la politique de notre Commission, dans la droite ligne de la loi du 6 août 2004 ».

La création d'une direction de la prospective à la CNIL : quelle vision pour l'institution ?

Développer la prospective à la CNIL, c'est analyser les nouveaux usages des technologies, mieux comprendre les innovations technologiques et leurs interfaces avec d'autres dimensions de la vie en société (juridiques, économiques, sociologiques) et en évaluer l'importance potentielle pour la protection des données personnelles et la vie privée.

Dans ce cadre, il s'agit, pour notre Commission, de « se placer au cœur des débats en tant qu'éclairer » et donc de fortement développer, dans tous les domaines qui la concernent, la veille prospective et, de fait, sa capacité d'anticipation.

Mieux identifier les évolutions, à court, moyen et long terme, dans tous les domaines qui relèvent de sa compétence et ainsi l'éclairer dans ses décisions et modes d'intervention, tel est l'objectif de cette nouvelle direction.

Développer la veille prospective

Cette mission consistera à assurer une veille de l'institution sur des thématiques nouvelles ou émergentes jugées prioritaires ainsi qu'une veille sur les programmes de recherche des grands acteurs (organismes de recherche, industriels, opérateurs de services, développeurs de logiciels).

C'est ainsi qu'a été décidée la mise en place d'une nouvelle politique de gestion de la connaissance, de diffusion en interne de l'information et de la documentation, pierre angulaire d'une véritable veille prospective. Une base documentaire de veille sur les thématiques prospectives intéressant la protection des données personnelles sera également constituée.

Pour mieux valoriser les travaux et les études conduits par la CNIL dans le domaine de la veille et de la prospective, faciliter le rapprochement avec le monde académique et industriel et accroître ainsi la visibilité de la CNIL, un certain nombre de productions sont envisagées tant en interne qu'en externe et notamment des notes de veille à destination du grand public.

Le pilotage d'études prospectives

Par la commande ou l'achat d'études extérieures, la CNIL entend développer plus fortement une approche **pluridisciplinaire – notamment économique, sociologique et philosophique** – des enjeux de protection des données et non pas seulement juridique ou technologique. Ceci constitue une réelle nouveauté qui permettra incontestablement d'enrichir et d'élargir les analyses de la Commission. C'est aussi l'occasion pour la CNIL d'être plus « visible » auprès de certains acteurs, de développer son influence dans le monde académique et de valoriser ses actions.

Le programme d'études pour 2011

Pour 2011, compte tenu de la création récente de cette direction et des ressources disponibles, deux grandes études prospectives seront conduites.

La première étude concerne l'écosystème des *Smartphones* et les transformations des usages.

En effet, on assiste à un véritable « boom » de ces « terminaux » avec près de 297 millions de *smartphones* vendus dans le monde en 2010⁸), et à une explosion des usages (suivi des activités, paiement sans contact, géolocalisation, etc.). Il est essentiel de s'intéresser au positionnement et d'identifier des acteurs clés (Apple, Google, Nokia, Microsoft...), les risques émergents (récupération de données, failles de sécurité), ainsi que les impacts potentiels sur la vie privée.

Par ailleurs, un chantier prospectif relatif à « la vie privée, les libertés et les données personnelles à l'horizon 2020. Quels enjeux pour la régulation et la CNIL », sera prochainement lancé. La question de fond est celle de savoir si la notion de vie privée est en voie d'être redéfinie par les usagers des nouvelles technologies. Ce chantier se déroulera sur plusieurs mois et consistera notamment à rencontrer un certain nombre d'acteurs clés qui apporteront ainsi leur vision de cette problématique. Ceci donnera lieu ensuite à un séminaire de réflexion ouvert aux parties prenantes ainsi qu'à des publications.

Le développement de partenariats de recherche

Il est aussi envisagé de développer des relations privilégiées avec certains organismes de recherche publique

tels que le CEA, l'INRIA ou le CNRS qui pourraient aussi se formaliser par des conventions, permettant ainsi un partage des connaissances et des compétences.

Des relations plus suivies peuvent aussi être construites avec les industriels qui disposent de ressources internes importantes en matière de recherche et développement ceci, bien entendu, en s'entourant des précautions nécessaires pour préserver l'indépendance de notre institution.

De même s'agissant des grandes écoles, il est apparu intéressant d'envisager, là aussi sous forme d'une convention, un partenariat permettant non seulement d'améliorer la connaissance de la loi « Informatique et Libertés » dans les grandes écoles mais aussi la réalisation d'études sur des thèmes intéressant la protection des données personnelles.

En outre, le Conseil général des technologies de l'information (CGIET) interroge chaque année la CNIL sur des thèmes d'étude à envisager. Les sujets retenus cette année portent sur la géolocalisation sur mobile.

Enfin, il peut être tout à fait opportun, de façon ponctuelle, de mutualiser les efforts notamment de financement sur des sujets d'intérêt commun : un premier exemple en est donné avec un sondage lancé en juin 2011 par l'UNAF en partenariat avec Action Innocence et la CNIL sur l'usage des réseaux sociaux chez les jeunes.

La mise en place et l'animation d'un réseau d'experts : vers un think tank de prospective ?

Il importe de structurer, autour des problématiques informatique et libertés, tant au niveau national qu'international, un réseau d'experts multidisciplinaires. Il pourrait être envisagé, à terme, un *think tank* de prospective ou « boîte à idées », apportant à la Commission des éclairages nouveaux. Des séquences d'auditions et de travail collectif pourraient ainsi être organisées de manière ouverte pour explorer les transformations économiques, sociales, technologiques intéressant la CNIL.

Les relations avec les réseaux de prospective devront aussi être développées de même qu'avec l'office parlementaire d'évaluation des choix technologiques et scientifiques.

Innover et expérimenter

- **Doter la CNIL d'un laboratoire interne de tests techniques**

Dans le cadre de cette mission, est créé un laboratoire, doté de moyens informatiques dédiés, pour tester et expérimenter, en réel, des produits et applications innovantes.

8. Chiffres Institut Gartner.

Il s'agit ainsi de :

- disposer des nouveaux produits le plus en amont possible de leur commercialisation afin d'en tester les fonctionnalités, et en évaluer leurs impacts sur la protection de la vie privée ; également tester de façon plus systématique certains matériels ou logiciels décrits dans le cadre des formalités préalables (exemple : nouveau dispositif biométrique) ou récemment mis sur le marché ;
- diffuser une culture technologique et une pédagogie des risques pesant sur la protection de la vie privée ;
- dans une logique de *privacy by design*, renforcer la mission de conseil auprès des entreprises en matière d'intégration des exigences de protection des données personnelles dans leur processus de développement technologique ;
- contribuer au développement de solutions technologiques protectrices de la vie privée ;
- renforcer la crédibilité technique et la capacité d'influence de la CNIL, notamment dans les communautés techniques et scientifiques ;
- réaliser des analyses techniques poussées sur des sujets précis à des fins, par exemple, de publication dans des revues spécialisées ;
- à terme, le rôle ou non d'un tel laboratoire dans le processus de labellisation et de certification méritera d'être précisé.

- **Développer un « laboratoire-démonstrateur » à visée pédagogique**

Il est envisagé de développer des outils à destination du grand public pour mieux protéger la vie privée et tester la faisabilité de solutions nouvelles protectrices de la vie privée.

Il s'agira aussi de suivre, voire d'accompagner (*privacy by design*), des produits ou des applications innovants, par exemple :

- des expérimentations soumises à la CNIL (tels que des systèmes de paiement sans contact avec authentification biométrique ou encore le dispositif biométrique de reconnaissance faciale en temps réel des personnes volontaires dans un stade ;
- des projets de recherche.

Il sera également utile de procéder à des visites de centres recherche et développement. La CNIL s'est déjà engagée dans cette voie comme en témoignent les visites déjà organisées dans le passé à l'Échangeur, au MINATECH de Grenoble, au *show room* biométrie de la société MORPHO (biométrie) et au laboratoire de recherche d'IBM à la Gaude.

Enfin, le développement de partenariats tels que ceux précédemment évoqués (ex. : CEA, INRIA...), ainsi que la participation à certains comités de pilotage de l'Agence

nationale de la recherche (ANR), devrait aussi permettre à la CNIL d'avoir une meilleure visibilité sur les projets technologiques innovants.

- **Renforcer le conseil et la réflexion stratégique**

En conclusion, la direction de la prospective pourra à terme apporter l'éclairage prospectif, indispensable pour contribuer à la préparation des positions stratégiques de la CNIL au regard des évolutions technologiques, des usages et des nouveaux modes de régulation de protection des données.

De quoi s'agit-il ?

La direction de la recherche du Commissariat à la vie privée du Canada

En 2004, le Commissariat à la vie privée du Canada a créé une direction de la recherche qui a pour mission d'effectuer des recherches sur les enjeux relatifs à la protection de la vie privée et à la technologie et d'administrer le programme de recherche.

L'objectif de ce programme annuel de recherches et de sensibilisation du public (programme dit de contributions, publié sur le site du Commissariat) est d'encourager, par un financement conséquent (budget annuel 500 000 \$) le développement d'une capacité nationale de recherche sur la protection de la vie privée.

Depuis sa création, 2 millions \$ ont ainsi été alloués à plus de 60 projets au Canada.

Les études font l'objet de publications tant sur le site web de l'autorité canadienne que sous forme de brochures largement diffusées (par exemple sur les réseaux sociaux, la biométrie, etc.).

Le programme 2011-2012 est axé sur quatre domaines prioritaires :

- l'intégrité et la protection de l'identité ;
- la technologie de l'information ;
- la génétique et la protection de la vie privée ; la sécurité publique.

Un comité consultatif externe, composé d'experts-conseils spécialisés dans le domaine des renseignements personnels, d'universitaires et de praticiens du secteur public, fournit des conseils sur les orientations stratégiques du Commissariat.

Par ailleurs, la direction des recherches dispose d'un laboratoire de tests depuis septembre 2010.

ANNEXES





LES MEMBRES DE LA CNIL

Le bureau

Président

Alex TÜRK, sénateur du Nord
Membre de la CNIL depuis 1992, président de l'autorité de contrôle Schengen de 1995 à 1997, de l'autorité de contrôle commune d'Europol (2000-2002), de l'autorité de contrôle d'Eurodac (2003) et vice-président de la CNIL de 2002 à 2004, Alex Türk est élu président de la CNIL le 3 février 2004. Il a été président du G29 de février 2008 à février 2010.

Vice-président délégué

Emmanuel de GIVRY, conseiller honoraire à la Cour de cassation

Secteur: Ressources humaines

Emmanuel de Givry est membre de la CNIL depuis février 2004, puis vice-président délégué depuis février 2009.

Vice-président

Isabelle FALQUE-PIERROTIN, conseiller d'État

Secteur: Groupe de l'article 29 – Administration et vote électronique

Isabelle Falque-Pierrotin est membre de la CNIL depuis janvier 2004 et vice-président depuis février 2009.

Les membres (commissaires)

Jean-Paul AMOUDRY, sénateur de la Haute-Savoie

Secteur: Banques et crédit

Jean-Paul Amoudry est membre de la CNIL depuis janvier 2009.

Jean-François CARREZ, président de chambre honoraire à la Cour des comptes

Secteur: Éducation et enseignement supérieur

Jean-François Carrez est membre de la CNIL depuis janvier 2009. Il est membre élu de la formation contentieuse.

Dominique CASTERA, membre du Conseil économique, social et environnemental

Secteur: Coopération policière internationale – Vie associative

Dominique Castera est membre de la CNIL depuis octobre 2010.

Jean-Marie COTTERET, professeur émérite des universités

Secteur: Police nationale et sûreté de l'État

Jean-Marie Cotteret est membre de la CNIL depuis janvier 2004. Il est membre élu de la formation contentieuse.

Claire DAVAL, avocate

Secteur: Justice

Claire Daval est membre de la CNIL depuis février 2009. Elle a été élue présidente de la formation contentieuse.

Claude DOMEIZEL, sénateur des Alpes-de-Haute-Provence

Secteur: Développement durable et logement

Claude Domeizel est membre de la CNIL depuis décembre 2008. Il est membre élu de la formation contentieuse.

Didier GASSE, conseiller maître à la Cour des comptes

Secteur: Télécommunications et internet

Didier Gasse est membre de la CNIL depuis janvier 1999. Il est le représentant de la France au sein de l'autorité de contrôle Eurojust.

Philippe GOSSELIN, député de la Manche

Secteur: Questions fiscales et sociales

Philippe Gosselin est membre de la CNIL depuis juin 2008.

Sébastien HUYGHE, député du Nord

Secteur: Identité, défense et affaires étrangères

Sébastien Huyghe est membre de la CNIL depuis juillet 2007. Il est membre élu de la formation contentieuse.

Jean MASSOT, président de section honoraire au Conseil d'État

Secteur: Santé et assurance-maladie

Jean Massot est membre de la CNIL depuis avril 2005.

Marie-Hélène MITJAVILE, conseiller d'État

Secteur: Recherche et statistiques

Marie-Hélène Mitjavile est membre de la CNIL depuis janvier 2009.

Éric PERES, membre du Conseil économique, social et environnemental

Secteur: Transports et assurance des biens

Éric Peres est membre de la CNIL depuis décembre 2010.

Bernard PEYRAT, conseiller honoraire à la Cour de cassation

Secteur: Commerce et marketing

Bernard Peyrat est membre de la CNIL depuis février 2004.

Dominique RICHARD, consultant

Secteur: Affaires culturelles et sportives

Dominique Richard est membre de la CNIL depuis janvier 2009. Il est membre élu de la formation contentieuse.

Commissaires du gouvernement

Élisabeth ROLIN

Catherine POZZO DI BORGIO, adjointe

LES SERVICES DE LA CNIL AU 4 MAI 2011

Secrétaire général

Yann PADOVA

DIRECTION DES ÉTUDES DE L'INNOVATION
ET DE LA PROSPECTIVE

DIRECTION DES AFFAIRES JURIDIQUES,
INTERNATIONALES ET DE L'EXPERTISE

DIRECTION DES RELATIONS AVEC LES USAGERS ET DU CONTRÔLE

DIRECTION DES RESSOURCES HUMAINES,
FINANCIÈRES, INFORMATIQUES ET LOGISTIQUES

LES MOYENS DE LA CNIL

Le personnel

La CNIL dispose en 2010 de 148 postes budgétaires, soit 85% de plus qu'en 2004 (80 postes). La création de 16 postes supplémentaires par rapport à 2009 représente une augmentation annuelle de plus de 12% des effectifs.

L'année 2010 confirme la tendance à l'augmentation régulière des personnels de la CNIL, qui s'est amorcée en 2004 avec la réforme de la loi « Informatique et Libertés ».

L'augmentation constante des effectifs depuis 2004 est la réponse à cet accroissement très sensible des missions confiées par le législateur : contrôles, sanctions, animation du réseau des correspondants, conseil, pédagogie auprès du grand public, autorisation des fichiers les plus sensibles, labellisation, veille et expertise informatique, etc. Les postes supplémentaires créés ont ainsi permis à la Commission de répondre en partie, d'une part, au fort accroissement de son activité et, d'autre part, à la nécessaire modernisation de son organisation, induite notamment par ses nouvelles missions.

Par ailleurs, le renforcement des moyens en personnels permet, peu à peu, de hisser les effectifs de la CNIL au niveau de ceux de ses homologues européens et des principales autorités administratives indépendantes nationales. L'autorité britannique dispose de 275 agents et l'autorité espagnole de 185 personnes pour une population d'environ 40 millions d'habitants.

Les crédits

Le budget global de la Commission a augmenté de 126% entre 2004 et 2010, répondant ainsi à l'augmentation

importante des missions de la CNIL. L'accroissement du budget global est de plus de 13% par rapport à 2009.

L'évolution de la dotation budgétaire est cependant différente selon les types de crédit qui composent le budget de la Commission.

Les crédits de personnel représentent 63% budget global. Ils ont augmenté de 12% par rapport à 2009, compte tenu notamment de l'obtention de postes budgétaires supplémentaires.

Les crédits de fonctionnement ne représentent que 37% du total. Ils ont augmenté de 15% par rapport à 2009.

Il convient de noter que, depuis 2004, l'augmentation des crédits de fonctionnement ne suit pas systématiquement celle des crédits de personnels. Ainsi, après la forte hausse de 2006, liée à la concrétisation du projet de déménagement de la CNIL sur un site unique, le budget de fonctionnement a augmenté à un rythme moins rapide que les crédits de personnels.

Ceci signifie que la Commission a mené des efforts de rationalisation et a cherché à faire des économies, bien qu'elle se situe dans le contexte d'un accroissement constant de son activité. Ainsi, le ratio des dépenses de fonctionnement par agent, hors dépenses d'immobilier, est constant entre 2004 et 2010.

On peut également souligner que l'augmentation du budget de fonctionnement obtenue en loi de finances initiale 2010, d'environ 698 000 €, a été amputée en gestion de près de 248 000 €. Ceci s'inscrit dans le cadre des mesures de précaution prévues par la loi organique relative aux lois de finances (LOLF) et pour l'abondement du « fonds État exemplaire » qui est un prélèvement opéré sur les moyens de fonctionnement de chaque ministère, susceptible d'être reversé en cas d'atteinte des objectifs de performance environnementale de l'État.

Évolution des moyens de la CNIL (loi de finances initiale)

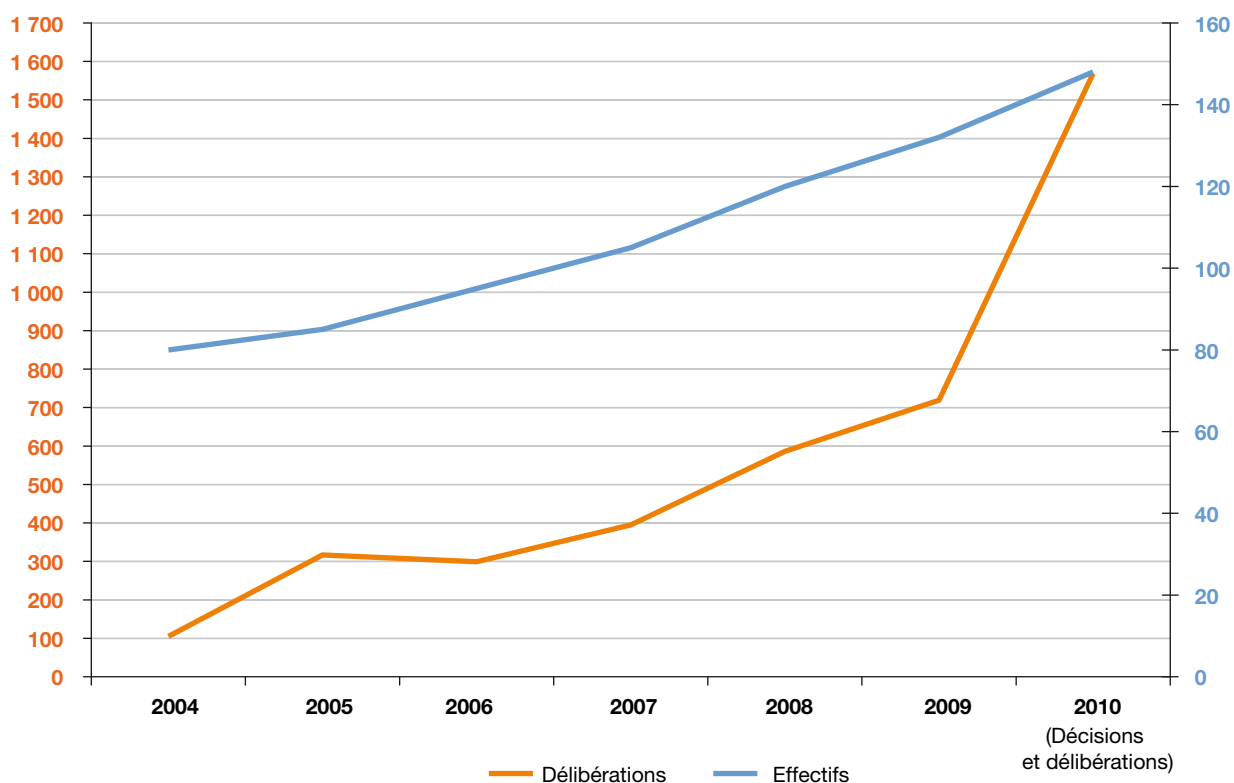
	2004	2005	2006	2007	2008	2009	2010	Évolution 2010-2004	
								en nombre	en %
Postes	80	85	95	105	120	132	148	68	85%
Crédits (en M€)	6,5	7,2	9,0	9,9	11,4	13,0	14,7	8,2	126%
- dont personnels	4,2	4,7	5,3	6,1	7,2	3,3	9,3	5,1	121%
- dont fonctionnement	2,3	2,5	3,7	3,8	4,2	4,7	5,4	3,1	135%

Évolution des moyens de la CNIL (loi de finances initiales)

Les moyens alloués à la CNIL ont augmenté de manière significative pour répondre aux nouvelles missions qui lui ont été confiées depuis 2004, démontrant ainsi l'attachement du gouvernement à l'action de notre autorité. Mais un effort est encore nécessaire pour rejoindre les pays de taille comparable en Europe.

Cette augmentation de moyen s'est traduite par une croissance bien supérieure de la « production » de la CNIL mesurée à l'aune des décisions et délibérations. En 2004, la CNIL avait adopté 105 délibérations contre 1569 décisions et délibérations adoptées en 2010, soit 1400% d'augmentation.

Évolution des délibérations et des effectifs



LISTE DES ORGANISMES CONTRÔLÉS EN 2010

ASSOCIATION

ASSOCIATION ESPOIR CENTRES FAMILIAUX JEUNES
ASSOCIATION JURICOM & ASSOCIÉS
ASSOCIATION LEXEEK
ASSOCIATION NORD FRANCE ET MER

ASSURANCE

AUTOFIRST
CHARTIS EUROPE
FAC INTERNATIONAL
VERSPIEREN

BANQUE

BANQUE POPULAIRE DU NORD
BNP PARIBAS
BPCE
CAISSE D'ÉPARGNE ET DE PRÉVOYANCE ÎLE-DE-FRANCE
CAISSE D'ÉPARGNE RHÔNE-ALPES
FINANCO

COLLECTIVITÉS LOCALES

COMMUNE D'ARGENTEUIL
COMMUNE D'AUCH
COMMUNE DE PARIS
COMMUNE DU CROTOY
COMMUNE DE VILLENEUVE-LE-ROI
CONSEIL GÉNÉRAL DE CORSE DU SUD
CONSEIL GÉNÉRAL DES CÔTES-D'ARMOR
CONSEIL GÉNÉRAL DU VAL-D'OISE

COMMUNICATIONS ÉLECTRONIQUES – NOUVELLES TECHNOLOGIES

GOOGLE FRANCE
GOOGLE INC.
GROUPE GLI
NERIM
PKY SERVICES
SFR
STREAMWIDE

COMMERCE

ACCOR SERVICES FRANCE
AIR FRANCE
ALAIN CRENN
AM DIFF
APEC
ARCYDIS
ARENA AUTO
ASCENSEURS SERVICES
AUDIT ET SOLUTIONS
BARROIDIS
BASE & CO
BERLANGE
BERTIN SERVICES
BLIZZARD ENTERTAINMENT INC
BLT DEVELOPPEMENT
BOUCHERON
CARREFOUR HYPERMARCHÉS
CASINO ANTIBES LA SIESTA
CASINO DE CHAUDES AIGUES

CAST PROD
 CHAMBRE D'AGRICULTURE DES PYRÉNÉES ORIENTALES
 CAMARSYL
 COLT TECHNOLOGY SERVICES
 COMPAGNIE EUROPÉENNE D'INTELLIGENCE STRATÉGIQUE
 COMPAGNIE DE RESTAURATION INTERNATIONALE
 CONFLANS LOISIRS
 COOKSON MÉTAUX PRÉCIEUX
 CORA
 CORSAIR
 CRÉATIVE PATTERNS
 D CLIM
 DÉCATHLON
 DENNEL PARCS ET JARDINS
 DGLA SUD
 DIGNE DISTRIBUTION
 DISTRIBUTION CASINO FRANCE
 DISTRIBUTION NANTAISE D'ALIMENTATION
 DISTRIFLY
 DOMICOURS HOLDING
 EADS
 EDUCAZEN
 ÉLYSÉES CONSULT
 ENTREPRISE CLARAC ET COMPAGNIE
 ENTREPRISE THÉBAULT
 EURAUDIT CONSEIL
 EURO DISNEY ASSOCIÉS SCA
 FACET
 FAÇONNABLE
 FEDERAL EXPRESS CORPORATION
 FROMAGER SAVOYARD
 GRAND HÔTEL ROI RENÉ
 GEIGER MULTIMEDIA SERVICES
 GIE 32 HOCHÉ
 GREY PARIS
 GROUPE UFG
 GUINNESS FRANCE
 GUYENNE ET GASCOGNE
 HISTOIRE ET PATRIMOINE
 HÔTEL DE NANTES
 IBIS BERCY VILLAGE
 INFOMIL
 JOLLY HÔTELS FRANCE
 KRAFT FOODS LAVERUNE PRODUCTION
 LA CURE GOURMANDE
 LALIQUE
 LA VOLONTÉ AU SERVICE DE L'HYGIÈNE
 LE CLOS DES FLEURS LUN
 LIANOUDIS
 LIBRAIRIE GOULARD
 LOTUS DÉVELOPPEMENT
 MAGFORCE INTERNATIONAL
 MARIANNE INTERNATIONAL
 MC DIFFUSION
 MELINE DISTRIBUTION
 MICHEL FRANCIS JEAN-LOUIS
 MILLIPORE
 NAPADE
 PAGESJAUNES
 PLANÈTE INFORMATIQUE
 RECREA
 RESOCOM-MTM
 ROUEN DISTRIBUTION
 SARATOGA
 SAUR
 SOCIÉTÉ DES CENTRES COMMERCIAUX
 SOCIÉTÉ COMMERCIALE DES HÔTELS ÉCONOMIQUES
 SOCIÉTÉ DE DISTRIBUTION CATALANE
 SOCIÉTÉ ELODIS
 SOCIÉTÉ D'EXPLOITATION DES ÉTABLISSEMENTS DANIEL BARRE
 SOCIÉTÉ NORDINE BOUHADJEB
 SOCIÉTÉ DE PROTECTION ÉLECTRONIQUE ET MÉCANIQUE
 SODICE EXPANSION
 SODIMODIS HYPERMARCHÉ

SONY PICTURES TELEVISION PRODUCTION FRANCE
SPEED CHRONO SERVICES
STARCO
STÉ NOUVELLE DU TERRASS HÔTEL
SURCOUF
TELECITYGROUP FRANCE
TITI SEBASTIANO – PHÉNIX SÉCURITÉ PRIVÉE
TRANSVERSAL FILMS
TRIGO
UNIVERS OPTIC
VALTIS
VERCERAL
VITAL CLUB JFM
VOYAGES.SNCF.COM
X. NOV
WEBFUTUR

ÉDUCATION

ANACOURS
COLLÈGE CLÉMENCE-ROYER
COLLÈGE JEAN-MOULIN
COLLÈGE HENRI-MATISSE
COLLÈGE MAX-ROUQUETTE
COLLÈGE VIA-DOMITIA
CROUS DE LYON
ÉCOLE DE BOULANGERIE ET DE PÂTISSERIE DE PARIS
ÉCOLE DANHIER DE PÉDICURIE PODOLOGIE INSTITUT
PRIVÉ DE FORMATION
ÉCOLE INTUIT LAB
ÉCOLE NATIONALE DES ARTS DU CIRQUE DE ROSNY
ÉCOLE SUPÉRIEURE DE JOURNALISME DE PARIS
EDUCATIONAL PROGRAMS MASTER FRANCE
GROUPE SCOLAIRE SAINT-DENIS
L'ÉCOLE MODERNE
ESPOIR CENTRES FAMILIAUX JEUNES
LES COURS LEGENDRE
PROFADOM
SECONDE ÉCOLE
VH BLUE
VH GREEN

IMMOBILIER

ACTIF IMMO
ACCESS2OWNERS
ADÉQUATION
ATLANTIQUE HABITATIONS
CERTIFIMMO
C&K COMPONENTS
CLUBHOTEL MULTIVACANCES
ÉLISABETH LUMINEAU
FIPAC
FONCIA GROUPE
FONCIA PARIS GESTION
GRATADE
GROUPE DIAGNOSTICS SANTÉ ENVIRONNEMENT
HEXAGONE EXPERTISES LYON – RHÔNE-ALPES
IMMOBILIÈRE TICHADOU
INFIMO
LVA TECHNOLOGY
OFFICE PUBLIC DE L'HABITAT IVRY-SUR-SEINE
OFFICE PUBLIC DE L'HABITAT DE PÉRIGUEUX
OLYMPIERRE
OLYMPIERRE GESTION
OPAC DE L'OISE
OPH DE CHARTRES
OPH DE GUERET
P.L. IMMOBILIER
PM PARTICIPATION
S.A.C.V.L.
S.D.I.

INDUSTRIE

ALSTOM POWER TURBOMACHINES
BERNARD MOREAU
DOMALAIT PRODUCTION
ENTREPRISE LAURENT
EURL AU FEU DU BOIS
GLOBAL CONCEPT
GRAFTECH FRANCE

INSTITUT TECHNIQUE DES GAZ ET DE L'AIR
LORRAINE PROPRETÉ
NEMOPTIC
RENAULT SAS
TÉLÉVISION VIDÉO SERVICES

POLICE – JUSTICE

BRIGADE DE GENDARMERIE DE VILLEFRANCHE-DE-ROUERGUE
COMMISSARIAT DE POLICE DE CARMAUX
DIRECTION DÉPARTEMENTALE DE LA SÉCURITÉ PUBLIQUE DU TARN-ET-GARONNE
GIE GROUPEMENT PÉRIPHÉRIQUE
GROUPEMENT DÉPARTEMENTAL DE GENDARMERIE DU TARN
DIRECTION GÉNÉRALE DES DOUANES ET DROITS INDIRECTS (STRASBOURG)
MINISTÈRE DE L'IMMIGRATION
MINISTÈRE DE L'INTÉRIEUR
MINISTÈRE DE LA JUSTICE
SCP ARNAUD ET NICOLAS PEYRONNIE
SCP LUCCHINI PASQUIN
SCP PATRICK CHAIX ET LAURENT CHAIX
SECURITAS TRANSPORT AVIATION SECURITY (STRASBOURG)

SANTÉ – SOCIAL

CCAS DE LOMME
CCAS DE MONS-EN-BAROEUL
CENTRE HOSPITALIER CORNOUAILLE – HÔPITAL LAENNEC
CENTRE HOSPITALIER DES ESCARTONS
CENTRE HOSPITALIER INTERCOMMUNAL DES ALPES DU SUD
CERNER FRANCE
CLINIQUE HERBERT
CLINIQUE MAUSSINS-NOLLET
CNAMTS CTI GRAND EST
EMC FRANCE
EXONHIT THERAPEUTICS SA

INSTITUT NATIONAL DE LA SANTÉ ET DE LA RECHERCHE MÉDICALE
LE RAMEAU D'OR – EHPAD DU LUBERON
MAISON DE RETRAITE LES MOUETTES
MAISON DE RETRAITE PROTESTANTE DE NANTERRE
NCS NORD DE FRANCE
PFIZER
SANTEOS
SOCIÉTÉ D'EXPLOITATION DES AMBULANCES NEPTUNE
SOCIÉTÉ DES PRATICIENS DE LA CLINIQUE GÉNÉRALE DE SAVOIE

SPORT

ASSOCIATION OLYMPIQUE DE MARSEILLE
FÉDÉRATION FRANÇAISE DE LUTTE OLYMPIQUE DE MARSEILLE
OM MÉDIAS

TRANSPORT

ALLO TAXI
AMBULANCES ATLANTIC
AMBULANCES GREINER
AMBULANCES PORT ROYAL
COMITÉ D'ENTREPRISE DES TRANSPORTS PRÉVOST
CONNEX EPINAL
CTPL
ÉTABLISSEMENTS BOTTE
EXPRESS MAREE
FRONTIGNY POIDS LOURDS
GIFI
GOLD PALACE
LES AUTOCARS DE MARNE-LA-VALLÉE
LES NOUVEAUX COURSIERS
SOCIÉTÉ NOUVELLE GROUPEMENT TAXI
TRANSPORTS PRÉVOST

LISTE DES SANCTIONS PRONONCÉES EN 2010

Date	Nom ou type d'organisme	Décision adoptée	Thème
18/03/2010	Grossiste en habillement *	Interruption de traitement	Biométrie
22/04/2010	Transport routier *	Interruption de traitement	Vidéosurveillance
22/04/2010	AIS2 sous l'enseigne Acadomia	Avertissement	Données excessives, commentaires excessifs, gestion clients
22/05/2010	Association culturelle et pédagogique *	Absence d'interruption (relaxe)	Biométrie
17/06/2010	JPSM	Sanction pécuniaire de 15 000 €	Prospection commerciale par télécopie
30/09/2010	Club de remise en forme *	Sanction pécuniaire de 1 500 €	Biométrie
30/09/2010	Agence d'hôtesse *	Relaxe	Commentaires excessifs
21/10/2010	Cours à domicile *	Avertissement et dénonciation au Parquet	Données excessives
21/10/2010	Constructeur automobile *	Sanction pécuniaire de 15 000 €	Prospection commerciale droit d'opposition
25/11/2010	Groupe scolaire *	Avertissement	Biométrie vidéosurveillance
07/12/2010	Banque *	Sanction pécuniaire de 1 000 €	Droit d'accès

* Sanctions non rendues publiques.