rapport d'activité 2012

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Protéger les données personnelles,
accompagner l'innovation,
préserver les libertés individuelles

CNIL
Commission Nationale de l'Informatique et des Libertés

La documentation Française

COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

RAPPORT D'ACTIVITÉ **2012**

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

LES CHIFFRES CLÉS DE 2012

DÉCISIONS ET DÉLIBÉRATIONS

2 078
DÉCISIONS ET DÉLIBÉRATIONS ADOPTÉES
(+ 5,5% par rapport à 2011)

316
AUTORISATIONS, DONT 3 AUTORISATIONS UNIQUES

113
AVIS

3
DISPENSES

2
RECOMMANDATIONS PORTANT SUR LA COMMUNICATION POLITIQUE ET LES COMPTEURS COMMUNICANTS

MISES EN DEMEURE ET SANCTIONS

43
MISES EN DEMEURE

4
SANCTIONS FINANCIÈRES

9
AVERTISSEMENTS

2
RELAXES

PLAINTES ET DEMANDES DE DROIT D'ACCÈS INDIRECT

6 017
PLAINTES
(+ 4,9 % par rapport à 2011)

3 682
DEMANDES DE DROIT D'ACCÈS INDIRECT
(+ 75 % par rapport à 2011)

INTERVENTIONS EXTÉRIEURES

160
INTERVENTIONS

FORMALITÉS PRÉALABLES

8 946
DÉCLARATIONS RELATIVES À DES SYSTÈMES DE VIDÉOSURVEILLANCE
(+49,3 % par rapport à 2011)

5 483
DÉCLARATIONS RELATIVES À DES DISPOSITIFS DE GÉOLOCALISATION
(+ 22,3 % par rapport à 2011)

795
AUTORISATIONS DE SYSTÈMES BIOMÉTRIQUES
(+6,8 % par rapport à 2011)

CONTRÔLES

458
CONTRÔLES
(+19 % par rapport à 2011)

173
CONTRÔLES VIDÉOPROTECTION

CORRESPONDANTS

10 709
ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT
(+24 % par rapport à 2011)

LABELS

10
LABELS DÉLIVRÉS
(au 15 février 2013)

SOMMAIRE

AVANT-PROPOS DE LA PRÉSIDENTE

UNE ANNÉE PLEINE D'AUDACE

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

Pour réaliser cet objectif, un plan stratégique triennal a été adopté en juillet 2012. Il inscrit l'action quotidienne de notre institution autour de trois directions :

- celle de l'ouverture et de la concertation avec les acteurs car le régulateur ne peut plus travailler et réfléchir seul ;
- celle de la conformité à travers laquelle nous responsabilisons ceux qui traitent des données personnelles et, en particulier les entreprises et construisons avec eux des outils concrets de mise en œuvre des principes informatiques et libertés ;
- celle enfin du respect de la régulation via une politique répressive plus ciblée et plus efficiente.

> “Protection des données et innovation sont les deux faces d'une même médaille. L'une sans l'autre et nous risquons une crise de confiance généralisée”

Ce dessein représente un effort considérable pour notre institution. Grâce au travail des équipes et des membres de la CNIL, il est en train d'être mis en œuvre et nous sommes en chemin vers cette nouvelle CNIL ; une e-cnil, plus réactive, plus agile, plus ancrée dans le réel. Il est rendu d'autant plus complexe qu'il s'inscrit dans un environnement qui, en ce début d'année 2013, est marqué par de fortes tensions.

Pour commencer, évoquons la compétition économique croissante autour des données personnelles.

Ce constat dépasse le cadre d'internet puisque le numérique est présent dans tous les secteurs économiques traditionnels et constitue le socle des innovations et des services de demain dans la banque, l'assurance, l'énergie, l'automobile, la santé, etc.

Les formules utilisées pour illustrer la richesse et le caractère central des données personnelles dans l'économie ont fleuri dans les médias : « pétrole du numérique », « matière première », « ruée vers l'or », « eldorado », etc.

Cette ressource est un peu particulière car elle est, pour partie, produite par les individus eux-mêmes.

On aurait donc tort d'ignorer ou de minorer cette dimension humaine. L'économie se construit désormais à partir de l'individu ; c'est de plus en plus lui qui est le produit, la ressource-clé. Or, le citoyen/consommateur numérique a mûri. S'il veut profiter pleinement des services qui sont à sa disposition, il demande en contrepartie des garanties par rapport à ses données personnelles car il s'inquiète de plus en plus par rapport à l'utilisation de celles-ci (79 % des Français se disent inquiets de l'utilisation qui peut être faite de leurs données personnelles à des fins de marketing direct ou de publicité en ligne*).

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

Isabelle Falque-Pierrotin,
présidente de la CNIL

Il veut donc avoir une vie en ligne mais aussi plus de transparence et plus de maîtrise sur ses données. On a vu la confusion et la méfiance suscitées par le « bug Facebook » en septembre 2012. Faux bug informatique mais vrai bug psychologique ! Quelques semaines plus tard, c'est Instagram qui a dû faire machine arrière après le tollé provoqué par l'annonce de ses nouvelles conditions générales qui le rendait propriétaire des photos de ses clients.

Les acteurs économiques doivent réaliser qu'en procédant à marche forcée, ils installent un inconfort, un déficit de sécurité dans l'esprit de leurs clients qui peuvent se retourner contre eux de façon brutale. L'innovation impose souvent la rupture, ou au moins de rompre avec des règles établies. Mais un modèle économique fondé sur l'innovation doit reposer sur la confiance et la transparence. Lorsque la confiance est rompue, le modèle économique se fragilise.

On le voit, la protection des données personnelles est en train de rentrer dans le débat concurrentiel ; loin d'être un frein, la protection des données peut aujourd'hui être considérée et présentée comme un atout commercial. Opposer l'innovation et la protection des données est dès lors une vue simpliste et à très court terme qui ne reflète pas la complexité de l'écosystème numérique et les attentes du consommateur.

Au même moment, une autre bataille a lieu sur le terrain géostratégique.

À Bruxelles, les différents blocs géographiques se font face et s'affrontent pour élaborer le cadre juridique européen de la protection des données du XXIe siècle. S'il en était besoin, l'importance des enjeux stratégiques peut se mesurer aux 3000 amendements déposés sur le projet de règlement. De même, par le déploiement d'une armée de lobbys qui, de mémoire de parlementaires européens, n'avait jamais envahie Bruxelles à ce point. Pour l'Europe, le moment est en effet historique et le défi est grand. Elle doit moderniser son modèle et le rendre compétitif, par rapport aux initiatives étrangères comparables, tout en réaffirmant la protection des données personnelles en tant que droit fondamental. Elle doit concilier croissance économique et libertés.

Dans cette bataille, la CNIL, aux côtés de ses homologues européens, ne ménage pas ses efforts. Elle a mobilisé les parlementaires, le gouvernement, ses homologues pour expliquer, convaincre et proposer des alternatives allant dans le sens d'une gouvernance européenne décentralisée reposant sur des autorités puissantes évoluant à armes égales et coopérant fortement entre elles. L'année 2013 sera déterminante car le texte européen pourrait être adopté tout comme les cadres du Conseil de l'Europe, de l'OCDE et de l'APEC.

Au-delà de ces affrontements, des questions fondamentales émergent et la CNIL souhaite lancer le débat.

Depuis quelques semaines en effet se multiplient dans les journaux français et internationaux des analyses sur le rôle croissant des données dans le développement de l'économie numérique et notamment du Big data et, face à ces belles promesses économiques, le débat public se noue sur le meilleur cadre de régulation souhaitable, le plus à même d'assurer le développement de celles-ci.

Pour certains, une régulation excessive des données personnelles handicaperait les acteurs français dans l'élaboration de nouveaux services alors même que nos concitoyens ne s'inquiètent pas outre mesure de la protection de leur vie privée. Nous devrions au contraire « libérer » les données, et ainsi favoriser la croissance.

▸▸▸

▸▸▸

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

Ce débat sur la régulation, sa nécessité et son ancrage pertinent n'est pas nouveau concernant Internet et le numérique. Nous en parlons depuis 10 ans ! Les données personnelles succèdent ainsi à la protection de l'enfance ou à la propriété intellectuelle. Ces questions, quoique différentes peuvent nous aider à construire une action de régulation efficace et légitime en matière de protection des données personnelles.

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

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

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

Nous avons besoin d'innover, de créer de nouveaux usages et services. Notre croissance et notre rayonnement international en dépendent. Fixer le cadre de cette innovation, les responsabilités respectives de l'État, des entreprises et des citoyens n'est pas superfétatoire. En réalité, protection des données et innovation sont les deux faces d'une même médaille. L'une sans l'autre et nous risquons une crise de confiance généralisée.

La CNIL, consciente de cette ambivalence, souhaite qu'un débat ouvert et constructif se mette en place afin de fixer les contours de nos choix et collectifs. Elle a lancé celui-ci début 2013 et veut y associer l'ensemble des parties prenantes concernées.

La CNIL est donc en marche. Elle est déterminée à prendre le virage du numérique et à se positionner comme une autorité de régulation crédible.

Les mesures annoncées par le Premier ministre, à l'issue du séminaire gouvernemental sur le numérique le 28 février 2013, constituent par ailleurs une étape importante vers le renforcement des droits numériques de nos concitoyens. Elles confortent également le rôle de la CNIL en lui accordant une place et des pouvoirs plus importants.

L'ensemble de ces mesures, tout comme la constitutionnalisation de la protection des données personnelles que la CNIL appelle de ses vœux, contribueront ainsi à construire un environnement de confiance, élément indispensable pour accompagner le développement d'une innovation durable.

Dans ce contexte de bouleversement permanent, la CNIL doit, plus que jamais, faire preuve d'inventivité, d'écoute, et surtout d'audace. **L'audace, c'est affirmer une identité forte, tout en évoluant et tenant compte de la complexité du monde** dans lequel ces initiatives s'inscrivent. Nous n'en manquons pas cette année comme dans les années à venir.

Accompagnement, pédagogie, ouverture et prospective : une méthode de travail qui guide l'action de la CNIL

MOT DU SECRÉTAIRE GÉNÉRAL

L'activité de la CNIL a poursuivi sa forte croissance en 2012 : quel que soit l'indicateur retenu, tous les secteurs de la CNIL connaissent une hausse de leur activité, comme cela est constamment le cas depuis le début des années 2000. Le nombre de délibérations adoptées par la Commission (plus de 2 000) comme l'importance du nombre d'appels (plus de 134 000) ou de plaintes reçues (plus de 6 000) témoignent en effet de l'explosion des données personnelles dans tous les domaines, et de l'importance de la régulation par la CNIL, dans cet environnement évolutif qu'est l'univers numérique. Outre cette forte croissance de ses missions traditionnelles, l'activité de la CNIL a également été portée, en 2012, par la mise en œuvre des deux nouvelles missions que lui avait confiées le législateur en 2011 : le contrôle de la vidéoprotection, d'une part, et la notification des failles de sécurité des opérateurs de communication électronique, d'autre part. Sur le premier point, la CNIL a effectué, pour la deuxième année consécutive, plus de 170 contrôles en matière de vidéoprotection et vidéosurveillance, s'assurant ainsi que le développement de cet outil intervient dans le respect de la vie privée. Sur le second point, l'intervention du décret d'application en mars 2012 a déclenché les premières notifications de failles auprès de la CNIL, le dispositif étant appelé à monter en puissance en 2013. Enfin, les premiers labels ont été délivrés, en matière de formation et d'audits de traitement, et les demandes se succèdent à un rythme soutenu. En un mot, la CNIL est donc caractérisée par une activité en croissance dans un environnement en expansion.

Mais si la régulation passe par l'encadrement en amont ou les contrôles, elle implique également un double effort de pédagogie et d'accompagnement.

Pédagogie, tout d'abord : l'information des citoyens comme des responsables de traitement est une priorité de la CNIL, afin de faire connaître les droits et les exigences pesant sur chacun dans des termes opérationnels.

Édouard Geffray,
Secrétaire Général

La CNIL a ainsi lancé la mise en ligne de fiches pratiques thématiques, téléchargeables gratuitement depuis son site. 6 fiches sur la vidéoprotection/vidéosurveillance ont été mises en ligne en juin 2012, et ont d'ores et déjà été téléchargées plus de 40 000 fois sur notre site. 5 fiches pratiques sur les données personnelles au travail, mises en ligne en janvier 2013, ont également fait l'objet de dizaines de milliers de téléchargements, permettant ainsi à tout à chacun de bénéficier d'une approche pratique des questions quotidiennes en la matière. En termes de sensibilisation, la CNIL a également mis en ligne une vidéo interactive (Share the party) permettant aux jeunes de prendre conscience des impacts de la mise en ligne de vidéos sur Internet. Plus de 100 000 personnes ont ainsi fait cette expérience en quelques mois.

▸▸▸

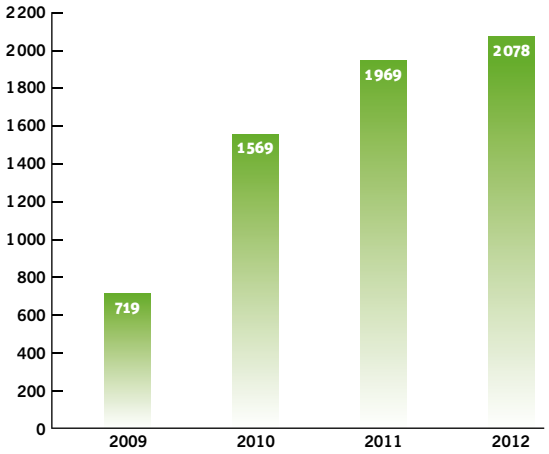
Accompagnement, ensuite, des acteurs publics ou privés : l'enjeu n'est pas seulement, en effet, d'effectuer telle ou telle formalité auprès de la Commission. L'enjeu est bien, pour les responsables de traitements, de s'assurer de la conformité permanente de leurs traitements aux exigences légales et aux bonnes pratiques dans un contexte d'évolutions technologiques et économiques extrêmement rapides. La CNIL s'est donc engagée dans la mise en œuvre de véritables outils d'accompagnement des acteurs publics ou privés dans cette dynamique de mise en conformité. Des nouveaux outils, comme le guide de la sécurité informatique destiné aux professionnels, ont ainsi été mis à disposition du public.

L'année 2012 a également été marquée par la poursuite, plus que jamais, d'un dialogue avec les parties prenantes autour de sujets structurants et du développement d'une vision prospective. La CNIL poursuit ainsi son ouverture et un dialogue construit avec les chercheurs, acteurs privés, acteurs publics, créateurs d'entreprises ou porteurs de projets innovants. Cette méthode a été expérimentée à de nombreuses reprises sur différentes thématiques : à titre d'exemple, la CNIL a fixé le cadre de la mise en ligne des archives publiques (état civil, etc.) après une concertation approfondie avec les services publics compétents. Elle a lancé une consultation publique sur le Cloud, avant de proposer des recommandations pratiques permettant aux entreprises de fixer les conditions optimales de protection des données personnelles qu'elles souhaitent voir héberger. La modification de l'autorisation unique sur les dispositifs biométriques a, de la même façon, été précédée d'un dialogue nourri avec les principaux acteurs du secteur, notamment les organisations syndicales et patronales, avant d'aboutir au retrait du contrôle des horaires des salariés du champ de cette autorisation.

Elle a, enfin, consulté les professionnels afin d'élaborer des premières recommandations relatives aux compteurs communicants et participe à un groupe de travail au sein de la FIECC (Fédération des Industries Électriques, Électroniques et de Communication).

La même méthode d'ouverture et de dialogue est également au cœur du développement de la recherche prospective. Créée en 2011, la direction des études, de l'innovation et de la prospective est montée en puissance en 2012, avec la création d'un comité de la prospective

Nombre des décisions et délibérations depuis 2009



comprenant des personnalités extérieures, la réalisation d'études mais aussi l'organisation de la journée « vie privée 2020 », qui a réuni un public d'experts large et divers en novembre 2012.

Forte progression de l'activité, accompagnement des acteurs dans leur démarche de conformité, évolution de nos méthodes de travail : autant de priorités pour l'organisation et les services de la CNIL, qu'il convient de mettre en perspective pour améliorer la qualité du service rendu et la performance de l'institution. C'est chose faite avec la fixation, par la Présidente de la CNIL, d'un nouveau plan d'orientation stratégique triennal pour les années 2012-2015, qui fixe les grandes priorités pour l'institution. Celui-ci s'inscrit également dans le contexte de l'évolution prochaine du cadre juridique européen sur la protection des données personnelles.

Ces évolutions sont appelées à se poursuivre en 2013. Pour y faire face, la CNIL peut s'appuyer sur l'augmentation de ses moyens décidée par le législateur, et sur la mobilisation et l'investissement de ses équipes, que je tiens à souligner ici. Dans un contexte contraint, cet investissement, porté par la conscience partagée de la nécessité d'une régulation équilibrée, constitue un atout majeur pour notre institution.

1. INFORMER ET ÉDUQUER

LA CNIL VOUS INFORME AU QUOTIDIEN

La CNIL est investie d'une mission générale d'information des personnes sur les droits que leur reconnaît la loi « Informatique et Libertés ». Elle mène des actions de communication grand public, que ce soit à travers la presse, son site internet, sa présence sur les réseaux sociaux ou en mettant à disposition des outils pédagogiques. Directement sollicitée par de nombreux organismes, sociétés ou institutions pour conduire des actions de formation et de sensibilisation à la loi « Informatique et Libertés », la CNIL participe aussi à des colloques, des salons ou des conférences pour informer et s'informer.

PARTENARIAT FRANCE INFO

Le partenariat débuté en 2007 a été renouvelé en 2012. 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 : comment sécuriser son smartphone, la communication politique, les tarifs sociaux de l'énergie, la réalité augmentée, le *big data*, les arnaques à la webcam, le *quantified self*[1], la télémédecine, etc.

Youtube.com/lacnil

SENSIBILISER AUX BONNES PRATIQUES SUR INTERNET

Depuis plusieurs années, la CNIL mène des actions à destination des jeunes, des enseignants et des familles pour les sensibiliser aux bonnes pratiques sur les réseaux sociaux. À l'occasion de la Fête de l'internet 2012, la CNIL a proposé une campagne web innovante.

L'objectif de la vidéo interactive *Share the Party* est de faire vivre une expérience aux internautes et de les responsabiliser en les immergeant dans une scène de la vie courante d'un jeune. Un adolescent participe à une soirée et en filme les temps forts avec la possibilité de les « partager ou pas » sur les réseaux sociaux. En fonction de ses choix, la soirée ne se terminera pas de la même manière et l'adolescent devra assumer les conséquences, heureuses ou malheureuses, de ses actes. Ainsi, 11 fins différentes sont possibles. Les jeunes internautes peuvent ainsi faire l'expérience réaliste des conséquences positives ou négatives du partage de vidéos ou photos en ligne.

Youtube.com/cnil :

Tutoriel CNIL #4 **Limiter ses traces sur internet**

Tutoriel CNIL #3 **Comment surfer en sécurité?**

Tutoriel CNIL #2 **Sécuriser son smartphone**

LES TUTORIELS VIDÉO

La question de la sécurité des données est devenue incontournable avec internet et avec la multiplication des smartphones et autres tablettes numériques. Mais les internautes ne savent pas toujours, par exemple, comment gérer la géolocalisation de leur smartphone, comment effacer les traces de leur navigation sur Internet ou encore comment se protéger des virus. La CNIL a donc souhaité montrer de manière pédagogique, avec la réalisation de tutoriels vidéo, comment sécuriser son smartphone, comment surfer en sécurité et comment limiter ses traces sur Internet.

L'internaute découvre, étape par étape, quelques conseils pratiques : comment se prémunir contre les virus ou les vols de données ? Comment chiffrer les données de sauvegarde de son téléphone ? Comment reconnaître un site avec une connexion sécurisée au moment d'un achat en ligne ? Comment garder la confidentialité de vos communications entre votre ordinateur et les sites internet ? Comment mettre en place un code de verrouillage sur son smartphone ?

> La CNIL se positionne comme un acteur central de l'accompagnement de la vie numérique

LES PUBLICATIONS

En 2012 la CNIL a publié deux nouveaux guides.

Lorsqu'on souscrit un abonnement de téléphonie fixe ou mobile auprès d'un opérateur de téléphonie ou d'un fournisseur d'accès à Internet (FAI), on est amené à lui communiquer des données personnelles. Quelles informations a-t-il le droit de détenir ? Comment exploite-t-il ses données ? Comment ne plus être démarché par téléphone ? Pourquoi un abonnement téléphonique a-t-il été refusé ? Le guide téléphonie répond à toutes ces questions et fait le point sur les droits et obligations « Informatique et Libertés » dans le cadre de l'utilisation de la téléphonie.

La CNIL a réalisé 173 contrôles relatifs aux dispositifs de vidéosurveillance/vidéoprotection et reçu plus de 360 plaintes en 2011. C'est pourquoi elle a souhaité accompagner les professionnels et les particuliers en mettant à leur disposition

▸▸▸

[1] Le « Quantified Self » est la pratique de la « mesure de soi ». Ce terme désigne un mouvement né en Californie qui consiste à mieux se connaître en mesurant des données relatives à son corps ou à son état de santé

sur son site 6 fiches pratiques. Celles-ci expliquent très concrètement comment installer des dispositifs dans le respect de la loi et du droit des personnes filmées.

Ces 6 fiches ont été téléchargées 30 000 fois depuis leur mise en ligne.

À partir des recommandations sur la communication politique élaborées par la CNIL en janvier 2012, un nouveau guide pratique a été publié et adressé aux partis. Ce véritable «manuel de campagne à l'ère numérique» à destination des partis et des candidats comme de leurs prestataires, propose de nombreux exemples, cas concrets et modèles de clauses (mentions d'informations, recueil du consentement des personnes, etc.).

41 860
ABONNÉS À LA LETTRE INFOCNIL

LE SITE INTERNET WWW.CNIL.FR

En 2012, la CNIL a entrepris un travail sur l'outil de webanalytics du site, dans le but de se doter d'un outil de mesure performant, tout en respectant ses recommandations en matière de protection des données personnelles. Un développement spécifique a été mené afin d'offrir aux internautes la possibilité de s'opposer aux statistiques, et d'exercer leur droit d'accès aux données statistiques les concernant. Depuis le 1er juin 2012, la CNIL établit des statistiques de consultation hebdomadaires et mensuelles.

En moyenne sur les 6 derniers mois de l'année, 235 710 pages vues ont été consultées par 32 147 visiteurs uniques par semaine. La durée moyenne de la visite est de 5 minutes et 13 secondes.

Face à l'internationalisation des enjeux en matière de protection des données personnelles, la CNIL a investi dans une communication régulière auprès du public anglophone. Elle traduit désormais systématiquement les actualités traitant des sujets à vocation internationale ou européenne.

L'OBSERVATOIRE DES ÉLECTIONS 2012

Dans le cadre des campagnes présidentielle et législative, la CNIL a mis en place sur son site un « Observatoire des élections », chargé de veiller au respect de la protection des données personnelles par les partis politiques et leurs candidats. Un formulaire de témoignage a été mis en ligne afin de permettre aux électeurs de témoigner, par un moyen simple et rapide, des difficultés rencontrées dans le cadre des campagnes électorales.

Ce dispositif a permis à la CNIL d'identifier de manière concrète les problèmes posés par la prospection politique, et de réagir rapidement auprès des candidats et des électeurs en diffusant notamment de l'information sur les pratiques à respecter et les actions à entreprendre en cas de non-respect.

LES RÉSEAUX SOCIAUX

En 2012, la CNIL a affirmé sa présence sur les réseaux sociaux Twitter, Facebook, Google+, Youtube, Dailymotion et les réseaux professionnels Viadéo et LinkedIn. Avec maintenant 20 000 abonnés sur Twitter et 5 159 « J'aime » sur Facebook, ces nouveaux canaux de communication prennent de l'importance dans la diffusion des messages de l'institution.

La CNIL arrivait en **neuvième** position dans l'outil de classement des institutions françaises sur Twitter, mis en place par La Netscouade[1].

20 000
ABONNÉS SUR TWITTER

L'IMAGE DE LA CNIL

Depuis 2004, la CNIL mesure sa notoriété ainsi que la connaissance des droits. Le baromètre de l'IFOP porte sur un échantillon de 967 personnes, représentatif de la population française âgée de 18 ans et plus. Les interviews ont eu lieu en face à face au domicile des personnes interrogées du 21 au 27 novembre 2012. ■

55 %
DES PERSONNES CONNAISSENT LA CNIL CONTRE 32 % EN 2004

[1] Classement de la CNIL sur Twitter au 13/02/2013. À l'heure où la plupart des organisations se mettent à Twitter, La Netscouade a réalisé un outil auto régénérateur permettant de classifier le poids et l'influence des institutions françaises sur le site de micro-blogging Twitter : http://www.lanetscouade.com/sites/default/files/top20/

L'ÉDUCATION AU NUMÉRIQUE : UNE PRIORITÉ POUR LA CNIL

Les équipements et usages numériques des jeunes explosent. 48 % des 8-17 ans sont connectés à Facebook et 18 % des moins de 13 ans[1] y ont leur propre compte, alors que les clauses d'utilisation fixent l'âge minimum à 13 ans. 90 % des 15-17 ans prennent des photos ou font des vidéos sur leurs smartphones[2].
Mais si l'utilisation des nouvelles technologies du numérique se généralise, leur appropriation implique une prise de conscience individuelle et collective concernant les enjeux, les risques et les bonnes pratiques en la matière. Soucieuse d'informer et de sensibiliser les citoyens, et notamment les plus jeunes, la CNIL a mené, depuis plusieurs années, de nombreuses actions pédagogiques.

Les principales actions engagées par la CNIL :

- La création d'un site dédié (jeunes.cnil.fr), sur lequel les internautes peuvent par exemple avoir accès à des vidéos, des éditions spéciales de *Mon quotidien* et *l'Actu*, au quiz des *Incollables* sur la protection des données personnelles. Dans l'espace « parents », les internautes peuvent trouver des tutoriels vidéo sur des thèmes tels que « Comment créer des listes d'amis sur Facebook ? » ou « Sécuriser son smartphone ». Des fiches pédagogiques sont disponibles dans l'espace « enseignants ».
- La réalisation d'un *serious game* sur les réseaux sociaux et les traces, en partenariat avec Internet sans crainte.
- La CNIL délivre un label pour les « formations Informatique et Libertés ».
- Dans le cadre de la francophonie, la CNIL accompagne la mise en place de nouvelles autorités de protection des données, notamment par des actions de formation.

En 2012, elle a décidé d'aller plus loin et de faire de l'éducation au numérique une priorité stratégique. Elle souhaite ainsi renforcer son action avec l'élaboration de nouveaux outils et l'élargissement de leur diffusion.

Cette politique aura vocation à s'articuler avec celle des autres acteurs concernés, publics – notamment le ministère de l'Éducation nationale – et privés. La CNIL a créé un poste de responsable de l'éducation au numérique en novembre 2012 en charge du pilotage de cette politique. ■

[1] Étude réalisée par TNS Sofres pour l'UNAF, la CNIL et Action innocence du 10 au 17 juin 2011 par téléphone, auprès d'un échantillon national représentatif de 1 200 enfants et adolescents, âgés de 8 à 17 ans. / [2] Enquête en ligne réalisée par Médiamétrie du 4 au 14 novembre 2011 auprès de 2 315 utilisateurs de smartphones âgés de 15 ans et plus.

LES RÉPONSES AU PUBLIC

Le service d'orientation et de renseignement du public (SORP) est le point d'entrée de tous les appels et courriers adressés à la CNIL par les usagers (particuliers et professionnels responsables de traitements). Il procède également à l'enregistrement de tous les dossiers de formalités préalables, instruit une partie des déclarations et conseille les particuliers et les professionnels.

En 2012, la CNIL a traité 88 990 dossiers de formalités qui se décomposent de la façon suivante :

- **48 833** déclarations simplifiées, dont :
  - 2 255 engagements de conformité à un acte réglementaire unique
  - 4 720 engagements de conformité à une autorisation unique
  - 255 engagements de conformité à la méthodologie de référence
  - 319 engagements de conformité à une déclaration unique.
- **33 588** déclarations normales
- **1 534** demandes d'autorisation
- **1 671** demandes d'avis
- **658** demandes d'autorisation de recherche médicale
- **162** demandes d'autorisation évaluation de soins dont
- **540** demandes de modification effectuées par courrier

En 2012, la CNIL a délivré les récépissés **dans un délai moyen de 48 h pour les déclarations simplifiées et de 5 jours calendaires pour les déclarations**.

La CNIL a pour mission générale de conseiller les personnes (particuliers et professionnels) et de leur délivrer toute information utile en ce qui concerne notamment les démarches à accomplir pour l'exercice de leurs droits et les procédures à suivre pour les formalités déclaratives.

Cette mission s'effectue au quotidien par courrier (**9 155** courriers adressés en 2012 contre **5 720 en 2011**) et par téléphone. La permanence quotidienne de renseignements juridiques) a pris en charge **62 340** appels en 2012 (contre **69 620 en 2011**). ■

35 924
COURRIERS REÇUS

134 231
APPELS TÉLÉPHONIQUES

88 990
DOSSIERS DE FORMALITÉS TRAITÉS

93 % des formalités sont effectuées en ligne

FOCUS

Les usagers sont-ils satisfaits ?

- **95 % des usagers sont satisfaits de l'accomplissement des formalités préalables**
- **88 % des usagers sont satisfaits du contact avec la CNIL**

Source : Enquête de satisfaction réalisée par l'IFOP début octobre 2012 auprès de 1 012 usagers.

GROS PLAN

LA PLACE DES PHOTOS DANS LA VIE NUMÉRIQUE

TAGS ET RECONNAISSANCE FACIALE : DE NOUVEAUX ENJEUX POUR LA VIE PRIVÉE

« 84 % des possesseurs français de smartphones l'utilisent pour prendre des photos » (90 % chez les 15-17 ans)[2]

Photos et vidéos sont devenues omniprésentes dans le monde numérique, en particulier avec la pénétration rapide des smartphones. Ces photos numériques ne sont pas seulement prises, elles sont aussi largement partagées et stockées en ligne. Ainsi, 300 millions de photos sont publiées chaque jour sur Facebook[1]. L'identification automatique des photos est en train de se généraliser. Les photos de personnes voire de certains lieux peuvent être considérés comme particulièrement sensibles dans la mesure où il devient de plus en plus facile d'appliquer sur elles des technologies d'analyse d'images sophistiquées, en particulier la reconnaissance faciale. Qui plus est, les images qui restent stockées et qui sont largement dupliquées alimentent la question du droit à l'oubli.

Les français utilisateurs de smartphones et de réseaux sociaux sont confrontés quotidiennement à la question de cette place des images et photos dans leur « patrimoine numérique personnel » et de nombreuses études montrent que des stratégies et comportements individuels particuliers et sophistiqués se développent[3].

Au sein d'un plan d'action plus large (comprenant en particulier une feuille de route technologique et des travaux au sein du laboratoire de la CNIL), la CNIL a souhaité explorer ces pratiques et évaluer le niveau de perception des enjeux de protection de la vie privée et des données personnelles liés à ces usages.

Réalisée sur proposition du nouveau Comité de la Prospective de la CNIL, l'étude[4] confiée à TNS-Sofres avait pour objet d'étudier les comportements, les stratégies de publication des internautes et leurs perceptions des outils de tag et de reconnaissance faciale.

Les résultats confirment qu'une proportion importante des internautes est concernée par la publication et le partage de photos. En effet, plus de la moitié des internautes **(58 %) déclarent publier des photos sur Internet**. Ce nombre atteint même 86 % chez les 18-24 ans, et ils sont d'ailleurs 54 % à prendre une photo d'abord dans le but de la publier. Toutes les générations partagent des photos, même si les pratiques et stratégies de publication diffèrent en fonction de l'âge. Globalement, plus les utilisateurs sont jeunes, plus ils ont tendance à se photographier eux-mêmes. À l'inverse, leurs ainés vont préférer des photos moins directement personnelles (paysages, voyage ou centres d'intérêts). Dans tous les cas, les résultats soulignent un changement de nature de la photo qui est désormais commentée ou « likée » par 75 % des internautes. Au travers de ces nouvelles pratiques, la photo en ligne constitue un champ en pleine expansion, qui représente un enjeu économique important pour les acteurs d'Internet.

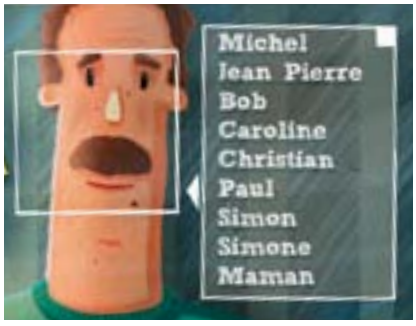
> Les technologies de reconnaissance faciale pourraient transformer la photo en nouvel identifiant numérique

LE TAG ET LA RECONNAISSANCE FACIALE : LES NOUVELLES PRATIQUES SENSIBLES ?

Un des sujets principaux de l'enquête était de s'intéresser au « tag », une dimension nouvelle née avec le partage, qui consiste à identifier les personnes figurant sur les photos. Les outils de reconnaissance faciale viennent quant à eux compléter cette pratique en automatisant l'association entre une personne et son nom, sur la base de l'analyse et de la reconnaissance des traits de son visage.

Le tag, utilisé par 41 % des internautes, transforme la photo en un objet qui devient requêtable, indexable par un moteur de recherche, et donc plus accessible, plus visible et plus facile à trouver. Dans un contexte où **43 % des internautes disent avoir déjà été gênés par une photo**, les technologies permettant d'y associer automatiquement leur nom suscitent aussi des inquiétudes pour 41 % d'entre eux, malgré une faible utilisation pour le moment (par 12 % des internautes) à l'exception notable des plus jeunes (déjà 27 % des 18-24 ans). Or, l'étude montre par ailleurs que seuls 44 % des internautes demandent systématiquement l'avis des personnes qu'ils photographient avant de publier des photos… Ce chiffre est encore plus faible (34 %) pour ce qui est du tag. D'où l'importance d'offrir des outils permettant aux utilisateurs de mieux contrôler la manière dont ils sont identifiés dans des publications (cf. conseils aux utilisateurs p.19).

Un autre enseignement de l'étude réside en effet dans le faible degré de maîtrise des paramètres permettant de régler la visibilité des photos publiées. Moins d'un tiers des personnes interrogées disent bien les connaître et elles sont une large majorité **(75 %) à éprouver le besoin de mieux protéger leurs publications**. Ce constat s'amplifie lorsque l'avenir des contenus est évoqué : si les deux tiers des internautes pensent supprimer certaines de leurs photos postées sur Internet, 73 % estiment que cela sera difficile. ▸▸▸



12 %

DES INTERNAUTES UTILISENT LA RECONNAISSANCE FACIALE

[1] Résultats 1er trimestre 2012, Facebook / [2] Source Médiamétrie, étude CNIL, novembre 2011 / [3] Par exemple l'étude en ligne « Sociogeek » : http://sociogeek.admin-mag.com/
[4] Sondage réalisé en novembre 2012 à la demande de la Cnil par TNS-Sofres auprès de 1554 internautes âgés de 13 ans et plus. Résultats du sondage disponible sur le site de la Cnil http://www.cnil.fr/la-cnil/actualite/article/article/publication-des-photos-sur-internet-comment-partager-sans-se-sur-exposer/Enquête

> On assiste à un véritable changement de nature de la photo qui devient un objet vivant

AMBIVALENCE DES COMPORTEMENTS : ENTRE LE RESPECT DE L'IMAGE DE L'AUTRE ET L'ENVIE DE DIFFUSER

En se focalisant sur les stratégies de publication, l'un des apports importants du sondage de la CNIL est de souligner l'ambivalence des comportements des internautes. Tout en étant soucieux des réutilisations qui pourraient en être faites (73 % se disent inquiets de l'utilisation par d'autres de leurs photos), ils ne savent pas vraiment qui y a accès (seuls 38 % disent le savoir exactement). Cette ambivalence s'explique à la fois par l'envie de se montrer, par une maîtrise approximative des outils permettant de régler la visibilité de leurs albums et par une certaine résignation des internautes (80 % pensent que leurs photos resteront sur Internet).

VERS UNE CONVERGENCE DES OUTILS ET DES PLATEFORMES POUR PLUS DE PARTAGE, TOUJOURS PLUS VITE

Le besoin de partager, de se dévoiler est largement entretenu par les nouveaux appareils photos connectés et de nouvelles fonctionnalités proposées par les plateformes. Une des tendances marquantes est représentée par les options de synchronisation automatique mises en avant par les grands acteurs d'Internet, aussi bien par Google (instant upload), Apple (« flux de photos ») et plus récemment Facebook (photo sync) au moyen de son application mobile. L'activation de ces options permet de synchroniser automatiquement toute nouvelle photo prise avec le terminal concerné dans un dossier stocké en ligne. En supprimant l'étape de « transfert » de la photo, le but de ces fonctionnalités est d'encourager le partage des photos qui se retrouvent à un clic d'être accessibles publiquement. On assiste ainsi à une convergence dans l'écosystème des services de gestion de photos visant à faciliter et à accélérer le partage et le stockage de ces données. Ce mouvement semble traduire une évolution de la norme autour de la photogra-

phie : alors que jusqu'à présent, c'est la sauvegarde ou la publication qui requérait une action, ce serait désormais la volonté d'effacement ou d'oubli qui nécessiterait une démarche et un effort de la part des utilisateurs. Et ceci dans un contexte où les technologies de reconnaissance faciale – aujourd'hui en plein essor – pourraient bien transformer la photo en un nouvel identifiant numérique.

Cette étude constitue la première étape d'un chantier plus vaste sur les changements sociétaux induits par le développement des outils et technologies de reconnaissance. C'est tout le sens de la réflexion prospective engagée par la CNIL sur la biométrie dans la vie quotidienne à l'horizon 2020. ■

INFOS +

5 conseils aux utilisateurs

1 Adaptez le type de photos au site sur lequel vous les publiez.

• Certains espaces de publication et de partage sont totalement publics et ne permettent pas de restreindre la visibilité des photos. Il est important d'avoir conscience que les photos qui y sont partagées sont alors accessibles à tout le monde et d'adapter le contenu en conséquence.

• Évitez d'utiliser la même photo de profil sur des sites ayant des finalités différentes (Facebook, Viadéo ou LinkedIn, Meetic), la photo pouvant être utilisée (moteur de recherche d'images) pour faire le lien entre les différents profils.

2 Limitez l'accès aux photos que vous publiez sur les réseaux sociaux.

Il est important de bien définir dans les paramètres de confidentialité quel groupe d'amis a accès à quelle photo ou à quel album photo. Sur Facebook, ce contrôle de l'accès peut passer par la création de listes d'amis et le paramétrage des albums photos ou de chaque photo publiée.

3 Assurez-vous que la personne dont vous voulez publier la photo est bien d'accord. Il est préférable de s'assurer qu'une photo dans laquelle elle apparaît n'incommode pas une personne avant de la publier.

4 Contrôlez la manière dont vous pouvez être identifié (« taggué ») sur les photos dans lesquelles vous apparaissez et qui sont publiées sur les réseaux sociaux.

Il est généralement possible de paramétrer la façon dont vous pouvez être taggué sur les réseaux sociaux de manière à :

• Déterminer les contacts ou listes de contacts autorisés à vous identifier ;

• Recevoir une alerte lorsqu'un contact souhaite vous identifier afin de l'approuver (ou non) ;

• Être alerté lorsque vous êtes identifié dans une photo / publication

5 Faites attention à la synchronisation automatique des photos, en particulier sur smartphone, tablette ou sur les nouveaux appareils photos numériques connectés.

L'activation de cette fonctionnalité permet de synchroniser automatiquement toute nouvelle photo prise avec le terminal concerné dans un dossier stocké en ligne (ex. : « Flux de photos » d'Apple, « Instant Upload » de Google+ ou « Photo Sync » de Facebook). Il est recommandé de ne l'activer que si vous avez l'intention réelle de publier ces photos. Ces services ont en effet vocation à faciliter le partage des photos et non à les sauvegarder, comme peut le proposer un coffre-fort numérique. En outre, il vous sera plus difficile de supprimer les photos une fois qu'elles seront synchronisées en ligne. Vous aurez alors à vous rendre sur chacun des espaces de synchronisation pour les effacer manuellement. Qui plus est, même si ces photos ne sont pas automatiquement rendues publiques, elles sont accessibles à l'éditeur du site ou service et pourraient être utilisées par lui pour affiner votre profil, par exemple à des fins publicitaires.

2.
CONSEILLER ET RÉGLEMENTER

TAJ : UN NOUVEAU FICHIER D'ANTÉCÉDENTS POUR REMPLACER LE STIC ET LE JUDEX

Le décret n° 2012-652 du 4 mai 2012, pris après l'avis de la CNIL du 7 juillet 2011, a créé le traitement d'antécédents judiciaires (TAJ), en remplacement du STIC et du JUDEX, mis en œuvre respectivement par la police et la gendarmerie nationale. Ce nouveau traitement, qui est le plus important fichier utilisé par les services enquêteurs, a pour finalité de faciliter la constatation d'infractions, le rassemblement de preuves et la recherche des auteurs d'infractions. S'il apporte de nouvelles garanties pour les personnes, il a également suscité quelques réserves de la part de la CNIL.

Créé en application des articles 230-6 à 230-11 du Code de procédure pénale, le traitement d'antécédents judiciaires (TAJ) constitue un fichier d'antécédents commun à la police et à la gendarmerie nationale, en remplacement du STIC (système de traitement des infractions constatées) et du JUDEX (système judiciaire de documentation et d'exploitation), qui seront définitivement supprimés le 31 décembre 2013. Comme ces fichiers d'antécédents judiciaires, TAJ sera utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et des enquêtes administratives (par exemple, les enquêtes préalables à certains emplois publics ou sensibles). Ses principales caractéristiques sont semblables à celles des fichiers STIC et JUDEX, notamment pour ce qui concerne les données traitées, leurs durées de conservation et les destinataires de ces données.

La CNIL avait procédé au contrôle du STIC dans le cadre de son programme de contrôle pour l'année 2007. Elle avait alors constaté et mis en lumière plusieurs dysfonctionnements dans un rapport remis au Premier ministre en date du 20 janvier 2009, lequel était ponctué par 11 recommandations, concernant tout particulièrement les conditions d'utilisation du traitement à des fins administratives.

Les ministères de l'Intérieur et de la Justice avaient alors considéré qu'une automatisation complète de la chaîne pénale (constatation de l'infraction, enquête judiciaire, jugement et exécution de la peine), *via* diverses interconnexions, permettrait d'éviter les risques d'erreur et d'améliorer le fonctionnement de ces fichiers. Par ailleurs, le ministère de l'Intérieur a jugé nécessaire de mutualiser les fichiers d'antécédents de la police et de la gendarmerie.

LES NOUVELLES GARANTIES OFFERTES PAR TAJ

La loi d'orientation et de programmation de la performance de la sécurité intérieure (LOPPSI) du 14 mars 2011 a introduit une section relative aux fichiers d'antécédents au sein du Code de procédure pénale. Si ces dispositions reprennent le cadre général qui avait été défini par l'article 21 de la loi du 18 mars 2003 sur la sécurité intérieure, de nouvelles garanties, notamment de mise à jour des données, sont applicables au TAJ.

Les conditions de mise à jour des données qui sont enregistrées dans TAJ ont été renforcées.

En effet, les suites décidées par l'autorité judiciaire devraient être à terme renseignées automatiquement dans TAJ grâce à une interconnexion avec le traitement CASSIOPEE utilisé par les juridictions. Cette évolution devrait permettre d'éviter l'absence de mise à jour à l'issue de la procédure judiciaire (classement sans suite, acquittement, non lieu). Ce problème essentiel du fichier STIC avait été révélé par les contrôles de la CNIL.

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

- Toutes les décisions de classement sans suite seront dorénavant mentionnées ;

FOCUS

Un nouveau contrôle du STIC en cours

Au vu des enjeux pour les droits et libertés des citoyens, la Commission a souhaité inscrire au programme annuel des contrôles de l'année 2012 une nouvelle série de vérifications. Elles ont pour objet de mesurer le degré d'application des recommandations formulées en 2009 ainsi que l'effectivité des nouvelles dispositions législatives. Ce contrôle s'inscrit dans la perspective de la mise en œuvre du TAJ. Il est en effet essentiel que la CNIL vérifie à ce stade la qualité des données qui ont vocation à y être versées. Une attention particulière est ainsi portée, lors des contrôles, à la transmission des suites judiciaires par les procureurs de la République pour la mise à jour, voire l'effacement, des données dans le fichier STIC.

- Il sera impossible de consulter les données relatives aux personnes ayant fait l'objet d'une mention dans le cadre des enquêtes administratives ;
- Les parquets ont l'obligation de répondre aux demandes de rectification et d'effacement dans un délai d'un mois et transmettront directement au ministère de l'Intérieur les décisions prises.

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

UN FICHIER AVEC DE NOUVELLES FONCTIONNALITÉS

TAJ offre des nouveaux outils d'analyse et de rapprochement des données permettant de réaliser des recherches d'éléments communs dans des procédures différentes ainsi que de nouvelles fonctionnalités d'identification des personnes.

Pour la première fois dans un fichier de police, des procédés de reconnaissance faciale des personnes à partir de la photographie de leur visage sont mis en œuvre. Par exemple, les personnes impliquées dans une infraction, et dont le visage aura été filmé par une caméra de vidéoprotection, pourront être automatiquement identifiées si elles ont déjà une fiche dans TAJ, c'est-à-dire si elles sont déjà connues par les services de police et de gendarmerie.

Dans son avis sur le projet de décret, la CNIL a considéré que cette fonctionnalité d'identification voire de localisation des personnes à partir de l'analyse biométrique de la morphologie de leur visage, présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection. Elle sera donc particulièrement attentive à cette nouvelle utilisation des fichiers d'antécédents.

Enfin, le nouveau fichier fait l'objet d'un triple contrôle. Il est tout d'abord soumis au contrôle de la CNIL et fera l'objet d'une vérification globale à l'issue de son déploiement sur l'ensemble du territoire national. Par ailleurs, les procureurs de la République sont chargés de demander la mise à jour des données et ont également pour responsabilité essentielle de contrôler la qualification pénale des faits, laquelle détermine la durée de conservation des données enregistrées, pouvant aller jusqu'à quarante ans. Ce traitement est enfin contrôlé par un magistrat dit « référent », chargé de contrôler la mise en œuvre du traitement et la mise à jour des données. ■

> La fonctionnalité de reconnaissance faciale présente des risques importants pour les libertés individuelles

TAJ DEVRAIT CONCERNER :

61 194 991
PROCÉDURES

12 057 515
PERSONNES PHYSIQUES MISES EN CAUSE

39 819 811
PERSONNES PHYSIQUES VICTIMES

CAMPAGNES ÉLECTORALES 2012 : QUEL BILAN DE L'UTILISATION DES FICHIERS, QUELLES PROPOSITIONS D'AMÉLIORATION ?

Dans la perspective des élections présidentielles et législatives organisées au printemps 2012, la CNIL a actualisé ses recommandations en matière de communication politique, au regard notamment des récentes évolutions technologiques. Elle a également mis en place un observatoire interne, pendant l'ensemble des campagnes électorales nationales de l'année 2012, afin de renseigner les citoyens sur leurs droits et les partis politiques sur leurs obligations en matière de protection des données.

DES INSTRUMENTS JURIDIQUES ET PRATIQUES MIS À JOUR

Des recommandations revues et augmentées

Adoptées en 1991, puis révisées en 1996 et 2005, les recommandations de la CNIL en matière de fichiers mis en œuvre dans le cadre d'activités politiques ont été actualisées en janvier 2012, après consultation des principaux partis politiques. Cette mise à jour poursuivait trois objectifs :

1 Recenser les fichiers pouvant être utilisés à des fins de communication politique

La CNIL a souhaité rappeler les conditions d'accès et d'utilisation des fichiers constitués par les partis ou les candidats, de certains fichiers publics (listes électorales, répertoire national des élus et des candidats, par exemple) et des fichiers de prospection commerciale loués ou achetés à des sociétés privées.

2 Préciser les opérations de communication possibles vers les différents interlocuteurs des partis et candidats

La CNIL a fixé le cadre des « primaires » et des consultations internes à un parti. Elle a également rappelé les règles applicables selon la nature des rapports qu'un parti ou un élu entretient avec ses membres, ses soutiens, ses contacts ou de simples citoyens.

3 Prendre en compte le recours aux nouvelles technologiques à des fins de communication politique

La CNIL a précisé le cadre « Informatique et Libertés » et les garanties à adopter pour mener des opérations de communication par l'intermédiaire de courriers électroniques, de SMS, des

réseaux sociaux, des sites de « microblogging » ou des pétitions en ligne.

Des supports pratiques actualisés et une déclaration facilitée

La Commission a élaboré un nouveau guide pratique relatif à la communication politique. Véritable « manuel de campagne à l'ère numérique », il recense les bonnes pratiques à adopter par les partis et les candidats en fonction du fichier utilisé, de la population visée et du support de communication choisi. Ce guide est illustré par de nombreux exemples, cas concrets et modèles de mentions qui aident les partis, candidats et leurs prestataires à se conformer à leurs obligations légales et aux recommandations de la Commission.

La CNIL a également mis à jour la norme simplifiée applicable aux opérations de communication politique (NS n° 34) pour faciliter le respect de l'obligation déclarative qui incombe aux responsables de traitement. Ce guide pratique et cette norme simplifiée sont accessibles en ligne, sur le site web de la CNIL (www.cnil.fr).

LA MISE EN PLACE D'UN OBSERVATOIRE DES ÉLECTIONS

Les missions et les travaux

À la veille d'une intense période d'activité électorale, pendant laquelle les données personnelles des électeurs allaient susciter beaucoup d'intérêt, la Commission a mis en place un observatoire interne des élections. Les missions de cette structure légère et réactive ont principalement consisté à :

- identifier les nouvelles pratiques de communication politique et celles suscitant des difficultés au regard de la protection des données ;
- répondre aux témoignages et instruire les plaintes reçues à l'occasion des élections ;
- mettre à disposition des électeurs et des acteurs des campagnes électorales des supports pratiques répondant à leurs questions ;
- établir un bilan de ses travaux et émettre des propositions afin d'améliorer les pratiques constatées du point de vue de la protection des données ;
- sensibiliser les formations et les responsables politiques dans la perspective des consultations et scrutins à venir.

Le bilan et les propositions

Le bilan dressé par l'Observatoire à l'issue des élections présidentielles et législatives fait apparaître que **la prospection par message électronique a concentré l'essentiel des critiques des citoyens**. Deux points en particulier doivent faire l'objet d'améliorations significatives :

- **l'information des destinataires doit obligatoirement porter sur** les modalités d'exercice des droits reconnus par la loi et la procédure de désabonnement. La Commission recommande aussi que l'origine des données utilisées (fichier de contacts, listes électorales communales ou consulaires, base de données commerciale louée, etc.), la fréquence d'envoi et l'identité des émetteurs de messages (candidat, équipe du candidat, fédération locale, etc.) soient précisés.
- **l'effectivité du droit d'opposition a suscité de nombreuses difficultés pendant les deux campagnes (absence de lien de désinscription, lien ne fonctionnant pas, boîte de réception pleine, etc.)**. Les demandes de désabonnement doivent

▸▸▸

INFOS +

Les fiches pratiques de l'Observatoire

• Le tract : de la feuille volante au fichier informatique ;
• Les kits de campagne et la loi « Informatique et Libertés » ;
• Les listes électorales consulaires en questions ;
• La communication politique par courrier électronique en questions ;
• Politique et Internet : quelques conseils pour une navigation plus Net ! ;
• Communication politique : rappel des droits et obligations « Informatique et Libertés ».

Ces documents sont accessibles en ligne, à l'adresse : http://www.cnil.fr/elections/

La prospection par message électronique a concentré l'essentiel des critiques des citoyens

FOCUS

Les élections organisées en 2012 ont suscité 327 témoignages et 156 plaintes auprès de la CNIL, les deux tiers (67 %) émanant de Français de l'étranger.

Modes de prospection mis en cause :
- **e-mail : 86 %**
- **courrier : 6 %**
- **SMS : 2 %**
- **téléphone fixe : 1,5 %**
- **réseaux sociaux et blogs : 1,5 %**

Principaux motifs de plaintes :
- **la réception non sollicitée de messages : 87 %**
- **leur fréquence excessive : 49 %**
- **les problèmes de désabonnement :**
  - **absence de prise en compte : 70 %,**
  - **absence de lien de désinscription : 23 %,**
  - **présence d'un lien non valide : 7 %.**

▸▸▸

donc être facilitées et prises en compte immédiatement (« un clic pour s'abonner, un clic pour se désabonner »). Si plusieurs expéditeurs (candidat, équipe du candidat, fédération locale, etc.) utilisent la même base d'adresses électroniques, les demandes d'oppositions reçues par l'un doivent être répercutées aux autres.

Les propositions

Les problèmes identifiés par l'Observatoire soulignent **la nécessité de mieux encadrer la prospection politique, tout particulièrement lorsqu'elle est effectuée par message électronique**.

La CNIL propose donc que ce mode de communication soit soumis aux mêmes règles que la prospection commerciale et, notamment, que l'envoi de messages électroniques de prospection politique soit limité aux seules personnes ayant préalablement consenti à cette utilisation de leurs données.

De même, la fréquence d'envoi des courriers électroniques, mais aussi des SMS et des MMS, le traitement des demandes d'opposition à recevoir de nouveaux messages, les mentions d'information minimales devant figurer dans chaque message sont autant de sources de difficultés. Ces sujets mériteraient donc de faire l'objet de précisions réglementaires dans le code électoral.

Enfin, un effort particulier d'information et de protection des données doit être accompli par le ministère des Affaires Étrangères s'agissant des listes électorales consulaires puisque la loi impose d'y faire figurer l'adresse électronique fournie lors de l'inscription au registre des Français de l'étranger tenu par chaque consulat.

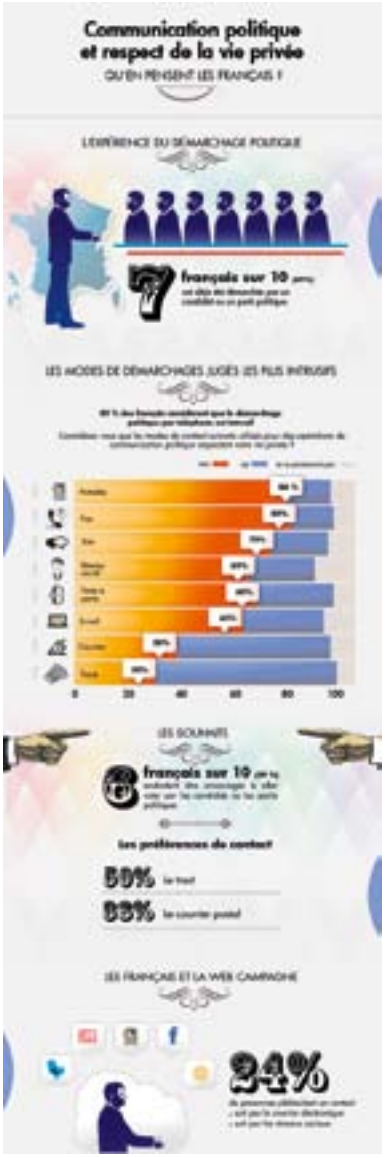
La CNIL a adressé au Gouvernement diverses propositions de modification du cadre juridique actuel tirant les enseignements des travaux de l'Observatoire.

L'Observatoire après les élections de 2012

L'amélioration de la protection des données en période électorale passe par une collaboration accrue avec tous les acteurs concernés : partis politiques et leurs courants, candidats, comités de soutien, sociétés pourvoyeuses de fichiers de prospection ou sous-traitants chargés des opérations de communication politique. Des rencontres ont déjà eu lieu afin de sensibiliser les principales formations politiques à ces questions et de leur présenter les avantages de la désignation de correspondant « Informatique et Libertés ».

De même, la concertation avec les sociétés louant des fichiers de prospects et les prestataires réalisant les campagnes de prospection va se poursuivre afin de mieux leur faire connaître les recommandations de la CNIL en la matière.

Enfin, la CNIL va continuer de collaborer avec les ministères concernés et suivre l'état de la réflexion du Gouvernement sur ses propositions. ■



RELATIONS AVEC LE PARLEMENT : LA PROTECTION DES DONNÉES AU CŒUR DE NOMBREUX TRAVAUX

La protection des données personnelles a occupé une place importante dans les travaux parlementaires en 2012, comme en atteste, notamment, les nombreuses initiatives législatives portant, par exemple, sur la lutte contre le surendettement, la tarification progressive de l'énergie, le projet de Règlement européen… qui ont rythmé les travaux du Parlement.

Alors que l'année 2012 a été marquée par une suspension des travaux des deux assemblées de près de quatre mois, en raison des élections présidentielle et législatives, la CNIL a participé à plus d'une vingtaine de rendez-vous et d'évènements parlementaires (auditions, rendez-vous de travail…), au cours desquels elle a répondu aux questions des parlementaires, informé et sensibilisé les élus de l'ensemble des groupes politiques aux questions « Informatique et Libertés », et aux enjeux dont est porteuse la révolution numérique que connaissent nos sociétés.

Les deux assemblées se sont notamment exprimées dans des termes identiques par deux résolutions européennes sur la proposition de Règlement européen relatif à la protection des données personnelles, partageant les positions exprimées par la CNIL.

En outre, au-delà de l'expertise juridique et technique qu'elle a mise à disposition du Parlement sur de nombreuses initiatives législatives, la Commission a mis en œuvre différentes opérations de sensibilisation à l'attention des parlementaires : participation à des colloques et tables rondes, envoi régulier de notes d'informations sur l'ensemble des thématiques intéressant les élus, participation à des rendez-vous organisés avec les présidents des deux assemblées et de certaines commissions permanentes, etc.

Pour la première fois, notre Commission a organisé, le 28 novembre 2012, une réunion de travail à l'Assemblée nationale, à l'attention de l'ensemble des députés et de leurs collaborateurs, sur le thème « *Révolution numérique et vie privée : vos données les intéressent !* ». Cette rencontre a donné lieu à des démonstrations développées par les services de la CNIL, qui illustrent l'impact potentiel des nouvelles technologies sur la vie privée de nos concitoyens. Un évènement identique sera proposé au Sénat dans le courant de l'année 2013.

Les principales initiatives législatives intéressant la CNIL :

- Rejet, le 26 janvier 2012, de la proposition de loi tendant à prévenir le surendettement ;
- Adoption de deux résolutions européennes (n°888 et 105), par l'Assemblée nationale et le Sénat, sur le projet de Règlement européen en matière de protection des données personnelles ;
- Promulgation, le 27 mars 2012, de la loi relative à la protection de l'identité ;
- Auditions menées par la commission sénatoriale pour le contrôle de l'application des lois sur l'application de la législation française concernant la sécurité intérieure et en matière de lutte contre le terrorisme ;
- Début des travaux menés par le groupe de travail sénatorial sur le répertoire national des crédits aux particuliers ;

- Début des travaux parlementaires sur la proposition de loi instaurant une tarification progressive de l'énergie ;
- Publication, le 26 septembre, du rapport d'information (n°784) sénatorial sur les effets sociétaux de la révolution numérique. ■

GROS PLAN

CLOUD COMPUTING : QUELS CONSEILS AUX ENTREPRISES ?

> Le cloud, une révolution majeure à utiliser de manière responsable ”

Les offres de « *cloud computing* » se sont fortement développées ces dernières années. Cependant, le recours par les entreprises à ces services pose des questions nouvelles en termes juridiques et de gestion des risques. Afin d'aider les organismes français, notamment les PME, qui souhaitent avoir recours à des prestations de cloud, la CNIL a publié un ensemble de recommandations pratiques.

> 94 % des PME s'intéressent à des offres de SaaS[2]

LE CLOUD : QU'EST-CE QUE C'EST ?

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

Le *cloud computing* est une évolution majeure des services informatiques d'une organisation. Il propose de nombreux avantages, notamment celui de mutualiser les coûts d'hébergement et d'opérations. Toutefois, les questions de sécurité, de qualification du prestataire, de loi applicable et de transfert des données sont particulièrement délicates dans le cadre du *cloud computing*. Les organisations souhaitant recourir à ces services ont donc besoin d'une clarification des responsabilités y afférant.

Or, la gamme d'offres correspondantes a connu un fort développement ces quatre dernières années, notamment au travers du stockage et de l'édition en ligne de documents, ou même des réseaux sociaux par exemple. De nombreuses offres de services de *cloud computing* sont désormais disponibles sur le marché, que ce soit pour l'hébergement

d'infrastructures (IaaS – Infrastructure as a Service), la fourniture de plateformes de développement (PaaS – Platform as a Service) ou celle de logiciels en ligne (SaaS – Software as a Service). Ces offres sont proposées dans des cloud publics (service partagé et mutualisé entre de nombreux clients), privés (cloud dédié à un client) ou hybrides (combinaison des modèles public et privé).

À la suite de la consultation publique menée en 2011, la CNIL a publié en juin 2012 un ensemble de recommandations à destination des organismes qui souhaitent avoir recours à des prestations de cloud et notamment les PME. Ces recommandations sont assorties de modèles de clauses contractuelles qui peuvent être insérés dans les contrats de services de *cloud computing* afin de couvrir les questions liées à la protection des données à caractère personnel.

LES ÉTAPES À SUIVRE LORS D'UN PASSAGE AU *CLOUD COMPUTING*

1 **Cartographier les données et les traitements** : quelle est la nature des données et des traitements que l'on pense transférer dans le cloud ?

2 **Définir ses exigences de sécurité technique et juridique** : quelles sont les exigences légales et normatives ? (par exemple, les données de santé ne peuvent être hébergées que par un prestataire agréé par le Ministre de la Santé).

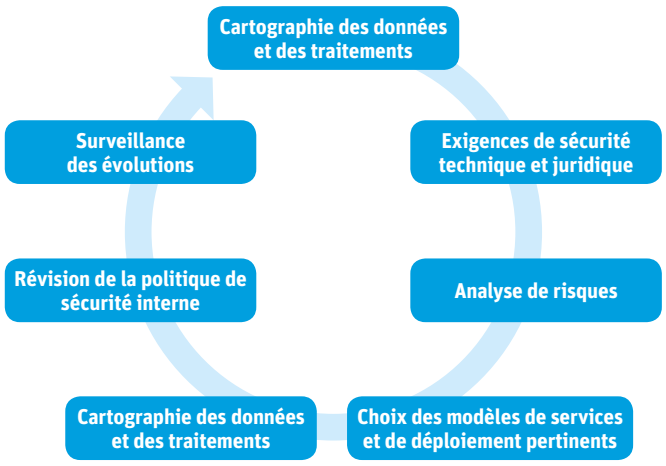
3 **Analyser les risques nouveaux engendrés par le passage dans le cloud** : réfléchir à l'impact sur les personnes concernées et sur l'organisme d'un passage des données et traitements identifiés dans le cloud, par exemple en ce qui concerne la perte de gouvernance sur le traitement, la dépendance technologique vis-à-vis du fournisseur de *cloud computing*, ou les réquisitions judiciaires, notamment par des autorités étrangères.

4 **Choisir des modèles de services (IaaS, PaaS ou SaaS)**[3] **et de déploiement (privé, public ou hybride)**[4] **pertinents** : en fonction des résultats de l'analyse de risques et des exigences définies à la seconde étape, différents types de cloud pourront être envisagés.

5 **Choisir un prestataire présentant des garanties suffisantes** : la CNIL propose dans ses recommandations un ensemble d'éléments pour identifier un prestataire « de confiance ». Pour cela, un prestataire doit être transparent et doit fournir à ses clients des garanties juridiques (ex : engagement que les durées de conservation sont limitées, raisonnables et proportionnelles aux finalités de collecte des données) et techniques (ex : droit du client d'auditer ou de faire auditer son prestataire sous-traitant) suffisantes en matière de protection des données à caractère personnel. La CNIL met à disposition dans ses recommandations une liste des éléments essentiels devant figurer dans un contrat de prestation de *cloud computing* qui permet d'évaluer si un prestataire fournit des garanties suffisantes.

6 **Réviser sa politique de sécurité interne** afin de prendre en compte les conclusions de l'analyse de risques et d'adapter les procédures internes en conséquence.

7 **Surveiller les évolutions dans le temps** et mettre à jour l'analyse de risques si nécessaire, afin de s'assurer que le service utilisé est toujours adapté. ■



[1] Bien avant qu'apparaisse l'expression « cloud computing «, les architectes réseau schématisaient internet par un nuage. En anglais, le terme « the cloud « était couramment utilisé pour désigner Internet. / [2] Enquête Markess International, « 6e Baromètre des Prestataires Cloud Computing », www.evoliz.com/blog/67-20120412-barometre-prestataires-cloud-computing-markess-international-2012.html / [3] IaaS (« Infrastructure as a Service ») désigne la fourniture d'infrastructures de calcul et de stockage en ligne - PaaS (« Platform as a Service ») désigne la fourniture d'une plateforme de développement d'applications en ligne - SaaS (« Software as a Service ») désigne la fourniture de logiciels en ligne. / [4] Un cloud est privé lorsqu'il est dédié à un seul client, au contraire du cloud public qui désigne un service partagé et mutualisé entre de nombreux clients. Le cloud hybride est un service partiellement public et partiellement privé.

BIOMÉTRIE : L'AUTORISATION UNIQUE AU-007 NE PORTE PLUS SUR LES CONTRÔLES D'HORAIRES DES SALARIÉS

L'autorisation unique n°7 (AU-007) concerne les dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès des salariés et des visiteurs ainsi que la restauration sur les lieux de travail. Depuis le 12 octobre 2012, elle ne couvre plus la finalité de gestion des horaires des salariés.

L'EXCLUSION DE LA FINALITÉ DE CONTRÔLE HORAIRE DES SALARIÉS

Ces dernières années, les techniques de contrôle des salariés sur leurs lieux de travail ont connu un essor sans précédent (géolocalisation, cybersurveillance, biométrie, etc.). Face au recours croissant à des dispositifs biométriques reposant sur la reconnaissance du contour de la main, la Commission a souhaité recueillir l'avis d'organisations syndicales et patronales, de la Direction Générale du travail ainsi que de certains professionnels du secteur. La problématique de la biométrie comme outil de gestion des présences et de contrôle des horaires a donc été analysée au regard de la loi « Informatique et Libertés » et dans le respect du code du travail.

> Un consensus s'est clairement exprimé pour considérer comme disproportionnée l'utilisation de la biométrie aux fins de contrôle des horaires

La Commission s'est toujours montrée vigilante concernant les données biométriques ayant les particularités d'être uniques, irréversibles et permanentes. Elles permettent en effet d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales (empreinte digitale, contour de la main, etc.). Elles ne sont pas attribuées par un tiers ou choisies par la personne. Elles sont produites par le corps lui-même et le désigne de façon définitive permettant de ce fait le « traçage » des individus, ainsi que leur identification certaine.

Le caractère sensible de ces données[1] justifie que la loi « Informatique et Libertés » prévoie un contrôle spécifique de la CNIL fondé essentiellement sur la proportionnalité du dispositif au regard de la finalité recherchée, telle la gestion des horaires. Le 27 avril 2006, la Commission avait adopté une autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et identifiant une triple finalité : le contrôle d'accès aux locaux de l'entreprise et à la restauration sur les lieux de travail, ainsi que la gestion des horaires (AU-007).

À la suite de plus d'une dizaine d'auditions, notamment avec les syndicats de salariés ou patronaux, un consensus s'est clairement exprimé pour considérer comme disproportionnée l'utilisation de la biométrie aux fins de contrôle des horaires. La raison principale en était le risque accru de détérioration du climat social, allant à l'encontre de la relation de confiance employeur-salarié.

Dès lors, la Commission a décidé de modifier l'AU-007 qui autorisait l'utilisation du contour de la main aux fins de gestion des horaires. Désormais, aucun dispositif biométrique, y compris ceux reposant sur le contour de la main, ne peut permettre de contrôler les horaires des salariés, sauf circonstances exceptionnelles dont doit justifier l'organisme demandeur. Les dispositifs de reconnaissance du contour de la main ne sont pas interdits en tant que tels. Le contrôle d'accès et la restauration d'entreprise sont ainsi toujours couverts par l'autorisation unique n° 7 (délibération n° 2012-322 du 20 septembre 2012 modifiant l'AU-007).

QUELLE EST LA PORTÉE DE LA MODIFICATION DE L'AU-007 ?

L'autorisation unique est un moyen de simplification des formalités préalables relatives à un certain type d'usages. Elle permet aux responsables de traitement concernés de répondre à leur obligation légale de déclarer le traitement au moyen d'un simple engagement de conformité disponible sur le site de la CNIL.

À titre transitoire, les organismes qui recourent déjà à un dispositif pour contrôler les horaires de leur personnel et qui ont effectué un engagement de conformité avant la publication de cette nouvelle délibération le 12 octobre 2012, pourront continuer à l'utiliser pendant une période de cinq ans. Passé ce délai, ils devront cesser de recourir à la fonctionnalité biométrique du dispositif pour le contrôle des horaires, ce qui n'impliquera pas systématiquement de changer de matériel. Les organismes pourront en effet paramétrer le système pour inhiber la fonction biométrique et utiliser, à la place, des codes, cartes et/ou badges sans biométrie.

En outre, les entreprises qui souhaitent mettre en œuvre un contrôle des horaires par biométrie peuvent toujours déposer une demande d'autorisation spécifique sur le fondement de l'article 25-I-8° de la loi du 6 janvier 1978 modifiée, sous réserve de faire état d'une justification particulière. ■

1 230

ENGAGEMENTS DE CONFORMITÉ À L'AU-007 ONT ÉTÉ ENREGISTRÉS AUPRÈS DE LA CNIL

[1] *Même si celles-ci ne figurent parmi les données visées dans l'article 8 de la loi du 6 janvier 1978 modifiée.*

GROS PLAN

LES COMPTEURS COMMUNICANTS :

UNE INNOVATION ACCOMPAGNÉE PAR DES PREMIÈRES RECOMMANDATIONS

« La CNIL étudie les impacts des compteurs sur la vie privée des personnes »

De nouveaux compteurs, dits compteurs communicants, seront déployés dans toute la France à partir de 2014. Ces compteurs vont collecter beaucoup plus de données que les compteurs actuels et pourront permettre de déduire des informations sur les habitudes de vie des personnes. Au vu des risques présentés par ces compteurs en termes d'atteintes potentielles au respect de la vie privée, la CNIL a adopté une première recommandation pour encadrer leur utilisation.

Le compteur communicant est une des composantes des réseaux de distribution d'énergie intelligents (également appelés « *smart grids* »). Ces réseaux utilisent des moyens informatiques évolués afin d'optimiser la production et l'acheminement de l'électricité. Ils devraient également permettre de faciliter la facturation des abonnés, ainsi que la réalisation de certaines opérations techniques à distance (coupure ou changement de puissance du compteur, par exemple).

Les compteurs communicants commenceront à être déployés dans toute la France à partir de 2014 et devraient concerner environ 35 millions de foyers d'ici à 2020.

La CNIL mène depuis plus de deux ans une réflexion sur ces compteurs et étudie notamment leur impact sur la vie privée des personnes.

En effet, leur futur déploiement n'est pas sans risque, tant au regard du nombre et du niveau de détail des données qu'ils permettent de collecter, que des problématiques qu'ils soulèvent en termes de sécurité et de confidentialité de ces données.

UNE MULTIPLICATION DU NOMBRE DE DONNÉES COLLECTÉES

Les compteurs électriques permettent de calculer la consommation d'électricité d'un foyer grâce aux index de consommation.

Les compteurs actuels peuvent avoir au maximum deux index, l'un pour les heures pleines et l'autre pour les heures creuses. Disposer de plusieurs index permet en effet au fournisseur d'énergie (EDF ou Poweo, par exemple) d'appliquer des tarifs différenciés (un tarif normal le jour et un tarif réduit la nuit, par exemple).

Ces index sont aujourd'hui relevés manuellement par un agent du fournisseur d'énergie qui se déplace au domicile de l'abonné : c'est ce qu'on appelle la relève à pied des compteurs. Cette relève a lieu au mieux tous les 6 mois, au pire tous les 2 ans.

Les nouveaux compteurs disposeront de dix index journaliers, ce qui permettra au fournisseur d'énergie d'appliquer jusqu'à dix tarifs différents en fonction de l'heure de la journée. En outre, ces index seront relevés, non plus tous les 6 mois au mieux, mais tous les jours, grâce à la télétransmission des données. La relève à pied a donc vocation à disparaître.

Cette augmentation du nombre des index et de la fréquence de leur relève permettra au fournisseur d'énergie de facturer les clients sur du réel (et non plus sur la base d'estimations), de réguler la production et de proposer des tarifs d'énergie plus complexes.

INFOS +

Qu'est-ce qu'un index de consommation ?

L'index de consommation est le chiffre qui apparaît sur le compteur et qui, comparé au dernier index relevé, permet de calculer la consommation d'électricité du ménage.

Index de fin de période – index de début de période = quantité d'énergie consommée sur la période

> Le nombre d'index va être multiplié par 5 et la fréquence de relève de ces index par 180

UNE CONNAISSANCE PLUS FINE DES HABITUDES DE VIE DES PERSONNES

Le principal risque présenté par ces nouveaux compteurs provient d'une nouvelle fonctionnalité offerte par les compteurs communicants, à savoir la courbe de charge. Cette courbe de charge est constituée d'un relevé, à intervalles réguliers, de la consommation électrique d'un abonné. Une analyse approfondie de cette courbe de charge peut permettre de déduire un grand nombre d'informations sur les habitudes de vie des personnes. En effet, plus les relevés sont rapprochés, plus la courbe de charge est précise et plus il est possible d'en déduire des informations. Par exemple, une courbe de charge avec une mesure toutes les 10 minutes permet notamment d'identifier les heures de lever et de coucher, les heures ou périodes d'absence, la présence d'invités dans le logement, les prises de douche, etc.

Cette courbe de charge ne servira pas à facturer le client, les index de consommation suffisant à procéder à cette facturation. En revanche, elle permettra au gestionnaire de réseau (ERDF, par exemple) de mieux gérer son réseau basse tension. Elle permettra également au fournisseur d'énergie de proposer des tarifs adaptés à la consommation des ménages, mais également à des sociétés spécialisées de faire des diagnostics énergétiques et de proposer des travaux de rénovation ciblés (remplacement des fenêtres, par exemple).

▸▸▸

LES ACTIONS DE LA CNIL

Au vu de ces risques pour la vie privée des personnes, la Commission a adopté une première recommandation afin d'encadrer l'utilisation des compteurs communicants.

Cette recommandation, adoptée au regard des connaissances techniques du moment, pose notamment comme principe que la courbe de charge ne peut être collectée de façon systématique, mais uniquement lorsque cela est justifié pour réaliser des travaux sur le réseau ou lorsque l'abonné en fait expressément la demande pour bénéficier de services particuliers (tarifs adaptés à la consommation, bilans énergétiques, par exemple).

Elle pose également un certain nombre d'exigences en termes de sécurité, des garanties sérieuses devant être apportées pour assurer la confidentialité des données. Elle prévoit notamment la réalisation d'études d'impact sur la vie privée avant le déploiement des compteurs et d'analyses de risques pour déterminer les mesures techniques adéquates à mettre en place.

La CNIL mène en parallèle des travaux sur les nouveaux produits et services qui seront installés hors de l'infrastructure des compteurs (par exemple, directement sur le tableau électrique, en aval des compteurs). En effet, les logements seront bientôt équipés de multiples objets connectés qui permettront d'agir sur la température du logement, de baisser les volets en fonction du niveau d'ensoleillement, de lancer le préchauffage d'un four, etc. Ces produits et services collecteront des données encore plus détaillées que celles collectées par les compteurs eux-mêmes. ■

35
MILLIONS DE FOYERS SERONT CONCERNÉS D'ICI À 2020

FOCUS

Pour définir les règles qui viendront encadrer ces futurs traitements, la Commission a récemment mis en place un partenariat avec la Fédération des Industries Électriques, Électroniques et de Communication (FIEEC). Dans ce cadre, un groupe de travail a été créé afin d'aboutir à la publication de bonnes pratiques, en concertation avec les industriels du secteur. Ces bonnes pratiques devraient être disponibles à l'été 2013. Elles constitueront, avec les recommandations, un premier « pack de conformité » pour le secteur de l'énergie.

3. ACCOMPAGNER LA CONFORMITÉ

2012 : l'année des premiers labels

Le correspondant : acteur essentiel de la conformité des organismes

GROS PLAN

Vidéosurveillance/vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée

Pour mieux gérer les risques sur la vie privée : suivez le guide

Bientôt un « pack de conformité » dédié au logement social

2012 : L'ANNÉE DES PREMIERS LABELS

Depuis un an, la loi « Informatique et Libertés » permet à la CNIL de délivrer des labels « à des produits ou des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel », une fois qu'elle les a reconnus conformes aux dispositions à la loi (article 11).

Afin de délivrer des labels, la CNIL élabore un mécanisme en deux temps. Dans un premier temps, elle adopte, sur proposition du Comité de labellisation et à l'initiative d'organisations professionnelles et d'institutions, un référentiel relatif à des produits ou des procédures. Dans un second temps, les demandeurs peuvent déposer une demande d'homologation individuelle au regard de ces référentiels.

L'objectif de cette labellisation est d'attester de la qualité des produits ou procédures. En effet, le label CNIL permet aux organismes de se distinguer en garantissant un haut niveau de protection des données. Pour les utilisateurs, c'est également un indicateur de confiance qui permet ainsi d'identifier et de privilégier les organismes respectueux de leurs données.

Les labels sont délivrés pour une durée limitée de trois ans, renouvelable au moins six mois avant l'échéance. Si les procédures concernées font l'objet d'une modification dans ce délai, l'organisme

> Le label CNIL permet aux organismes de se distinguer par la qualité de leur service

25
DEMANDES DE DÉLIVRANCE DE LABELS

10
LABELS DÉLIVRÉS[1]

[1] *À la date du 15 février 2013*

FOCUS

Comment déposer une candidature ?

Pour obtenir un label CNIL, les organismes doivent se conformer aux exigences d'un référentiel déjà établi par la CNIL, justifier la conformité de la procédure ou du produit labellisé à travers un dossier de candidature (téléchargeable depuis le site internet de la CNIL et à retourner par courrier postal ou par courrier électronique à l'adresse dédiée « label[at]cnil.fr ») et fournir, pour chaque exigence, des éléments de justification (procédures internes, contrats types…).
Le dossier de candidature comprend des exigences relatives à la méthode de la procédure (EM) et à son contenu (EC et ES pour les modules complémentaires des formations). Les exigences relatives à la méthode (EM) et au contenu principal de la procédure (EC) sont toutes obligatoires.

ayant obtenu le label devra en informer automatiquement la Commission.

La CNIL a pour l'instant créé deux référentiels : un pour les procédures d'audit de traitement et un pour les formations en matière de protection des données.

Depuis, elle a reçu vingt-cinq demandes de délivrance de labels.

La CNIL analyse ensuite la recevabilité de la demande dans les deux mois qui suivent son dépôt. Elle vérifie que la demande correspond bien au champ d'un référentiel et qu'elle est dûment complétée (champs remplis et annexes citées jointes au dossier).

Si le dossier a été déclaré recevable, le Comité de labellisation évalue la conformité du dossier puis le présente à la formation plénière de la Commission qui décidera, *in fine*, de délivrer - ou non - le label.

Une fois le label obtenu, l'organisme a la possibilité d'utiliser le logo « label CNIL » qui lui est attribué. L'utilisation de la marque « Label CNIL » est soumise au respect du règlement d'usage de la marque collective qui s'impose, de fait, aux labellisés.

La Commission a commencé à délivrer ses labels à partir de juin 2012 et délivre depuis, régulièrement, de nouveaux labels.

La Commission s'attachera à vérifier l'utilisation qui sera faite des labels et des logos. Elle peut ainsi vérifier par tout moyen que les produits ou procédures labellisés respectent les conditions définies par le référentiel. Parmi les mesures de contrôle prévues pour les labels qui ont été délivrés, figure notamment la transmission d'un bilan d'activité annuel, mais des vérifications sur place ne sont pas, non plus, à exclure pour les années à venir.

À noter que cette nouvelle activité est appelée à se développer fortement dans les années à venir, notamment avec l'arrivée de prochains référentiels. ■

INFOS +

Qu'est-ce que le Comité de labellisation ?

Le Comité de labellisation est composé de 3 membres de la Commission qui élisent en leur sein un président. Le Comité de labellisation a pour mission de proposer des orientations relatives à la politique de labellisation, d'élaborer de nouveaux projets de référentiels aux fins de labellisation de produits ou de procédures et d'évaluer la conformité des demandes de labels aux référentiels existants.

LE CORRESPONDANT : ACTEUR ESSENTIEL DE LA CONFORMITÉ DES ORGANISMES

2012 est une année de consolidation pour les correspondants « Informatique et Libertés » (CIL). La reconnaissance de leur métier a été étendue au secteur public et la CNIL a poursuivi ses actions d'accompagnement. Avec le futur règlement européen, la collaboration entre les CIL et les autorités de contrôle va entrer dans une nouvelle ère qu'il nous faut préparer dès à présent.

CONSOLIDER LE PRÉSENT

Chaque année, le correspondant s'affirme un peu plus comme un acteur essentiel de la mise en conformité des organismes avec la loi « Informatique et Libertés ». L'enjeu est en effet, désormais, d'assurer une mise en conformité dynamique des traitements de données à caractère personnel, dans un environnement technologique extrêmement évolutif.

Cette tendance est confirmée par le développement continu du réseau des CIL. **Le nombre d'organismes dotés d'un correspondant est ainsi passé de 4 152 en 2008 à 10 709 fin 2012.**

Elle résulte également de la reconnaissance du correspondant en tant que métier à part entière. Ce processus a été initié en 2011 avec l'insertion du CIL dans le répertoire opérationnel des métiers de Pôle Emploi (code Rome). Il a été poursuivi en 2012 par le centre national de la fonction publique territoriale (CNFPT) qui a intégré le CIL dans son référentiel des métiers. Cette démarche du CNFPT, soutenue par la CNIL, devrait encourager les collectivités et les établissements publics à désigner des correspondants, alors que le secteur privé représente actuellement 90 % des désignations. À cet égard, le CIL constitue pour eux un véritable atout qui leur permettra de mieux maîtriser les enjeux juridiques, techniques et économiques liés au développement de l'e-administration ou de l'Open data.

Au quotidien, la CNIL s'est mobilisée pour accompagner cette professionnalisation des CIL au travers notamment, des différents services qu'elle leur propose. Son engagement auprès des correspondants s'est traduit en 2012 par l'instruction de 2 068 demandes de conseils écrites, la réponse à 4 053 appels téléphoniques, l'organisation de 34 ateliers d'information impliquant l'accueil de 1 121 CIL dans ses locaux.

34

ATELIERS D'INFORMATION RÉUNISSANT 1 121 CIL ORGANISÉS À LA CNIL

L'action de la CNIL s'inscrit dans une tendance générale partagée par de nombreux pays et consacrée par le projet de Règlement européen, qui consiste à faire du correspondant la pierre angulaire de la future réglementation en matière de protection des données.

PRÉPARER L'AVENIR

Consacré par le projet de Règlement européen, le CIL devient un pilier de la conformité à la protection des données tant dans les organismes publics que privés.

Alors que la désignation d'un CIL est actuellement optionnelle et constitue encore un élément accessoire des actions de mise en conformité, le futur délégué à la protection des données sera au cœur du modèle proposé par le projet de Règlement européen.

En effet, obligatoire pour certains organismes, le futur délégué veillera à instaurer des procédures pour s'assurer de l'effectivité de la conformité à la protection des données personnelles de la structure qui l'aura désigné. Il aura notamment pour nouvelle mission de contrôler la documentation, la notification et la communication relatives aux violations de données (failles de sécurité). À cet effet, son niveau de compétences profession-

FOCUS

Une réflexion en cours sur le statut et les missions du CIL

Dans la perspective de l'évolution du métier envisagée dans le cadre du projet de Règlement européen, il est apparu nécessaire à la CNIL de consulter les CIL sur la perception qu'ils ont de leur statut et de leurs missions. Un questionnaire a ainsi été proposé sur l'extranet dédié aux CIL du 25 mai 2012 au 30 septembre 2012. Complété par 17 % des CIL en exercice (593 participants), il comportait des questions relatives au statut actuel du CIL et aux évolutions prévues dans le projet de Règlement européen. L'objectif de ces questions était principalement d'identifier les besoins et les attentes des CIL sur leur métier. Ils ont notamment été consultés sur la possibilité de recourir à un CIL interne ou externe, sur l'implication du CIL dans la mise en œuvre des traitements, son pouvoir d'alerte mais aussi sur l'effectivité des protections apportées au statut du CIL et la nécessité ou non de les faire évoluer.

Qu'il s'agisse du statut ou des moyens mis à disposition des CIL, il ressort de l'enquête une forte attente des CIL pour être accompagnés par la CNIL dans leurs missions.

À la lumière de ces résultats et des futures exigences du législateur européen, le service des correspondants mènera en 2013 des réflexions en collaboration directe avec les CIL et les têtes de réseaux d'associations professionnelles de CIL sur la nécessaire élaboration de méthodes et outils destinés à les accompagner vers ces nouvelles missions.

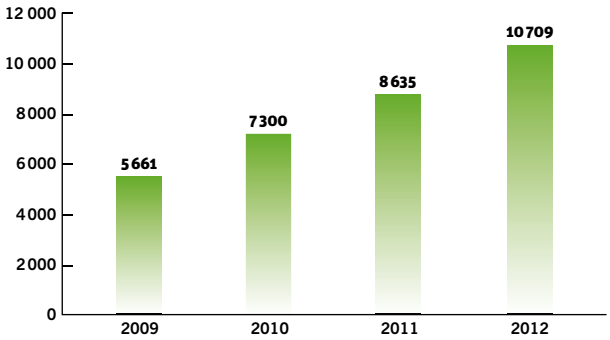
nelles devra être en accord avec la nature des traitements concernés (importance, sensibilité). En outre, le futur délégué à la protection des données aura l'obligation d'être régulièrement formé dans le cadre de ses fonctions.

Par ailleurs, le projet de Règlement européen vise à obliger le responsable de traitement ou le sous-traitant à prendre des mesures organisationnelles et à définir des procédures internes de nature à rendre effectives ses missions et obligations (personnels, locaux, équipements).

Au vu de ces évolutions tant sur leur statut que sur leurs missions, la CNIL proposera aux CIL les outils d'accompagnement dans la conduite du changement.

Ces orientations doivent être validées par le Parlement européen et le Conseil de l'Union européenne. De nombreuses modifications sont donc susceptibles d'être encore apportées au projet initial. ■

Nombre d'organismes ayant désigné un CIL



GROS PLAN

VIDÉOSURVEILLANCE/ VIDÉOPROTECTION :

LES BONNES PRATIQUES POUR DES SYSTÈMES PLUS RESPECTUEUX DE LA VIE PRIVÉE

« La CNIL souhaite accompagner les professionnels et les particuliers dans une démarche de conformité »

Dans la rue, dans les magasins, les transports en commun, les bureaux, les immeubles d'habitation, difficile d'échapper aux 935 000 caméras installées en France. Depuis mars 2011, la CNIL est compétente pour contrôler l'ensemble de ces dispositifs sur le territoire national.

EN 2012

173
CONTRÔLES RÉALISÉS

300
PLAINTES

QUEL CADRE LÉGAL ?

L'installation de ces outils est soumise au respect de plusieurs dispositions légales, selon qu'elles sont mises en place dans un lieu ouvert ou non au public.

Les dispositifs de vidéoprotection **installés sur la voie publique et dans les lieux ouverts au public** (rues, commerces) sont soumis aux dispositions du code de la sécurité intérieure. Depuis la loi du 14 mars 2011, dite LOPPSI 2, on ne parle en effet plus, dans ces cas, de vidéosurveillance, mais de vidéoprotection. Ces dispositifs doivent obtenir une autorisation préfectorale, après avis d'une commission départementale présidée par un magistrat.

Les dispositifs de vidéosurveillance **installés dans les lieux non ouverts au public** (zones réservées aux salariés) sont quant à eux soumis aux dispositions de la loi du 6 janvier 1978 modifiée, dite « Informatique et Libertés ».

À ce titre, ils font l'objet d'une déclaration à la CNIL.

QUEL CONTRÔLE ?

La CNIL contrôlait jusqu'alors les dispositifs de vidéosurveillance. Depuis la LOPPSI 2, la CNIL est également chargée de contrôler les dispositifs de vidéoprotection afin de s'assurer qu'ils sont conformes aux obligations légales. La CNIL peut procéder à ces contrôles de sa propre initiative ou à la demande de la commission départementale de vidéoprotection. Le responsable d'un dispositif de vidéoprotection peut aussi demander à la CNIL de vérifier la légalité des caméras qu'il a installées. Le contrôle mené par la CNIL consiste alors en une visite sur place.

En 2012, la CNIL a réalisé 173 contrôles portant sur les dispositifs de vidéoprotection. À cette occasion elle a constaté :

- Une nécessaire clarification du régime juridique,
- Une information des personnes insuffisante ou inexistante,
- Une mauvaise orientation des caméras,
- Des mesures de sécurité insuffisantes.

En 2012, la CNIL a reçu plus de 300 plaintes en la matière. 75 % de ces plaintes (soit 220 plaintes) concernaient la vidéosurveillance au travail.

INFOS +

La CNIL et l'AMF (Association des Maires de France) ont élaboré conjointement des bonnes pratiques à destination des maires qui souhaitent installer des systèmes de vidéoprotection dans le respect des libertés individuelles. Ces 10 conseils sont disponibles sur les sites de l'AMF et de la CNIL depuis juin 2012. Cette initiative commune s'inscrit dans le cadre de la convention de partenariat signée le 15 juin 2011.

QUELLES BONNES PRATIQUES POUR CONCILIER SÉCURITÉ COLLECTIVE ET RESPECT DE LA VIE PRIVÉE ?

La CNIL souhaite accompagner les professionnels et les particuliers. C'est pourquoi elle a mis à leur disposition des fiches pratiques leur expliquant concrètement comment installer des dispositifs dans le respect de la loi et du droit des personnes filmées. 6 fiches pratiques ont été ainsi mises en ligne sur le site de la CNIL en juin 2012 :

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

Ces fiches ont été téléchargées 30 000 fois en 9 mois. ■

CNIL. Commission Nationale de l'Informatique et des Libertés — AMF Association des Maires de France

Vidéoprotection des lieux publics

10 POINTS POUR ASSURER LA SÉCURITÉ COLLECTIVE DANS LE RESPECT DES LIBERTÉS INDIVIDUELLES

n° 1 : définir l'objectif recherché
n° 2 : délimiter les zones placées sous vidéoprotection
n° 3 : désigner un point de contact
n° 4 : informer le public
n° 5 : garantir le droit d'accès
n° 6 : accueillir les demandes de renseignement et rectifier toute erreur signalée
n° 7 : limiter la conservation des données
n° 8 : identifier les destinataires des images
n° 9 : sécuriser l'accès au système
n° 10 : évaluer et contrôler le système

POUR MIEUX GÉRER LES RISQUES SUR LA VIE PRIVÉE : SUIVEZ LE GUIDE

La CNIL a publié en juillet 2012 une méthode et un catalogue de mesures pour aider les organismes à gérer les risques sur la vie privée. Ces outils opérationnels doivent faciliter l'intégration de la protection de la vie privée, notamment dans les traitements complexes ou à risques grâce à une approche pragmatique, rationnelle et systématique.

PRÉSERVER LA SÉCURITÉ DES DONNÉES : UNE OBLIGATION LÉGALE

La loi « Informatique et Libertés » prévoit, dans son article 34, que les responsables de traitement doivent « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».

En d'autres termes, chaque responsable doit identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire. Pour ce faire, il convient d'adopter une vision globale et d'étudier les conséquences sur les personnes concernées.

DEUX GUIDES POUR DÉTERMINER LA SÉCURITÉ ADÉQUATE

Après le guide sécurité destiné aux PME qui a été publié en 2010, les deux nouveaux guides de la CNIL ont pour objectif d'aider à la mise en place d'une démarche d'analyse complète pour les traitements complexes. Ils s'adressent ainsi aux responsables de traitements, maîtrises d'ouvrage, maîtrises d'œuvre, correspondants « Informatique et Libertés » et responsables de la sécurité des systèmes d'information. Ils les aident à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité, organisationnelles et techniques, nécessaires et suffisantes.

Le but est en effet de disposer d'une cartographie des risques, estimés en termes de gravité et de vraisemblance, afin de décider de les accepter ou de les traiter à l'aide de mesures qui les éviteraient, les réduiraient, ou les transféreraient, jusqu'à ce qu'ils soient acceptables.

Ces guides se composent :

- d'une **méthode de gestion des risques sur les libertés et la vie privée**, expliquant comment utiliser la méthode EBIOS dans le contexte spécifique de la protection des données à caractère personnel ;
- d'un **catalogue de bonnes pratiques**, permettant au responsable de choisir des mesures pour traiter les risques identifiés avec la méthode, de manière proportionnée à ces risques, et adaptée en fonction du contexte du traitement.

Des études de cas ont été publiées par le Club EBIOS :

- une sur la gestion des patients d'un cabinet de médecine du travail ;
- une autre sur la géolocalisation de véhicules d'entreprise.

Pour répondre au besoin des sociétés internationales et des organismes étrangers, la CNIL propose également une version anglaise de ces deux guides.

Ces guides ont déjà été téléchargés 8 000 fois sur **www.cnil.fr** ■

BIENTÔT UN « PACK DE CONFORMITÉ » DÉDIÉ AU LOGEMENT SOCIAL

Au cours de l'année 2012, la CNIL a procédé à des contrôles dans le secteur du logement social qui ont notamment abouti à une mise en demeure publique à l'encontre d'un bailleur. À la suite de cette mise en demeure, la CNIL a souhaité engager une réflexion pour comprendre et résoudre les difficultés rencontrées par les bailleurs dans l'élaboration et la gestion de leurs systèmes d'information.

Dans cette optique, la Commission a initié une concertation avec plusieurs acteurs du logement social, en vue de prendre connaissance de leurs pratiques, de leurs besoins et d'identifier les difficultés qu'ils rencontrent au quotidien dans la gestion et la tenue de leurs fichiers.

La CNIL a ainsi invité l'Union sociale pour l'habitat (USH) à lui transmettre des remontées de terrain, avant d'organiser des réunions de travail avec des bailleurs sociaux, accompagnés de représentants de l'USH, ainsi que des associations représentant les intérêts des locataires.

Cette concertation doit permettre à la Commission d'établir prochainement un nouveau type d'outil, appelé « pack de conformité ». Celui-ci permettra aux acteurs du logement social de mettre en œuvre plus aisément les obligations issues de la loi « Informatique et Libertés », tant dans leurs relations avec les locataires (demande d'attribution, vie dans le logement, sortie du logement), qu'avec les accédants à la propriété.

Le pack de conformité dédié au logement social, actuellement en cours d'élaboration, pourrait comprendre des outils de simplification des formalités préalables à accomplir auprès de la CNIL :

- une norme simplifiée mise à jour permettant de déclarer aisément les traitements visant à l'enregistrement et l'instruction des demandes de logement social en locatif ou en accession à la propriété, ainsi qu'à la gestion du patrimoine immobilier à caractère social ;
- une nouvelle autorisation unique concernant les traitements mis en œuvre pour élaborer ou suivre un accompagnement social personnalisé, d'une part, ou gérer des précontentieux et contentieux, d'autre part ;
- des fiches pratiques pour aider les bailleurs à mettre concrètement en application les principes « Informatique et Libertés », sur le modèle des fiches déjà proposées sur la vidéosurveillance et les données personnelles et le travail. ■

FOCUS

Les nouveaux outils de la conformité

Les récentes et rapides évolutions de l'environnement numérique auquel la CNIL est confrontée l'ont amenée à repenser son action et ses outils d'intervention. Elle souhaite désormais associer et responsabiliser les acteurs des différents secteurs qu'elle a vocation à réguler. Ce partage ne peut se faire qu'en mettant à leur disposition des outils permettant de mettre en œuvre concrètement, et le plus en amont possible, les principes « Informatique et Libertés ». Qu'il s'agisse de codes de bonne conduite ou bonnes pratiques, de chartes, de labels, de packs de conformité, de réseaux de correspondants « Informatique et Libertés », ces leviers ont vocation à être au service de la conformité des organismes, en étant ancrés dans la réalité et les spécificités du secteur, efficaces et pérennes dans le temps.

4. PROTÉGER LES CITOYENS

Les plaintes

Le droit d'accès indirect :
des demandes en forte progression

LES PLAINTES

HISTOIRES VÉCUES

Usurpation d'identité

Madame A constate que des commandes ont été passées sur son compte en ligne d'un site de commerce électronique par un tiers qui a usurpé son identité. Mme A signale cette fraude à la société de commerce en ligne et lui en apporte la preuve. La société ne procède pas aux modifications requises. L'historique des commandes frauduleuses faites au nom de Mme A demeure donc dans son dossier. Cette conservation a pour conséquence un fichage par la société Fia-net et le refus par un opérateur de téléphonie d'honorer la commande passée par Mme A qui adresse une plainte à la CNIL. La CNIL demande à la société de commerce en ligne de prendre en considération le droit de rectification et de suppression de Mme A dans les plus brefs délais (article 40 de la loi). À la suite de l'intervention de la CNIL, la société procède enfin aux modifications.

Faux compte Facebook

Un professeur constate que d'anciens élèves lui ont créé à ses nom et prénom deux faux comptes Facebook. Ces profils portent atteinte à sa réputation, suggérant que ce professeur a un penchant pédophile. Ce professeur sollicite la CNIL afin de connaître les démarches à effectuer. La CNIL l'invite à utiliser les procédures disponibles sur le site de Facebook, permettant de signaler les faux comptes et d'en demander la suppression. La CNIL le guide dans ses démarches et lui explique comment accéder à cette procédure à partir de la rubrique « Aide » du site. À la suite de ces signalements, les deux profils concernés ont été supprimés.

Surveillance permanente des salariés

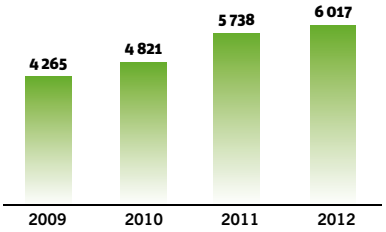
Des agents de sécurité d'un immeuble parisien saisissent la CNIL pour dénoncer la présence d'une caméra qui les filme en continu (PC sécurité). Le syndicat de copropriétaires utilisait la caméra pour surveiller l'activité et la présence des salariés en se prévalant d'une finalité liée à la protection des biens et des personnes de l'immeuble. Le syndicat de copropriétaires est mis en demeure de retirer le dispositif et de recourir à des moyens de surveillance de l'activité des salariés moins intrusifs. À l'issue d'un contrôle sur place et face au refus persistant du syndicat de retirer ou réorienter le dispositif, la formation restreinte de la CNIL a prononcé une sanction publique d'un euro assortie d'une injonction de mettre un terme au caractère continu du dispositif.

PLUS DE 6 000 PLAINTES EN 2012 : UN NOMBRE RECORD

Le nombre de plaintes reçues pour non-respect de la loi « Informatique et Libertés » continue d'augmenter : le seuil des 6 000 plaintes a été dépassé en 2012.

Comme en 2011, il convient d'y ajouter les milliers de demandes écrites de particuliers traitées par la CNIL et les nombreuses questions traitées par téléphone.

Comparatif du nombre de plaintes reçues par la CNIL entre 2009 et 2012



Le service de « plainte en ligne » accessible depuis le site de la CNIL a été utilisé par 44 % des usagers qui saisissent la CNIL contre 26 % en 2011. En 2013, il est prévu d'élargir le recours à ce dispositif pour les secteurs de la banque et du travail.

Les plaintes du secteur Internet/Télécom représentent 31 % des demandes adressées à la CNIL (suppression de photographies, de vidéos, de commentaires, de coordonnées, réseaux sociaux, référencements par les moteurs de recherche, faux profils, inscription dans le fichier Préventel…). **1 050 plaintes sont relatives au droit à l'oubli.**

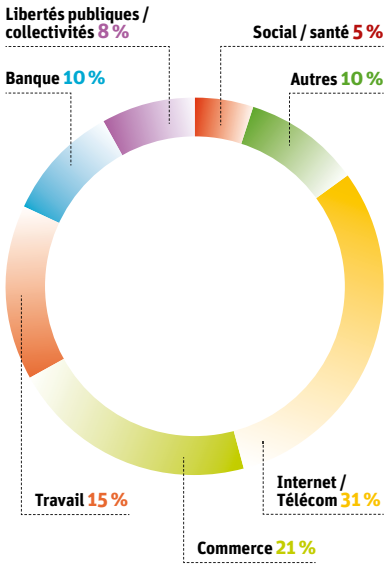
Le secteur du commerce représente 21 % des plaintes reçues (radiation de fichiers publicitaires, conservation des coordonnées bancaires, gestion des fichiers clients, défaut de confidentialité des données…)

Un nombre important de plaintes concerne le secteur du travail (15 % : vidéosurveillance, géolocalisation, accès au fichier professionnel) et le secteur bancaire (10 % : inscription au FICP, FCC…).

Une augmentation significative des plaintes portant sur les libertés publiques et les collectivités locales (8 %) est également à noter (élections législatives et présidentielles de 2012, presse en ligne, diffusion de documents publics par les collectivités locales sur Internet…).

Comme en 2010 et en 2011, l'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de saisine de la CNIL (46 % des plaintes reçues). ■

Répartition des plaintes par secteur



LE DROIT D'ACCÈS INDIRECT : DES DEMANDES EN FORTE PROGRESSION

En application des articles 41 et 42 de la loi du 6 janvier 1978 modifiée, les personnes qui souhaitent vérifier les données les concernant susceptibles d'être enregistrées dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique ou , le cas échéant, qui ont pour mission de prévenir, rechercher ou constater des infractions ou d'assurer le recouvrement des impositions (STIC, JUDEX, fichiers de renseignement...) peuvent en effectuer la demande par écrit auprès de la CNIL.

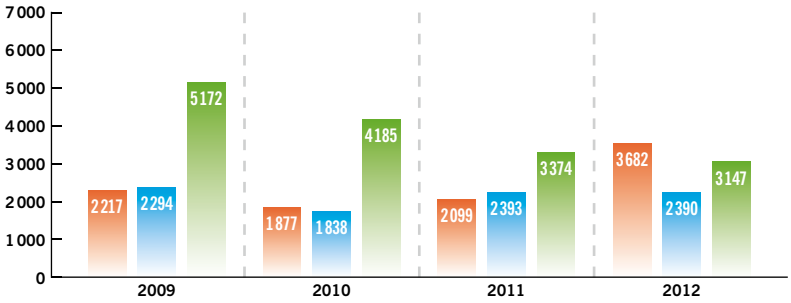
L'année 2012 a été marquée par une forte progression du nombre de demandes de droit d'accès indirect, puisque la CNIL a reçu 3 682 demandes, soit une augmentation de 75 % par rapport à 2011. Cette augmentation résulte principalement de l'importance des demandes (1 829 demandes) portant sur le fichier des comptes bancaires et assimilés (FICOBA) de l'administration fiscale, principalement dans le cadre du règlement des successions. Cela fait suite à la reconnaissance par le Conseil d'État en 2011, d'un droit d'accès des héritiers à ce fichier.

Les demandes de droit d'accès indirect portant sur les autres fichiers relevant de ce régime particulier sont d'un niveau équivalent, voire progressent sensiblement par rapport à l'année précédente. C'est le cas pour les fichiers STIC et JUDEX (+ 4 %), dont la vérification constitue toujours une préoccupation majeure pour les personnes qui, du fait de leur enregistrement en tant qu'auteur d'une ou plusieurs infractions, sont régulièrement confrontées à des refus de délivrance des agréments ou autorisations nécessaires à l'obtention ou la conservation d'un emploi dans certains secteurs d'activités. Ces fichiers sont appelés à être remplacés à la fin de l'année 2013 par le Traitement des Antécédents Judiciaires (TAJ), fichier commun aux forces de police et de gendarmerie nationales (voir chapitre 2).

▸▸▸

3682
DEMANDES DE DROIT D'ACCÈS INDIRECT
SOIT + 75 % PAR RAPPORT À 2011

Évolution des demandes de droit d'accès indirect 2009-2012

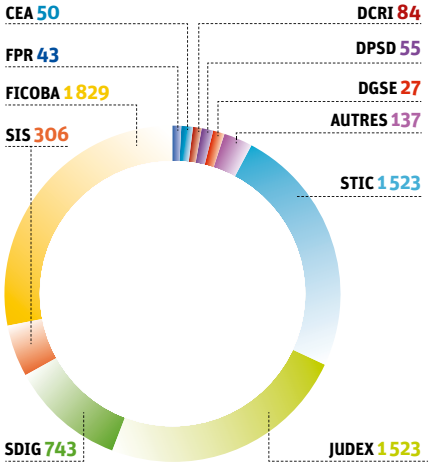


INFOS +

Comment ça marche ?

Une fois la demande accompagnée d'une copie d'un titre d'identité reçue, 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 et faire procéder, le cas échéant, aux modifications nécessaires. Les données peuvent ensuite être portées à la connaissance de la personne concernée si, en accord avec l'administration gestionnaire, cette communication n'est pas de nature à nuire à la finalité du fichier, la sûreté de l'État, la défense ou la sécurité publique.

Demandes de droit d'accès indirect 2012 : répartition par fichiers des vérifications à effectuer



FICOBA : Fichier des Comptes Bancaires et Assimilés / STIC : Système de Traitement des Infractions Constatées / JUDEX : Système Judiciaire de Documentation et d'Exploitation / SIS : Système d'Information Schengen FPR : Fichier des Personnes Recherchées / CEA : Direction Centrale de la Sécurité du Commissariat à l'Énergie Atomique / DCRI : Direction Centrale du Renseignement Intérieur / DGSE : Direction Générale de la Sécurité Extérieure / DPSD : Direction de la Protection de la Sécurité de la Défense / Autres : Fichier des Courses et Jeux (FICOJ), Fichier des Interdits de Stades (FNIS), Système de gestion informatisée des détenus en établissement pénitentiaire (GIDE), Europol…

INFOS +

Le fichier FICOBA

Les données du fichier FICOBA sont issues des déclarations auxquelles sont soumis les établissements bancaires en application de l'article 1649 A du code général des impôts.
Si ce fichier permet un recensement des comptes bancaires détenus par une personne (établissement bancaire concerné, date d'ouverture, de modification ou de clôture du compte), il ne comporte en revanche aucune donnée relative à l'historique des opérations bancaires effectuées ou au solde de ces comptes.

Chaque demande de droit d'accès indirect implique des vérifications dans plusieurs fichiers afin de répondre à l'ensemble des attentes de la personne concernée. Ainsi, les 3 682 demandes reçues au cours de l'année 2012 représentent 6 320 vérifications à mener portant sur les principaux fichiers suivants par ordre croissant : le fichier FICOBA, le Système de Traitement des Infractions Constatées (STIC), le Système Judiciaire de Documentation et d'Exploitation (JUDEX), les fichiers des services de l'Information Générale du ministère de l'Intérieur (Enquêtes Administratives liées à la Sécurité Publique -EASP-, Prévention des Atteintes à la sécurité publique – PASP), le Système d'Information Schengen (SIS).

Les membres de la CNIL ont mené 3 147 vérifications au cours de l'année 2012, ce qui a permis de clôturer la procédure pour 2 393 demandes de droit d'accès indirect, engagées pour la plupart au cours des années précédentes, compte tenu des délais inhérents à la vérification des fichiers d'antécédents judiciaires (STIC-JUDEX). En effet, afin qu'un magistrat de la CNIL puisse procéder à la vérification du bien fondé de l'enregistrement et de l'exactitude des données dans ces fichiers, les services gestionnaires doivent procéder à la centralisation préalable de pièces et éléments nécessaires (*copie des procédures établies, réponses des procureurs de la République territorialement compétents sur les suites judiciaires intervenues*).

LE DROIT D'ACCÈS INDIRECT AU FICHIER FICOBA

Par une décision du 29 juin 2011, le Conseil d'État a consacré l'existence d'un droit d'accès des héritiers aux données d'identification des comptes bancaires recensés dans ce fichier, en leur qualité « *d'ayant droit du solde des comptes détenus* » par la personne décédée. L'héritier se voit ainsi reconnaître, pour l'accès à ce fichier, le statut de « personne concernée » au sens de la loi du 6 janvier 1978 modifiée. L'inventaire des comptes bancaires détenus par le défunt est, en effet, pour tout héritier, indissociable de la transmission patrimoniale et essentielle pour lui permettre de procéder au règlement de la succession.

Depuis, la CNIL reçoit un nombre très important de demandes de la part d'héritiers ou de leur mandataire (notaire, avocat…). Pour le traitement de telles demandes, la communication de la seule copie de la pièce d'identité du demandeur n'est pas suffisante. La transmission à l'appui de toute demande, d'une copie de l'acte de décès, d'un document attestant de l'identité et de la qualité d'héritier (*extrait du livret de famille, acte de notoriété, certificat d'hérédité…*) sont indispensables, voire le mandat confié en cas d'intervention d'un notaire ou avocat car ce droit est uniquement rattaché à la personne de l'héritier.

Conformément aux dispositions de l'article 42 de la loi du 6 janvier 1978, le droit d'accès indirect à ce fichier n'ouvre pas droit à communication systématique des données qui y sont enregistrées. L'administration fiscale peut, en effet, s'y opposer pour des motifs liés à la lutte contre la fraude fiscale ou au recouvrement des impositions.

Si les modalités du droit d'accès indirect à ce fichier sont désormais arrêtées, le nombre important de demandes, allié à la nécessité pour l'administration fiscale de procéder à des recherches internes avant de se prononcer sur le caractère communicable des données, impose souvent des délais de traitement de l'ordre de plusieurs mois.

Principaux résultats des vérifications des fichiers STIC et JUDEX effectuées en 2012
(54 % des vérifications ont porté, en 2012, sur Les fichiers STIC et JUDEX)

	STIC	JUDEX
Nombre de vérifications individuelles effectuées	1227	946
Nombre de personnes inconnues	305	648
Nombre de personnes enregistrées uniquement en tant que victimes	276	71
Nombre de fiches de personnes « mises en cause » vérifiées	646	227
dont nombre de fiches supprimées	18 %	38 %
dont nombre de fiches mises à jour par mention de la décision judiciaire favorable intervenue (*classement sans suite, non-lieu, relaxe…*) rendant la personne inconnue du fichier sous profil de consultation administrative (*enquêtes administratives*)	18 %	30 %
dont nombre de fiches rectifiées ayant eu pour effet de réduire le délai global de conservation de l'enregistrement	2 %	32 %
dont nombre de fiches examinées avec maintien de l'enregistrement de la personne (*fiches exactes, rectifications mineures sans incidence sur la durée de conservation, défaut de réponse des parquets sur les suites judiciaires intervenues*)	62 %	58 %

Chaque fiche individuelle peut comporter une ou plusieurs procédures d'infraction

LES EFFETS DE LA LOPPSI II SUR LES CLASSEMENTS SANS SUITE

L'année 2012 permet de mesurer les effets du nouvel article 230-8 du code de procédure pénale, issu de la loi n°2011-267 du 14 mars 2011 (*dite Loppsi II*). Cet article prévoit que tous les faits ayant bénéficié d'une décision de classement sans suite, quel qu'en soit le motif (*rappel à la loi, dédommagement de la victime, préjudice peu important…*), doivent faire l'objet d'une mise à jour, par mention de cette décision, dans les fichiers d'antécédents judiciaires. Cette mention a pour effet de rendre l'affaire concernée inaccessible lors de la consultation de ces fichiers pour les enquêtes administratives qui sont notamment menées pour l'accès à certains types d'emplois (agents de sécurité privée, personnel navigant et personnes exerçant en zone aéroportuaire, agents de sûreté ferroviaire, agents de police municipale…).

Au terme des vérifications réalisées par la CNIL en 2012, près de 20 % des personnes sont ainsi devenues « *inconnues* » de ces fichiers sous le profil de consultation administrative : si les faits demeurent enregistrés dans ces fichiers à des fins de police judiciaire jusqu'à l'expiration du délai de conservation applicable (de 5 à 40 ans en fonction de la nature des faits), ils n'ont plus vocation à être consultés et donc opposés comme motif de refus des agréments ou habilitations nécessaires pour l'accès à l'emploi dans les secteurs d'activités soumis à enquêtes administratives (environ 1,3 million d'emplois concernés). ■

FOCUS

Suites judiciaires permettant l'effacement ou la mise à jour par mention dans les fichiers d'antécédents judiciaires

(article 230-8 du code de procédure pénale)

- **Jugement de relaxe ou d'acquittement : effacement sauf opposition du Procureur de la République auquel cas une mention de cette décision est alors apportée dans le fichier qui rend l'affaire inaccessible lors de sa consultation à des fins d'enquêtes administratives.**
- **Ordonnance de non-lieu – décision de classement sans suite pour « absence d'infraction » ou « infraction insuffisamment caractérisée » : mise à jour par mention de la décision ainsi intervenue sauf si le procureur de la République donne explicitement son accord concernant l'effacement des faits.**
- **Décision de classement sans suite pour tout autre motif que ceux précités (rappel à la loi, avertissement, injonction thérapeutique, dédommagement de la victime, etc.) : mise à jour du fichier par mention de cette décision.**

Ça la fiche mal !

Ajout d'une mention dans les fichiers au regard de la suite judiciaire intervenue

▸ Monsieur L, 39 ans, travaillant dans le domaine de la sécurité depuis 2004 sans avoir jamais eu la moindre difficulté, a souhaité exercer son droit d'accès indirect, craignant que les difficultés rencontrées dans le cadre de son divorce puissent lui être professionnellement préjudiciables. Le procureur de la République s'est opposé à l'effacement des faits (« *appels téléphoniques malveillants* » et « *menaces* ») dans la mesure où les suites judiciaires intervenues n'y ouvraient pas droit (classements sans suite pour « rappel à la loi » et « médiation pénale »). Les vérifications menées par la CNIL ont néanmoins permis de s'assurer de l'ajout d'une mention dans le fichier STIC pour ces deux affaires. Cette mention a pour effet de rendre l'affaire concernée inaccessible lors des enquêtes administratives

Absence de transmission par les parquets des suites judiciaires favorables intervenues

▸ Madame D., maire d'une commune, a saisi la CNIL au titre du droit d'accès indirect après s'être vu refuser l'accès en zone aéroportuaire pour assister à une réunion de travail dans le cadre de l'exercice de ses fonctions. À la suite des démarches de la Commission, les informations enregistrées la concernant dans le fichier STIC (« *atteinte à la liberté d'accès ou à l'égalité des candidats dans les marchés publics, usage de faux en écriture* »), ont été effacées. Le jugement de relaxe dont elle avait bénéficié en 2006 n'avait pas été porté, en son temps, à la connaissance des services gestionnaires de ce fichier par l'autorité judiciaire.

▸ Monsieur G, 30 ans, s'est vu opposer par le Préfet de son département, un refus de délivrance de sa carte professionnelle en raison d'une plainte déposée par le père de son beau-fils pour « *violences volontaires sur personne de moins de 15 ans par personne ayant autorité* ». Ces faits avaient été classés sans suite pour insuffisance de charges mais demeuraient enregistrés dans le fichier STIC car cette décision judiciaire favorable, avec accord d'effacement du procureur de la République concerné, n'avait pas été portée à la connaissance des services gestionnaires de ce fichier. La procédure de droit d'accès indirect qu'il a engagé a permis d'en assurer l'effacement.

▸ Monsieur F, 35 ans, ingénieur dans le génie civil industriel et nucléaire, est appelé à procéder à des visites et inspections de centrales nucléaires pour sa société. Il a saisi la CNIL d'une demande de droit d'accès indirect craignant que son enregistrement dans le fichier STIC pour une affaire classée sans suite (« *violences volontaires par conjoint* ») fasse obstacle à l'obtention des habilitations nécessaires d'autant que, par le passé, il s'est vu opposé un ajournement de sa demande de naturalisation pour ces mêmes faits. Au terme des vérifications, l'affaire a fait l'objet d'une suppression compte tenu de la décision de classement sans suite pour insuffisance de charges intervenue et de l'accord, en ce sens, du procureur de la République.

Mauvais enregistrement initial des faits

▸ Monsieur C. 29 ans, travaillant dans le domaine de la maintenance aéronautique s'est vu refuser son badge pour l'accès en zone aéroportuaire en raison de son inscription au fichier STIC. Dans le cadre des vérifications, il a été confirmé que l'intéressé était enregistré pour des faits de « *dégradations volontaires de véhicule* ». Toutefois, l'examen de la procédure établie pour ces faits a mis en évidence, comme il l'avait d'ailleurs indiqué, qu'il n'était pas mis en cause. L'affaire concernée a donc été supprimée par le service gestionnaire.

Requalification des faits

▸ Monsieur D., 35 ans, agent SNCF, s'est vu refuser sa mutation interne au sein du service de la surveillance générale de la SNCF en raison de son inscription au fichier STIC pour des faits de « *dégradations de biens privés* ». Les vérifications menées par la CNIL et la requalification en « *dégradations légères* » par le parquet ont conduit à la réduction du délai de conservation de 20 à 5 ans et à la suppression immédiate de cette affaire du fait de l'expiration de ce délai.

5.
CONTRÔLER ET SANCTIONNER

La notification des violations de données à caractère personnel, une nouvelle mission

Les contrôles

Les sanctions

LA NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL, UNE NOUVELLE MISSION

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

15
NOTIFICATIONS REÇUES

LE PRINCIPE : UNE OBLIGATION DE NOTIFICATION

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

Dès qu'il constate une violation de données, **le responsable de traitement doit sans délai en informer la CNIL**. Il doit également informer les personnes dont les données ont fait l'objet de la violation, sauf s'il a mis en œuvre en amont des mesures techniques qui rendent les données incompréhensibles à toute personne

INFOS +

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

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

non autorisée à y avoir accès. La CNIL peut cependant, si elle estime que la gravité de la violation le justifie, mettre en demeure le fournisseur d'informer les intéressés.

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

FOCUS

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

L'ACTION DE LA CNIL

En 2012, la CNIL a reçu une quinzaine de notifications de violation de données personnelles. Ce faible nombre de notifications s'explique par le fait que les modalités de mise en œuvre de cette nouvelle obligation n'ont été que récemment fixées. En effet, au niveau national, un décret d'application a été publié en mars 2012. Le règlement européen visant à harmoniser les procédures de notification des violations aux autorités de protection des données personnelles a quant à lui été adopté en janvier 2013.

Ce règlement prend largement en compte l'avis rendu par le G29 et auquel la CNIL a contribué. Il définit notamment le contenu et les délais de notification aux autorités de protection des données et impose à ces dernières de mettre à disposition des déclarants un moyen électronique sécurisé de notification.

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

De manière plus générale, ces nouvelles obligations s'inscrivent dans un processus de responsabilisation accrue des acteurs en charge des données personnelles. Il ne s'agit plus d'attendre que les victimes déposent plainte ou que la CNIL contrôle et sanctionne. Le responsable du traitement doit assumer pleinement la responsabilité des erreurs commises en amont, afin d'éviter toute conséquence pour les personnes concernées. Cette obligation permettra donc à la CNIL d'avoir une meilleure vision du niveau de sécurité mis en œuvre, mais également d'offrir un meilleur accompagnement. ■

> Ces nouvelles obligations s'inscrivent dans un processus de responsabilisation accrue des acteurs

LES CONTRÔLES

L'année 2012 a confirmé la tendance amorcée depuis plusieurs années, qui consiste à faire des contrôles sur place un moyen d'action privilégié de la Commission. Ainsi, le nombre de contrôles réalisés a encore notablement augmenté, qu'ils portent sur les fichiers soumis à la loi « Informatique et Libertés » ou sur les dispositifs de vidéoprotection relevant de la loi du 21 janvier 1995.

458

CONTRÔLES EN 2012

DONT 285
PORTANT SUR DES DISPOSITIFS RELEVANT DE LA LOI « INFORMATIQUE ET LIBERTÉS »

ET 173
PORTANT SUR DES DISPOSITIFS DE VIDÉOPROTECTION/ VIDÉOSURVEILLANCE

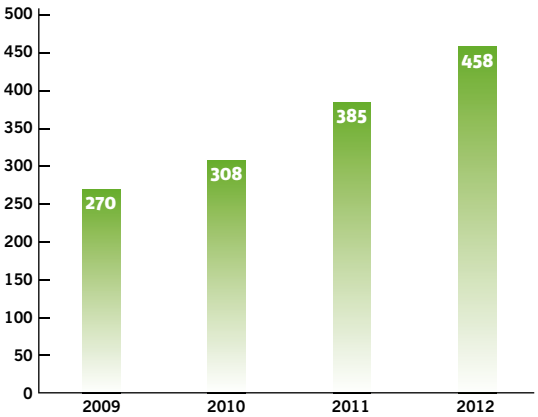
UNE AUGMENTATION DE 19 % PAR RAPPORT À 2011

La CNIL a effectué **458 contrôles au cours de l'année 2012, ce qui représente une augmentation de 19 % par rapport à l'année précédente**. Cette augmentation illustre une nouvelle fois la volonté de la Commission de vérifier, par ses contrôles sur place, le respect des textes dont elle est chargée d'assurer l'application.

L'activité de contrôle de la CNIL se répartit comme suit : 285 contrôles portant sur des dispositifs relevant de la loi « Informatique et Libertés » et 173 contrôles portant sur des dispositifs de vidéoprotection/vidéosurveillance.

Dans le premier cas, 23 % des contrôles ont été effectués dans le cadre de l'instruction de plaintes, 11 % dans le cadre de la procédure de sanction (par exemple, afin de vérifier le respect des engagements pris par un responsable de traitement mis en demeure par la Présidente de la CNIL) et 26 % au regard de l'actualité.

Évolution du nombre de contrôles depuis 2009



40 % des contrôles réalisés se sont inscrits dans les thématiques issues du programme annuel décidé par la Commission.

Ces contrôles ont donné lieu à l'adoption d'une vingtaine de mises en demeure par la Présidente de la CNIL et 4 avertissements par la formation restreinte. Pour autant, on doit constater que les courriers adressés à la suite de ces contrôles ont conduit, dans la quasi-totalité des cas, à ce que les organismes adoptent une démarche de mise en conformité vis-à-vis de la loi du 6 janvier 1978 modifiée, y compris parfois en désignant des correspondants à la protection des données.

Ce programme annuel était structuré autour des thèmes suivants :

- **« La sécurité des données de santé »** : une vingtaine de contrôles ont été réalisés dans ce cadre ; ils ont porté sur les conditions de traitement des données par des organismes aussi divers que les hébergeurs agréés, les centres d'étude et de conservation des œufs et du sperme humains (CECOS), les pharmacies (dossier pharmaceutique), un groupe hospitalier d'importance nationale, des laboratoires d'analyse médicale et des prestataires développant des logiciels ou produits destinés à traiter des données de santé.
- **« Les failles de sécurité »** : de nombreux contrôles ont porté sur les conditions de sécurité de traitement des données à caractère personnel. Ces contrôles ont pu être réalisés dans le cadre d'alertes adressées à la CNIL ou dans le cadre de notification de violations de données à caractère personnel (article 34 bis de la loi voir pages 52-53).
- **« Sport et vie privée »** : une vingtaine de contrôles ont également été menés auprès

d'acteurs de toute taille du secteur sportif, qui traitent pour certains d'entre eux des dizaines de milliers de données concernant leurs adhérents. Des contrôles ont ainsi été réalisés auprès de fédérations sportives ou auprès de clubs de sport. L'objet de ces contrôles visait essentiellement à apprécier la proportionnalité des données collectées, l'information des personnes et les mesures de sécurité mises en place.

▸ **« Les données à caractère personnel et la vie quotidienne »** : des contrôles de grande ampleur ont été effectués auprès des principaux fournisseurs de gaz, d'électricité ou de services de communications électroniques. Ces contrôles ont notamment porté sur l'analyse des zones dites « commentaires » afin de s'assurer que les données collectées sur les clients de ces opérateurs étaient conformes à la loi. Enfin, une série de contrôles a été opérée auprès de sociétés d'autoroute afin, notamment, d'apprécier la conformité de certains de leurs dispositifs innovants (lecture de plaque d'immatriculation, péage sans contact, etc.).

▸ **« La délivrance des visas »** : la Commission a également procédé à des contrôles afin de vérifier les conditions de recueil et de traitement des données biométriques des demandeurs de visas. Ces contrôles ont été effectués auprès des services centraux situés en France mais également auprès de consulats français situés à l'étranger et auprès de certains des prestataires privés auxquels il est fait appel dans ce cadre.

> Dans la quasi-totalité des cas, les organismes se mettent en conformité après un contrôle

LE CONTRÔLE DES DISPOSITIFS DE VIDÉOPROTECTION/ VIDÉOSURVEILLANCE

Les dispositifs dits « de vidéoprotection », qui filment la voie publique et les lieux ouverts au public sont soumis aux dispositions du code de la sécurité intérieure. Les dispositifs dits de « vidéosurveillance » qui concernent des lieux non ouverts au public (locaux professionnels non ouverts au public comme les bureaux ou les réserves des magasins) sont soumis aux dispositions de la loi « Informatique et Libertés ».

Dans les faits, on constate qu'il est rare de trouver un dispositif relevant d'une seule législation : les dispositifs comprennent généralement une partie des caméras filmant des zones ouvertes au public (les espaces de vente par exemple) et une partie filmant des zones non ouvertes au public.

C'est dans le cadre de sa mission de contrôle de l'ensemble de ces dispositifs que la CNIL a effectué 173 contrôles au cours de l'année 2012. Ce chiffre représente une augmentation de 14,5 % par rapport à l'année précédente et témoigne de la volonté de la CNIL de se saisir pleinement des pouvoirs qui lui ont été confiés par le législateur en 2011. On doit également relever que les contrôles ont porté sur des structures du secteur public et privé, de toute taille. Ces contrôles ont permis à la CNIL d'alimenter sa réflexion sur les conditions de mise en œuvre des systèmes de vidéoprotection/ vidéosurveillance.

De manière générale, ces contrôles ont conduit la CNIL à adopter 12 mises en demeure, une sanction pécuniaire et un avertissement. ■

FOCUS

Le contrôle STIC

En 2009, la CNIL a formulé 11 propositions d'amélioration du fichier STIC. En 2012, plus d'une vingtaine de contrôles ont été effectués afin de vérifier si des améliorations ont été apportées au fonctionnement de ce fichier. Les investigations ont été menées auprès de l'ensemble des acteurs chargés de garantir le bon fonctionnement et la bonne utilisation du fichier : services de police, tribunaux et préfectures notamment. Le bilan de ces constats fera l'objet d'une communication globale au premier semestre 2013.

- **23 contrôles sur place dans 9 départements ;**
- **61 contrôles sur pièces (concernant 27 préfectures et 34 tribunaux de grande instance) ;**
- **200 interlocuteurs entendus ;**
- **300 pièces papiers et numériques copiées.**

LES SANCTIONS

En 2012, la Présidente de la CNIL a adopté 43 mises en demeure dont 2 ont été rendues publiques. 13 sanctions ont été prononcées par la formation restreinte dont 4 sanctions pécuniaires, 9 avertissements et 1 injonction de cesser le traitement (certaines de ces sanctions pouvant se cumuler).

43
MISES EN DEMEURE

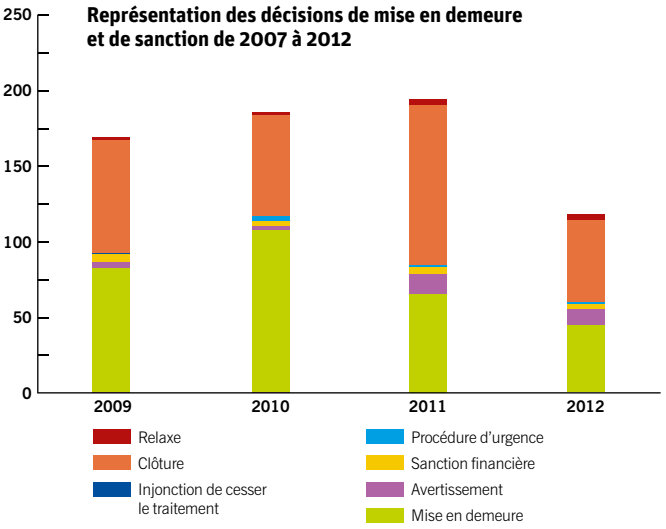
13
SANCTIONS DONT 8 SANCTIONS PUBLIQUES

9
AVERTISSEMENTS

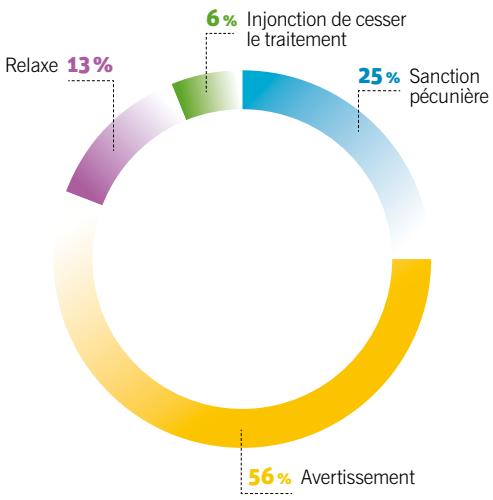
Le bilan de l'année 2012 est marqué par l'augmentation du nombre de sanctions rendues publiques par la formation restreinte. En effet, 8 des 13 décisions ont été rendues publiques, soit environ 60 % des sanctions, alors qu'en 2011, seules 21 % des sanctions ont été publiées.

L'année 2012 s'est également singularisée par l'adoption des premières mises en demeure publiques. Depuis la réforme introduite par la loi du 29 mars 2011 relative au Défenseur des droits, la Présidente de la CNIL peut demander au bureau de la CNIL (composé de la Présidente et des deux vice-présidents) de rendre publiques les mises en demeure qu'elle adopte (article 46 de la loi du 6 janvier modifiée). Les critères retenus pour justifier une telle publicité sont notamment la nature et la gravité des manquements et le nombre de personnes concernées. Pour respecter les droits des organismes faisant l'objet d'une telle décision, la clôture des mises en demeure est également rendue publique. En pratique, les mises en demeure puis les courriers de clôture sont diffusés sur le site internet de la CNIL.

Représentation des décisions de mise en demeure et de sanction de 2007 à 2012



Les sanctions prononcées en 2012

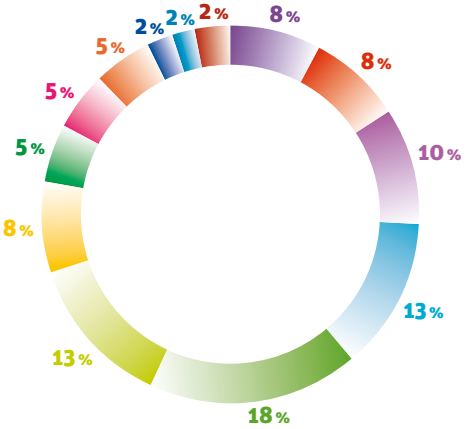


FOCUS

L'arrêt ACADOMIA du Conseil d'État du 27 juillet 2012

Dans un arrêt rendu le 27 juillet 2012, le Conseil d'État a confirmé l'avertissement public prononcé par la CNIL à l'encontre de la société AIS2 (enseigne ACADOMIA) le 28 mai 2010. Cette décision, apporte un éclairage intéressant sur différents aspects de la procédure mise en œuvre par la CNIL.
Dans cette décision, le Conseil d'État a estimé que la nouvelle procédure de contrôle mise en œuvre par la CNIL était conforme à la Convention européenne des droits de l'Homme (CEDH). En effet, la CNIL informe désormais expressément les organismes contrôlés de leur faculté de s'opposer à une mission de contrôle par la remise, en début de contrôle, d'un document spécifique leur rappelant leurs droits. Plus encore, le Conseil d'État a confirmé que la formation restreinte n'était pas tenue de développer une argumentation spécifique pour justifier de la publicité de ses décisions. Cette publicité, qui est une sanction complémentaire, peut être motivée par référence à la motivation d'ensemble de la sanction principale qu'elle complète. Enfin, la Haute juridiction a validé le fait de prononcer un avertissement à l'encontre d'un organisme et, concomitamment, de lui notifier une mise en demeure dès lors que celle-ci porte sur des faits postérieurs à l'avertissement et sont distincts de ceux-ci.

Les manquements proposés dans les rapports de sanction en 2012



- Obligation de procéder à une collecte loyale des données
- Obligation de respecter le droit d'opposition
- Obligation de répondre aux demandes de la CNIL
- Obligation d'accomplir les formalités préalables
- Obligation d'assurer la sécurité et la confidentialité des données
- Obligation d'informer les personnes
- Obligation de définir une durée de conservation non excessive
- Obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données
- Obligation de mettre à jour les données
- Obligation de garantir le droit d'accès
- Obligation de recueillir le consentement des personnes à la conservation de leurs informations bancaires
- Obligation de traiter des données de manière licite
- Obligation de proportionalité du dispositif

Liste des sanctions prononcées en 2012

Date	Nom ou type d'organisme	Décision adoptée	Manquements proposés	Thème
26/01/2012	Union régionale des syndicats CGT des établissements de l'enseignement supérieur	Sanction pécuniaire publique (5 000 euros)	Collecte déloyale, non respect du droit d'opposition, défaut de réponse à la CNIL	Prospection syndicale
16/02/2012	Commune	Avertissement non public	Défaut de formalités préalables, défaut de sécurité et confidentialité	Collectivité
08/03/2012	SYMEV	Avertissement public	Défaut de formalités préalables, collecte déloyale, défaut d'information, durée de conservation excessive	Fichier d'exclusion
08/03/2012	Organisme de ventes aux enchères publiques judiciaires	Avertissement non public	Défaut de formalités préalables, défaut d'information, défaut de sécurité	Fichier d'exclusion
08/03/2012	Organisme de ventes aux enchères publiques judiciaires	Avertissement non public	Défaut de formalités préalables, défaut d'information, défaut de sécurité, défaut de mise à jour des données et non définition d'une durée de conservation	Fichier d'exclusion
15/03/2012	Groupe scolaire	Sanction pécuniaire non publique (1 000 euros)	Caractère excessif des données, défaut d'information	Vidéosurveillance
29/03/2012	EURO INFORMATION	Avertissement public	Défaut de sécurité et de confidentialité des données	Travail
12/04/2012	Société de transport	Avertissement non public	Défaut de caractère pertinent et non excessif des données au regard de la finalité, défaut d'information	Vidéosurveillance
03/05/2012	YATEDO France	Avertissement public	Défaut de mise à jour des données, non respect du droit d'opposition, défaut de coopération avec la CNIL	Réseau social - internet
24/05/2012	Établissement Équipements Nord Picardie	Sanction pécuniaire publique (10 000 euros)	Non respect du droit d'accès, défaut de réponse à la CNIL	Travail
24/05/2012	Commune de Montreuil	Avertissement public	Traitement illicite, défaut de sécurité	Liste électorale
21/06/2012	FNAC DIRECT	Avertissement public	Défaut du recueil du consentement des personnes, non respect d'une durée de conservation, défaut de sécurité et de confidentialité des données	Données bancaires
13/09/2012	Établissement public	Relaxe	Défaut de formalités préalables, défaut de collecte loyale, défaut d'information, défaut de sécurité	Cybersurveillance
18/10/2012	Société	Relaxe	Non respect du droit d'accès	Travail/accès au dossier personnel
08/11/2012	Syndicat des copropriétaires "ARCADES CHAMPS ÉLYSÉES"	Sanction pécuniaire publique assortie d'une injonction de cesser le traitement	Non respect de proportionnalité du dispositif	Vidéosurveillance

6. CONTRIBUER À LA RÉGULATION INTERNATIONALE

Instances de régulation internationale et codes de bonne conduite

Rassembler les autorités de protection des données autour des valeurs de la francophonie

Quel cadre européen des données personnelles ?

GROS PLAN

Audit des règles de confidentialité Google : une première dans la coopération des autorités européennes

INSTANCES DE RÉGULATION INTERNATIONALE ET CODES DE BONNE CONDUITE

LE G29, GROUPE DES 27 « CNIL » EUROPÉENNES

INFOS +

Le groupe des autorités nationales de contrôle des États membres de l'UE, nommé en référence à l'article 29 de la directive de 1995 qui l'a institué.
Le G29 en 2012, c'est :
40 documents adoptés,
8 groupes de travail,
40 réunions, 5 plénières regroupant les 27 autorités de protection.

Au cours de l'année 2012, les activités du G29 ont été aussi diverses que nombreuses.

Le sous-groupe « Technologies » a vu ses travaux s'intensifier. Ont ainsi été adoptés des avis sur le *cloud computing*, la reconnaissance faciale, la biométrie, les exceptions au recueil du consentement pour les cookies. Le sous groupe s'est également attaché à analyser le projet de règlement envisagé par la Commission Européenne sur la notification des violations de données à caractère personnel. L'analyse des nouvelles règles de confidentialité de Google ainsi que le rapport d'audit de Facebook ont également fait l'objet de nombreuses discussions et d'une importante collaboration entre les membres du G29.

Le sous-groupe « e-government » s'est quant à lui penché sur le traitement des données personnelles qui peut être fait par les CERTS (Computer Emergency Response Teams), organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents, sur la proposition de directive concernant la réutilisation des informations du secteur public et sur la proposition de règlement sur l'identification électronique et les services de confiance pour les transactions électroniques.

Le G29 s'est également attaché à poursuivre ses travaux sur l'encadrement des **transferts internationaux**. Dans ce cadre, un modèle de règles d'entreprises contraignantes pour les sous-traitants élaboré par le sous groupe « Transferts » a été adopté, ainsi qu'un avis sur la demande d'adéquation de Monaco. Par ailleurs, des discussions ont été menées avec le groupe de travail « Vie privée » de l'APEC sur la possibilité de relier le système BCR et le système dénommé *Cross-Border Privacy Rules* (« CBPR ») existant dans la zone Asie – Pacifique.

Le sous-groupe « Questions financières » a poursuivi ses analyses sur le Foreign Account Tax Compliance Act **(FACTA)** qui vise à lutter contre la fraude fiscale, et sur la directive anti blanchiment.

Le sous-groupe « Frontières, voyage et activités répressives » a formulé des remarques à la Commission européenne concernant le programme Smart Borders et le projet de règlement Eurosur (système européen de surveillance des frontières). Il a également analysé le nouveau projet de dispositif d'inspection-filtrage des passagers aériens initié par **IATA** (association internationale des transporteurs aériens) ainsi que les informations sur les données passagers (API). Il a aussi suivi les questions relatives aux échanges de données **PNR** avec les pays tiers.

Le sous-groupe en charge d'analyser des problématiques transversales, a quant à lui étudié les dispositions de la directive 95/46 concernant la réutilisation des données pour un traitement ultérieur.

Enfin, **le sous-groupe « Futur de la vie privée »**, après avoir adopté un premier avis général sur le projet de réforme européen, a poursuivi ses travaux sur des sujets plus spécifiques, notamment l'expression du consentement, la définition de données personnelles, le recours aux actes délégués et d'exécution.

LE CONSEIL DE L'EUROPE ET L'OCDE

Le processus de modernisation de la Convention n° 108 du Conseil de l'Europe

Le Conseil de l'Europe a été une organisation internationale phare de la protection des données personnelles avec l'adoption du **premier instrument juridique européen contraignant en matière de protection des données en 1981** : la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite « Convention 108 »), complétée par un Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données.

Sur une initiative du Comité des ministres du Conseil de l'Europe de mars 2010, les travaux de révision de la Convention 108 ont débuté en 2011 avec pour objectif l'adaptation de ses dispositions aux réalités actuelles.

Les principales propositions d'évolution du texte sont notamment : l'insertion d'une référence au droit de chaque individu de « contrôler ses propres données » ; l'insertion d'un principe de minimisation des données ; l'inversion de la logique du droit d'opposition (le responsable de traitement devant justifier de l'existence de motifs légitimes prépondérants pour refuser de faire droit à la demande) ; la notification des failles de sécurité aux autorités de contrôle ; l'ajout des principes d'*accountability* et « de protection de la vie privée dès la conception » et la préservation de l'acquis communautaire en matière de transferts internationaux.

Le projet de modernisation de la convention 108 a été adopté par la plénière du comité consultatif dit « Comité T-PD » le 30 novembre 2012.

Il doit ensuite, après une étape de discussion au sein d'un comité intergouvernemental ad hoc (dont la première réunion est prévue pour le mois de juin 2013), être soumis au Comité des ministres du Conseil de l'Europe.

La révision des lignes directrices de l'OCDE

L'Organisation de coopération et de développement économiques (OCDE), fondée en 1960 et vouée au développement mondial, compte aujourd'hui 34 pays membres à travers le monde. Le 23 septembre 1980, l'OCDE a adopté des « *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel* », sous la forme d'une recommandation.

En 2010, à l'occasion du 30e anniversaire des lignes directrices, l'OCDE a engagé des travaux en vue de leur révision. Les principales modifications envisagées concernent notamment : l'insertion du principe *d'accountability* pour les responsables de traitements et l'obligation de notification des failles de sécurité (aux autorités compétentes et aux individus concernés).

INFOS +

L'OCDE compte 34 pays membres à travers le monde, de l'Amérique du Nord et du Sud à l'Europe, en passant par la région Asie-Pacifique et LE CONSEIL DE L'EUROPE, 47 pays membres dont la quasi-totalité des États du continent européen.

Les lignes directrices modifiées devraient être adoptées par le Conseil de l'OCDE à la fin du premier semestre 2013.

Certaines modifications impliquant de véritables changements de fond par rapport à l'approche initiale, la CNIL demeure **vigilante sur le maintien d'un niveau élevé de protection ainsi que de l'acquis communautaire, notamment en matière de règles applicables aux transferts internationaux de données personnelles**. La CNIL soutient également l'insertion d'un principe de limitation de la durée maximale de conservation des données au nombre des « principes fondamentaux » des lignes directrices.

LES RÈGLES INTERNES D'ENTREPRISE (« BCR »)

Les Binding Corporate Rules (BCR) constituent un code de conduite interne définissant la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne. Ces règles doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous les salariés de ces entités. Les BCR permettent alors d'assurer un niveau de protection suffisant aux données transférées hors de l'Union européenne au sein d'un même groupe.

Fin 2012, 40 groupes ont déjà adopté des BCR, dont **35 % ont choisi la CNIL comme autorité chef de file** pour mener ▸▸▸

40

GROUPES ONT DÉJÀ ADOPTÉ DES BCR

DONT 35 % ONT CHOISI LA CNIL COMME AUTORITÉ CHEF DE FILE

FOCUS

Le lancement des BCR sous-traitants

À compter du 1er janvier 2013, il sera également possible d'adopter des BCR « sous-traitants », destinés à encadrer les transferts intra-groupes de données traitées par un sous-traitant selon les instructions et pour le compte de ses clients responsables de traitement. Particulièrement adaptés aux évolutions technologiques telles que le Cloud computing, ces BCR créent une sphère de sécurité pour les transferts effectués par des sous-traitants, apportant alors des garanties suffisantes aux transferts pour les responsables de traitement.

les BCR, laboratoire pour la rédaction de l'*accountability* dans le projet de règlement

la procédure de coopération entre les autorités européennes de protection des données. Un guide sur les transferts, disponible sur le site de la CNIL, fournit davantage d'informations sur la procédure de coopération européenne pour les BCR.

Les BCR rencontrent de plus en plus de succès car ils constituent un outil d'encadrement des transferts, mais également parce qu'ils permettent de mettre en œuvre des mesures proactives et concrètes dites d'*accountability* (formations, audits, délégués à la protection des données, etc.). La Commission européenne a d'ailleurs récemment déclaré que les BCR avaient été « *un laboratoire pour la rédaction de l'accountability dans le projet de règlement* »[1], ce qui est confirmé par de nombreuses multinationales ayant adopté des BCR car elles les envisagent plus comme un **programme mondial de conformité** que comme un simple outil d'encadrement des transferts.

VERS UNE ARTICULATION DE L'ENCADREMENT DES FLUX ENTRE L'EUROPE (BCR) ET LA ZONE ASIE PACIFIQUE (CBPR) ?

La Coopération économique pour l'Asie-Pacifique (APEC) a récemment développé un système de règles transfrontalières de protection de la vie privée, les « Cross-Border Privacy Rules » (CBPR), afin d'apporter des garanties aux transferts de données et d'obtenir leur certification par des tiers certificateurs externes eux-mêmes agréés par l'APEC.

Partant du constat que les systèmes BCR et CBPR sont basés sur des approches similaires (codes de conduite sur les transferts internationaux développés par des entreprises et revus *a priori* par des autorités de protection des données ou par des tiers agréés), le G29 a étudié les CBPR afin d'identifier leurs similarités et leurs différences avec les BCR. Sur la base de cette comparaison, le G29 a lancé une réflexion pour développer des outils pratiques qui permettraient aux organisations d'adopter des politiques internes respectueuses des deux systèmes, et ce en vue d'obtenir **une « double certification BCR-CBPR »** dans le respect des procédures d'approbation propres à chaque zone.

En janvier 2013, des représentants d'autorités européennes de protection des données dont la CNIL, le Contrôleur européen, l'autorité allemande se sont réunis pour la première fois avec le Comité BCR/CBPR de l'APEC afin d'échanger leurs vues sur ce projet. ■

[1] *Déclaration de Marie-Hélène BOULANGER, chef de l'unité Protection des données de la Commission européenne dans le cadre du panel "A Great Ascent: How to Summit from BCR Basecamp to Accountability and Global Interoperability", organisé le 14/11 lors de la Conférence IAPP du 13-14 novembre 2012, Bruxelles*

RASSEMBLER LES AUTORITÉS DE PROTECTION DES DONNÉES AUTOUR DES VALEURS DE LA FRANCOPHONIE

Les autorités de protection des données personnelles membres de l'Association francophone des autorités de protection des données personnelles (AFAPDP) affichent une volonté de travailler ensemble. Ces autorités partagent non seulement une langue, des valeurs et traditions juridiques communes, mais également une vision de la protection des données personnelles : une vision humaniste, qui place l'individu au centre des préoccupations mais qui veut aussi offrir des solutions pragmatiques. Cette approche de la Francophonie a été réaffirmée dans la Déclaration de Monaco en 2012.

C'est également un argument retenu par les pays africains en construction ou consolidation démocratique. Au Maroc, par exemple, les responsables politiques ont compris les enjeux économiques mais également politiques de la protection des données personnelles. La protection des données personnelles est un marqueur de démocratie : l'adoption d'une législation, l'installation d'une autorité indépendante chargée de garantir l'application de la loi, est un message fort envoyé à la population marocaine en attente du renforcement des droits individuels, et aux partenaires internationaux en attente de garanties démocratiques et économiques.

La CNIL a renforcé son soutien à l'AFAPDP avec la signature d'une convention d'objectifs pluriannuelle pour 2011-2013. La CNIL affirme de cette façon son intérêt à renforcer ce réseau francophone autour de ses valeurs et de sa vision pour enrichir le débat international sur

▸▸▸

FOCUS

La Déclaration de Monaco, adoptée par l'Assemblée générale le 23 novembre 2012 à Monaco, réaffirme les principes défendus par l'association, dans le contexte de la concurrence internationale entre les conceptions de la protection des données personnelles. L'AFAPDP s'engage notamment à promouvoir l'adoption de standards internationaux de protection des données personnelles et à renforcer la coopération avec les institutions et autres réseaux concernés par la protection des données.

INFOS +

Créée en 2007, l'Association francophone des autorités de protection des données personnelles (AFAPDP) rassemble les autorités de protection des données personnelles (16 membres adhérents) et les pays de l'espace francophone qui n'ont pas encore adopté de loi dans ce domaine (membres associés de l'AFAPDP).
L'AFAPDP est un réseau de promotion du droit à la protection des données personnelles et d'échange de bonnes pratiques. Ses actions concourent à l'adoption de lois de protection des données personnelles et à la mise en place d'autorités de contrôle indépendantes.
La CNIL assure le secrétariat général de l'AFAPDP depuis 2007. Le Bureau de l'association est composé par ailleurs des représentants des autorités du Québec (présidence), du Burkina Faso et de Suisse (vice-présidences).

La voix singulière de la Francophonie est de nature à pondérer un débat mondial largement monopolisé par une approche anglo-saxonne

la protection des données personnelles. Dans le contexte d'une concurrence internationale forte entre les conceptions de la protection des données personnelles, la voix singulière de la Francophonie est de nature à pondérer un débat mondial largement monopolisé par une approche anglo-saxonne.

En outre, l'AFAPDP s'est rapprochée du Réseau ibéro américain des autorités de protection des données personnelles (www.redipd.org), puisque les deux réseaux partagent la même démarche (rassemblement autour d'une langue) et les mêmes valeurs humanistes. L'ambition des réseaux est de constituer une communauté internationale capable de proposer une vision originale et diversifiée de la protection des données personnelles.

Renforcement des compétences des autorités et de leurs outils

Depuis 2012, la CNIL participe aux travaux des groupes de travail sur l'encadrement des transferts de données dans l'espace francophone (BCR francophones) ainsi que sur la consolidation des fichiers d'état civil et des listes électorales, en partenariat avec le Réseau des compétences électorales francophones (RECEF). La CNIL accueille également tout au long de l'année les délégations des jeunes autorités francophones.

Soutien aux États qui souhaitent adopter une loi de protection des données personnelles

La présidente de la CNIL s'est rendue à Tunis en juin 2012 pour soutenir le projet de réforme de l'autorité nationale de protection des données personnelles devant les hauts responsables tunisiens. Ce type de mission de sensibilisation est réalisé en partenariat avec les réseaux institutionnels : institutions locales, Organisation internationale de la Francophonie, réseaux diplomatiques nationaux, réseaux institutionnels francophones.

Promotion de la diversité culturelle

Au sein de l'AFAPDP, la CNIL encourage l'interprétation en français lors des Conférences internationales des commissaires à la protection des données personnelles et à la vie privée. ■

QUEL CADRE EUROPÉEN DES DONNÉES PERSONNELLES ?

Suite aux consultations menées en 2011, la Commission européenne a proposé le 25 janvier 2012 une réforme de la directive de 1995 sur la protection des données personnelles, en deux volets : une proposition de règlement définissant un cadre général et une proposition de directive relative aux données traitées à des fins de police et de justice.

La réforme vise à doter l'Union de règles uniformes adaptées aux défis d'un environnement technologique en rapide évolution et d'une économie mondialisée. La directive de 1995 sur la protection des données à caractère personnel (95/46/CE) sera abrogée et remplacée par le nouveau règlement, d'application directe et qui devra être mis en œuvre dans les deux ans suivant sa publication. La nouvelle directive remplacera notamment la décision-cadre 2008/977 du Conseil du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

DES AVANCÉES SALUÉES PAR LA CNIL

Tout en réaffirmant les principes généraux relatifs aux traitements des données à caractère personnel, la proposition contient des avancées notables en ce qui concerne **les droits du citoyen**, notamment :

- le consentement des personnes au traitement de leurs données personnelles doit être explicite ;
- un « droit à l'oubli numérique » est créé – la CNIL souhaite d'ailleurs qu'il se prolonge d'un droit au déréférencement auprès des moteurs de recherche ;
- le droit à la portabilité des données est reconnu ;
- les obligations générales d'information et de transparence sont renforcées ;
- le sous-traitant se voit attribuer un statut légal à part entière.

Les formalités administratives (déclarations, consultations préalables) sont allégées au profit d'une plus grande **responsabilisation des organismes**. Ces derniers sont tenus de mettre en œuvre des mécanismes et des procédures internes afin de veiller au respect des règles contenues dans le règlement : analyse d'impact des traitements à risque, désignation d'un délégué à la protection des données pour les entreprises comptant plus de 250 employés, documentation, règles d'entreprise contraignantes, codes de bonne conduite et certification, etc.

Les autorités de contrôle voient leurs compétences et pouvoirs harmonisés (avec notamment des sanctions financières renforcées) et leur indépendance réaffirmée. Par ailleurs, une coopération renforcée entre autorités des différents États membres est mise en place, avec un rôle accru pour le G29 (rebaptisé Comité européen pour la protection des données).

> La CNIL préconise de retenir également le critère du ciblage, c'est-à-dire le lieu de résidence du citoyen concerné

DES MOTIFS DE PRÉOCCUPATION

Parmi les motifs de préoccupation identifiés par la CNIL, on retiendra principalement les suivants :

Lorsque l'entreprise a des établissements dans plusieurs États membres, l'autorité du pays de l'établissement principal de l'entreprise aurait, selon le projet initial, une compétence exclusive. La CNIL y voit une source d'insécurité juridique compte tenu de la difficulté d'identifier l'établissement principal. Elle craint également une incitation au « forum-shopping » et un facteur d'éloignement de la protection du citoyen. De plus, elle met en garde contre la possibilité de recours croisés entre autorités qui seraient contraires à l'esprit de la construction européenne.

- **La CNIL préconise de retenir, à côté de l'établissement principal du responsable de traitement ou du sous-traitant, le critère du ciblage, c'est-à-dire le lieu**

▸▸▸

de résidence du citoyen concerné. Une autorité chef de file disposant de compétence non exclusive serait désignée et agirait pour le compte des autres autorités concernées selon un système de codécision.

La possibilité est ouverte aux entreprises d'encadrer les transferts de données hors UE grâce à des instruments juridiques non contraignants ou résultant d'une autoévaluation des risques par le responsable de traitement.

La CNIL considère qu'il est essentiel de maintenir un contrôle *a priori* sur les transferts, sur la base de règles clairement définies, et d'écarter la possibilité de recours à des instruments sans valeur juridique pour encadrer ces transferts.

Le pouvoir est donné à la Commission européenne d'adopter des actes délégués et d'exécution dans un nombre important de domaines.

La CNIL souhaite une meilleure ventilation des compétences entre la Commission, le nouveau Comité européen et les autorités de contrôle nationales.

> L'intention est de parvenir à une adoption du règlement à la fin de l'année 2013, pour mise en œuvre dès 2016

LES AVIS DU G29

La CNIL a participé activement aux travaux du sous-groupe « Futur de la vie privée » du G29. Soucieuse que le citoyen reste au cœur du projet, elle s'est montrée particulièrement active sur la problématique de la compétence, multipliant les contacts avec ses homologues, la présidence du G29 et le Contrôleur européen de la protection des données.

Un **premier avis**, adopté le 23 mars 2012, reprenant sensiblement la position de la CNIL, démontre un partage des préoccupations eu égard à la proposition de règlement entre les autorités de protection des données membres du G29. Cet avis aborde d'autres questions, telles que le seuil pour l'application de certaines règles aux entreprises, la proportionnalité et la modulation des sanctions en fonction des mécanismes mis en place par les entreprises, les exemptions applicables aux autorités publiques ou la désignation d'un représentant du responsable de traitement qui n'est pas établi dans l'Union européenne. Le G29 a par ailleurs souligné la nécessité d'assurer la complémentarité et la cohérence des deux instruments proposés – règlement et directive.

Après la publication de ce premier avis général, le G29 a poursuivi ses travaux sur des problématiques plus spécifiques de la proposition de règlement, qui ont abouti à un **second avis** du 5 octobre 2012. Dans cet avis, le G29 défend le caractère nécessairement explicite du consentement, l'inclusion des adresses IP dans la définition des données personnelles et un recours limité aux actes délégués pour la mise en œuvre du règlement.

LE PROCESSUS DÉCISIONNEL

La CNIL a poursuivi ses échanges avec ses interlocuteurs à la direction générale de la justice, des droits fondamentaux et de la citoyenneté de la Commission européenne, afin d'exposer ses préoccupations. Toutefois, en 2012, les discussions se sont déplacées au Parlement européen et au Conseil de l'Union européenne. L'intention déclarée par la Commission européenne, le rapporteur au Parlement européen et la présidence irlandaise de l'Union est de parvenir à une adoption du règlement à la fin de l'année 2013, pour mise en œuvre dès 2016.

La CNIL a aussi sensibilisé la commission des affaires étrangères de l'Assemblée nationale et la commission des affaires européennes du Sénat. Respectivement en février et en mars, **les deux assemblées ont exprimé dans une résolution européenne des réserves sur la proposition de règlement en ce qui concerne les règles de compétence, rejoignant en cela la position exprimée par la CNIL**. Le 8 février 2012, à l'occasion d'un débat organisé en séance publique au Sénat sur la question de la protection de la vie privée, le Ministre de la Justice, garde des Sceaux, s'était prononcé très clairement contre le critère de l'établissement principal.

Les discussions avec le gouvernement français se sont poursuivies tout au long de l'année 2012 et devraient continuer en 2013. ■

GROS PLAN

AUDIT DES RÈGLES DE CONFIDENTIALITÉ GOOGLE : UNE PREMIÈRE DANS LA COOPÉRATION DES AUTORITÉS EUROPÉENNES

> Les autorités européennes demandent à Google de s'engager publiquement sur le respect des principes de protection des données"

Le 24 janvier 2012, Google annonçait l'entrée en vigueur de nouvelles règles de confidentialité et de nouvelles conditions d'utilisation applicables à la quasi-totalité de ses services à partir du 1er mars 2012. Face aux nombreuses questions soulevées par ces changements, la CNIL a été mandatée par le groupe des CNIL européennes (G29) pour conduire une enquête sur les nouvelles règles.

Dans le cadre de cette mission, la CNIL a envoyé un premier questionnaire à Google le 16 mars 2012. Un certain nombre des réponses fournies par Google s'étant avérées incomplètes ou approximatives, un questionnaire complémentaire a été envoyé le 22 mai 2012. En particulier, Google n'avait pas fourni de réponses satisfaisantes sur des points essentiels comme la description de tous les traitements de données personnelles qu'il opère ou la liste précise des plus de 60 politiques de confidentialité qui ont été fusionnées dans les nouvelles règles.

> 60 politiques de confidentialité ont été fusionnées dans les nouvelles règles

Sur la base de l'analyse des réponses fournies par Google et suite à l'examen, par les experts de la CNIL, de nombreux documents et mécanismes techniques, les autorités européennes ont tiré leurs conclusions et formulé des recommandations sous la forme d'un courrier adressé à Google le 16 octobre 2012 et signé par 27 autorités européennes de protection des données.

Cette initiative constitue une première et une avancée considérable dans la mobilisation et la coopération des autorités européennes. ▸▸▸

LES PRINCIPALES CONCLUSIONS ET RECOMMANDATIONS

L'analyse menée ne permet pas de s'assurer que Google respecte les principes essentiels de la Directive sur la protection des données personnelles que sont la limitation de finalité, la qualité et la minimisation des données, la proportionnalité et le droit d'opposition. En effet, les nouvelles règles de confidentialité suggèrent l'absence de toute limite concernant le périmètre de la collecte et les usages potentiels des données personnelles.

Google fournit des informations incomplètes ou approximatives sur les finalités et les catégories des données collectées

Avec les règles actuelles, l'utilisateur d'un service Google est incapable de déterminer quelles sont les données personnelles utilisées pour ce service et les finalités exactes pour lesquelles ces données sont traitées. Il arrive même que les utilisateurs ne reçoivent aucune information quant aux données qui sont traitées. Tel est le cas des utilisateurs passifs, c'est-à-dire de ceux qui n'interagissent avec Google qu'au travers des plateformes publicitaires tierces ou des boutons " +1 ".

Les autorités européennes ont donc demandé à Google de fournir une information plus claire et plus complète sur les données collectées et les finalités de chacun de ces traitements de données personnelles. Par exemple, les autorités européennes ont recommandé la mise en place d'une présentation avec trois niveaux de détails qui assurera une information conforme aux exigences de la Directive sans dégrader l'expérience des utilisateurs. L'ergonomie de la lecture des règles pourrait également être améliorée grâce à des présentations interactives.

Google ne permet pas le contrôle par les utilisateurs de la combinaison de données entre ses nombreux services

La **combinaison de données entre services** a été généralisée avec les nouvelles règles de confidentialité : concrètement toute activité en ligne liée à Google (l'utilisation de ses services, de son système Android ou la consultation de sites tiers utilisant des services Google) peut être rassemblée et combinée.

Les CNIL européennes relèvent que cette combinaison poursuit des finalités différentes. Il s'agit :

- de la fourniture de services où l'utilisateur demande la combinaison des données,
- de la fourniture de services demandés par l'utilisateur et où la combinaison s'opère sans que l'utilisateur en soit directement informé,
- de la finalité de sécurité,
- du développement de produits et d'innovation marketing,
- de la mise à disposition du Compte Google,
- de la publicité,
- de l'analyse de fréquentation,
- de recherche universitaire.

La législation européenne prévoit un cadre précis pour les traitements de données personnelles et exige notamment que le responsable de traitement dispose d'une base légale et que la collecte soit proportionnée aux finalités poursuivies. Or, pour certaines de ces finalités, notamment la publicité, Google ne peut s'appuyer ni sur le consentement de la personne, ni sur son intérêt légitime, ni sur l'exécution d'un contrat.

▸ Google doit donc modifier ses pratiques et notamment : renforcer le consentement des personnes pour la combinaison des données pour certaines finalités, offrir un meilleur contrôle des utilisateurs sur la combinaison de données en centralisant et simplifiant le droit d'opposition (opt-out) et en leur permettant de choisir pour quels services leurs données sont combinées, et enfin adapter ses outils afin de limiter cette combinaison aux finalités autorisées.

Google ne précise pas les durées de conservation des données récoltées

Enfin, en dépit des questions précises et réitérées soumises par les CNIL européennes, Google n'a pas été en mesure de fournir une durée maximale ou habituelle de conservation des données personnelles traitées.

▸ Les CNIL européennes ont donc demandé à Google de respecter le principe d'une durée de conservation strictement limitée au regard des finalités.

La CNIL et les autorités européennes accueillent favorablement l'initiative de Google de réduire et de simplifier ses règles de confidentialité. Toutefois, cette évolution ne doit pas se faire au prix d'une information moins transparente et moins complète. Google dispose de quatre mois à compter du 16 octobre 2012 pour se mettre en conformité sur les différents points évoqués. ■

7. ANTICIPER ET INNOVER

GROS PLAN

Vie privée a l'horizon 2020 : quelles transformations, quels enjeux et quelle régulation ?

Accompagner l'innovation : une activité centrale pour la CNIL

GROS PLAN

VIE PRIVÉE À L'HORIZON 2020 :

QUELLES TRANSFORMATIONS, QUELS ENJEUX ET QUELLE RÉGULATION ?

> À l'heure du « tous connectés », la protection des données personnelles au centre d'enjeux technologiques, économiques, juridiques, sociaux et éthiques ”

L'environnement a totalement changé depuis une dizaine d'années. L'informatique des grands fichiers publics qui prévalait en 1978 a, peu à peu, fait place à un « univers numérique », celui de la dématérialisation des activités, des professions et des usages. Des changements des pratiques sociales et des modèles économiques en ont résulté et sont toujours en cours.

Face aux défis pour la protection des données personnelles que sont le *cloud computing*, le *big data*, l'*Open data*, le développement des réseaux sociaux, l'internet mobile et la banalisation de la géolocalisation, il est nécessaire de bâtir le cadre juridique et éthique de l'univers numérique de demain. Or, la CNIL ne peut, ni ne doit intervenir de façon isolée. Il lui est indispensable d'être à l'écoute de la société civile, de dialoguer avec elle et de solliciter le plus grand nombre possible de points de vue, afin de mieux saisir l'environnement complexe et mouvant dans lequel elle intervient. Cela lui permet également de mieux anticiper les évolutions technologiques, les usages innovants, les risques émergents et les nouvelles attentes en termes de régulation des données personnelles, et d'apporter des réponses adaptées.

C'est dans ce contexte que la direction des études, de l'innovation et de la prospective de la CNIL a lancé, à l'automne 2011, un chantier prospectif. Il l'a conduit à rencontrer jusqu'au printemps 2012 une quarantaine d'experts d'horizons variés : sociologues, économistes, philosophes, juristes, historiens, chercheurs en sciences

de la communication et en sciences de l'ingénieur en informatique, représentants du monde de l'entreprise et d'associations intervenant dans les domaines du numérique et/ou de la défense des droits des personnes, etc.

Ces experts ont été interrogés sur :

- Les incidences des principales évolutions technologiques, économiques et sociétales dans le champ de la vie privée, des libertés et des données personnelles ;
- Les transformations, en cours ou à venir, dans la relation des individus et de la société à la vie privée et aux données personnelles ;
- Leur vision des formes de régulation de demain, leurs attentes à propos des autorités de protection des données ;
- Leurs projets et orientations dans le champ concerné.

Ces entretiens ont donné lieu à une synthèse qui a été publiée dans le premier numéro des *Cahiers IP - Innovation & Prospective* - sous la forme d'une étude sur les défis de la protection des données à l'horizon 2020.

La CNIL a aussi pris une deuxième initiative destinée à associer la communauté intellectuelle à ses réflexions, en organisant le 30 novembre 2012 une journée d'étude « *Vie privée 2020* » dans les locaux du Monde. Elle a ainsi souhaité apporter son concours à la constitution d'une communauté de recherche en matière de protection des données, qui réunirait des spécialistes de tous horizons.

Quatre tables rondes, symbolisant les principaux enjeux de la protection des données personnelles pour aujourd'hui et pour demain, se sont succédées, avec la participation des sociologues Dominique Cardon, Antonio Casilli, Dominique Boullier et Emmanuel Kessous, du directeur de recherche de l'INRIA Daniel Le Métayer, des avocats Olivier Iteanu et Alain Bensoussan, des économistes Fabrice Rochelandet et Alain Rallet, de la philosophe du droit Antoinette Rouvroy, de la spécialiste des sciences de gestion Caroline Lancelot-Miltgen, du juriste Jean Frayssinet, des acteurs du numérique Daniel Kaplan, Christine Balagué et Philippe Lemoine, du journaliste Jean-Marc Manach, ainsi que de la présidente d'IRIS, Meryem Marzouki.

JOURNÉE D'ÉTUDES VIE PRIVÉE 2020 : QUELQUES RÉFLEXIONS CLÉS DES EXPERTS

1/ La révolution du web social

La révolution du web social permet l'apparition d'une nouvelle forme d'expressivité, qui est ouverte à tous. Chacun peut dorénavant exprimer sa singularité au travers de manifestations de soi, de ses activités conversationnelles et de ses centres d'intérêt, et ainsi devenir une « *personne publique* ». L'individu peut s'exprimer dans un espace qui n'est pas exactement public, mais qui se situe entre le privé et le public. La tendance à la « *théâtralisation de soi* » qui s'en suit fait bouger le curseur entre vie privée et vie publique et l'individualise : chaque individu peut déplacer ce curseur pour ce qui le concerne. La vie privée devient une revendication des personnes dans un mouvement d'autonomie individuelle. Ce modèle n'en suscite pas moins des interrogations sur la réalité de la maîtrise sur sa vie privée et sur ses données personnelles.

Par ailleurs, ce qui est dit sur les réseaux sociaux est toujours lié à un contexte. Dès lors, la légitimité des regards extérieurs, par opposition à ceux des destinataires initiaux, est très incertaine. Or, on a, jusqu'à présent, surtout mis l'accent sur la personne qui s'expose sur les réseaux sociaux, en lui demandant d'être consciente des risques qu'elle prend. Ne faudrait-il pas également s'interroger sur l'attitude de celui qui regarde, hors contexte, des éléments qui ne le concernent pas ?

2/ Sommes-nous entrés dans la dictature du calcul des algorithmes ?

Le *big data* et le *cloud computing* banalisent les traitements de masse et offrent, grâce à des analyses algorithmiques toujours plus poussées, de nouvelles modalités de valorisation des données, des profilages de plus en plus individualisés et des analyses censées

▸▸▸

Les idées exprimées reflètent les avis formulés par les experts invités par la CNIL

JOURNÉE D'ÉTUDES VIE PRIVÉE 2020 : QUELQUES RÉFLEXIONS CLÉS DES EXPERTS suite

prédire les comportements. Avec le *big data*, l'extraction de connaissances nécessite l'utilisation de techniques d'intelligence artificielle, d'apprentissage informatique et de réseaux neuroniques. Ainsi apparaît une nouvelle manière de gouverner qui ne s'appuie que sur du pur calcul : il suffit de mettre en place des ensembles de données brutes et de leur appliquer des algorithmes qui fabriqueront automatiquement des modèles de comportements.

On assiste ainsi, avec les applications de *data mining* et de profilage, à une « *objectivation à distance des comportements* ». Les individus sont de plus en plus catégorisés, non pas au travers de catégories préexistantes, mais dans le cadre d'un « *nouveau régime d'intelligibilité du réel* » qui dispense de toute normativité préétablie. Dès lors, la personnalisation se passe de tout rapport à une norme commune. Ces dispositifs informatiques sont à l'origine d'une nouvelle manière d'interpréter le réel et le monde : ils font parler nos données à notre place. À la rationalité déductive succède une rationalité inductive qui, de plus, se veut prédictive.

Mais souhaitons-nous vivre dans une société dans laquelle toutes nos interactions et transactions pourraient être gouvernées par nos comportements passés ?

Ces évolutions sont également à l'origine d'autres questionnements : la personnalisation qui en résulte est paradoxale, puisque ce travail s'effectue sans jamais demander l'avis de l'individu sur ses désirs et ses intentions. Or, comment peut-on devenir des sujets si nos désirs nous précèdent, si l'on est de fait réduit à nos activités passées ? Comment, par ailleurs, garantir un espace public de délibération si l'on s'en remet à des systèmes algorithmiques pour évaluer le réel ?

3/ La donnée au cœur des modèles d'affaires

La donnée personnelle étant placée au cœur des modèles d'affaires du numérique, il n'est pas surprenant que l'on entende de plus en plus parler de monétisation des données personnelles. Mais peut-on croire à un « *marché* » des données personnelles ? Le droit à la souveraineté sur sa vie virtuelle passe-t-il par la reconnaissance d'un droit de propriété sur ses données ? La protection des données peut-elle être aussi source d'activités économiques ?

Au plan économique, la promesse du *big data* correspond à un monde totalement personnalisé dans lequel le calcul domine au détriment des autres formes de rationalités économiques. Dans ce monde, le système concurrentiel ne porte plus sur le rapport qualité-prix mais sur les mécanismes de singularisation du service. Le marché passe des « *biens* » au « *lien* », grâce aux traces d'usage. La vision collective de l'humanité ne risque-t-elle pas d'être ainsi mise à mal ?

4/ Quelles nouvelles formes de régulation pour demain ?

Depuis 1978, les frontières entre vie publique et vie privée sur lesquelles était initialement fondée la loi « Informatique et Libertés », se sont déformées. De nouvelles frontières sont apparues, entre économie de marché et logique d'émancipation des personnes. Ces changements sont essentiels, dans la mesure où de plus en plus de *business models* sont fondés sur la captation des données. À l'inverse, des mouvements visent à développer un internet citoyen.

Pour certains, une régulation purement procédurale devrait se substituer à l'actuelle régulation substantielle. Le consentement de l'individu devrait en être la clé, conduisant ainsi à faire de l'individu un personnage souverain. Mais celui-ci sera-t-il toujours en mesure de faire ses arbitrages ? Est-il souhaitable d'ailleurs de lui demander de s'installer dans une logique de marché ? Par ailleurs, le concept de *privacy* prend une place croissante dans les réflexions européennes.

Sur toutes ces questions, il est nécessaire de gagner la bataille conceptuelle et idéologique, car des modèles s'affrontent dans un contexte de concurrence internationale. Seul le plus attractif sera promu. Les Européens devront être capables de proposer des concepts nouveaux et de compléter ceux qui existent, par exemple en reconnaissant de nouveaux droits. Certains craignent que parler de régulation constitue une régression. Pourtant, au-delà des querelles de mots, il apparaît que la simple contrainte législative et réglementaire ne saurait suffire. La régulation est à comprendre comme un « *art de saltimbanque* », l'art de régir les rapports entre individus. Elle ne peut qu'être constituée par l'ensemble des outils qui sont utiles pour administrer le système. Ce qui comprend notamment la réglementation.

ACCOMPAGNER L'INNOVATION : UNE ACTIVITÉ CENTRALE POUR LA CNIL

Afin de renforcer sa mission de veille et de réflexion prospective, la CNIL a créé en mai 2012 un Comité de la Prospective faisant appel à des experts extérieurs. Ouverture, démarche pluridisciplinaire, confrontation d'idées, innovation dans son mode de gouvernance… tels sont les mots clés de cette initiative.

LA CRÉATION D'UN COMITÉ DE LA PROSPECTIVE : DE NOUVEAUX HORIZONS POUR LA CNIL

La Commission estime indispensable de développer sa compréhension des évolutions du numérique et d'innover dans son mode de gouvernance.

Ce comité se veut en premier lieu un comité d'orientation scientifique des études conduites par la CNIL. Il a donc un rôle de conseil notamment dans le cadre de l'élaboration du programme annuel d'études et dans l'exploration de nouveaux champs d'études (par exemple dans le domaine des neurosciences). Les premières réunions du comité ont d'ailleurs été l'occasion de définir plus précisément les sujets d'études pour les deux années à venir (cf. ci-après).

Véritable « Boîte à idées », le comité peut également jouer un rôle moteur dans le développement d'un espace d'échanges et de réflexion sur les problématiques « Informatique et Libertés ». Il peut par exemple initier ou animer des tables rondes avec d'autres experts et favoriser ainsi le débat public sur les enjeux « Informatique et Libertés ». Le comité a ainsi contribué à la préparation de la journée d'études « vie privée 2020 » organisée le 30 novembre 2012.

Enfin, il s'agit aussi de renforcer l'expertise de la CNIL, notamment dans les domaines économiques et sociologiques, pour mieux identifier, comprendre et anticiper les transformations technologiques présentes et à venir et en évaluer les enjeux éthiques.

INFOS +

Placé sous la présidence de la Présidente de la CNIL, le comité se compose de :

- **M. Pierre-Jean Benghozi, directeur de recherche au CNRS, professeur à l'École Polytechnique (directeur du pôle de Recherche en Économie et Gestion). Il est en charge de la Chaire d'enseignement et de recherche « Innovation et Régulation des services numériques »**
- **Mme Stefana Broadbent, psychologue, professeur d'Anthropologie à l'*University College* de Londres (UCL) où elle enseigne l'anthropologie numérique. Elle dirige le Master en Anthropologie du numérique dans le département d'Anthropologie de UCL et elle participe aux recherches du Center for Digital Anthropology de UCL**
- **M. Dominique Cardon, sociologue au Laboratoire des usages SENSE d'Orange Labs, chercheur associé au Centre d'étude des mouvements sociaux de l'École des Hautes Études en Sciences sociales (CEMS/EHESS)**
- **M. Olivier Oullier, professeur à Aix-Marseille Université, chercheur au laboratoire de psychologie cognitive (UMR CNRS 7290) et au Center for Complex Systems and Brain Sciences, conseiller scientifique au Département Questions sociales du Centre d'analyse stratégique et Young Global Leader du Forum Économique Mondial**
- **Mme Antoinette Rouvroy, chercheur qualifié du FRS-FNRS en philosophie du droit, associée au Centre de Recherche en Information, Droit et Société (CRIDS), chargée de cours à l'Université de Namur et maître de conférences à l'Université Libre de Bruxelles**
- **M. Henri Verdier, directeur d'Etalab, dirigeant d'entreprise, membre du conseil scientifique de l'institut Mines-Télécom**
- **M. Didier Gasse, conseiller maître honoraire à la Cour des comptes, membre de la CNIL en charge du secteur télécommunications et internet – sécurité - vote électronique**
- **M. Gaëtan Gorce, sénateur de la Nièvre, membre de la CNIL en charge du secteur libertés publiques et e-administration**

LE PROGRAMME D'ÉTUDES 2012-2013

Construit avec l'aide du **Comité de la Prospective** et approuvé par la Commission en juillet 2012, ce programme définit les principaux axes du programme d'études de la CNIL dans les domaines de l'innovation et de la prospective pour 2012 et 2013. Ces axes de travail sont les suivants.

Un travail autour des usages des photos et de la perception de la reconnaissance faciale

300 millions de photos sont publiées chaque jour sur Facebook. Chaque géant du web a acquis une entreprise développant une technologie de reconnaissance faciale. Les utilisateurs de smartphones et de réseaux sociaux sont confrontés quotidiennement à la question de cette place des images et photos dans leur « patrimoine numérique personnel ». Il apparaît nécessaire d'avoir une vision plus complète des comportements et usages réels des utilisateurs : appliquent-ils des règles particulières aux choix des photos publiées, à leur accessibilité, au tag de personnes,… et ce pour les différents types de photos : les photos de profil, les photos personnelles, les photos taguées ou non… comment conçoivent-ils le respect de l'intimité de leurs proches et amis, de quelle façon assurent-ils les droits des tiers ?

Pour répondre à ces questions un sondage a été réalisé fin 2012. Par ailleurs la CNIL élabore une feuille de route technologique comportant une analyse des technologies existantes et en émergence, complétée de démonstrations et d'expérimentations au sein du laboratoire de la CNIL.

Une étude prospective de la biométrie dans la vie quotidienne à l'horizon 2020

Les technologies biométriques sont de plus en plus nombreuses, et elles peuvent s'employer dans des contextes de plus en plus variés. Cependant, la biométrie reste une technologie qui semble encore peu utilisée dans la vie quotidienne, en dehors des usages de souverainetés – police… Les produits grand public qui ont été développés (verrouillage d'ordinateurs portables…) ont pour le moment eu un succès limité pour diverses raisons. Quel est l'état réel du marché des différents types de biométries en France et à l'étranger ? Quelle place pour la biométrie dans la vie quotidienne (Internet des objets,

enjeux de cybersécurité et d'identification, paiement mobile…) ? En lançant cette étude, il s'agit pour la CNIL de tenter d'anticiper sur d'éventuels champs d'applications nouveaux de la biométrie, de dresser un panorama comparatif des usages et technologies biométriques dans d'autres pays (Europe, Asie, Amérique du nord) et de contribuer aux travaux de réflexion engagés par la CNIL quant à l'évaluation de ses positions sur le sujet.

Deux chantiers exploratoires sont également engagés par la DEIP :

Le premier **autour de la question de la santé et du bien-être dans le monde numérique**, que bouleverse l'apparition de nombreux services nouveaux se trouvant souvent à la frontière entre le monde médical et la question du bien-être au quotidien : applications mobiles de santé sur smartphones, parfois avec des capteurs dédiés, services de réseaux sociaux centrés sur des communautés de patients, suivi et aide des malades de maladies chroniques, apparition de communautés pratiquant l'auto-mesure (*Quantified Self*). Il est, du point de vue prospectif, intéressant d'analyser le faisceau convergent de ces nouveaux usages et besoins de services de santé et d'en évaluer les enjeux éthiques et en particulier de protection des données personnelles.

Le second chantier ouvert se concentre sur **l'influence des usages numériques dans les relations de travail**, l'atténuation de la frontière entre la vie privée et la vie professionnelle, notamment avec l'essor du « *Bring your own device* », c'est-à-dire l'utilisation, de plus en plus massive, des smartphones et tablettes personnels au travail. Il s'agit de dresser un état des lieux des usages numériques au travail et de leurs conséquences en matière de relations entre employés, dans le management et dans les relations hiérarchiques. Il s'agira en particulier d'analyser l'évolution des **techniques de suivi d'activité** (monitoring de performance, reporting…) voire de **surveillance au travail**.

Ces thèmes feront l'objet de travaux internes d'analyse et de veille, ils alimenteront la feuille de route du laboratoire d'innovation et serviront de base à des partenariats ou des études externes.

PARTENARIATS ET COOPÉRATION

Poursuivant sa démarche de coopération avec le monde académique, la CNIL a signé, à l'occasion de la journée d'études vie privée 2020, le 30 novembre 2012 une convention de partenariat avec l'institut mines-telecom. Celle-ci permettra notamment de sensibiliser encore plus la communauté scientifique à la protection des données et de la vie privée et de mener des travaux de recherche en commun. Première application pratique, la direction des études, de l'innovation et de la prospective était présente aux 7e entretiens de Télécom ParisTech, les 5 et 6 décembre 2012 sur le thème *big Data*, *big value*, et est intervenue lors d'une table ronde consacrée à la protection des données personnelles.

Enfin, la Commission participe activement à plusieurs groupes de travail, en France et à l'international, afin de développer des bonnes pratiques de sécurité protectrices de la vie privée.

Elle est ainsi présente notamment :

• à l'ISO (organisation de normalisation internationale), dans laquelle un de ses agents joue le rôle d'éditeur de la principale norme en sécurité, l'ISO/IEC 27001, relative au système de management de la sécurité de l'information, où la CNIL agit en tant que liaison avec le G29 pour coordonner les positions de ses homologues européens sur les projets de normes relatifs à la protection de la vie privée, et où elle participe au développement de nouvelles normes relatives au *cloud computing*, à la gestion des risques sur la vie privée, etc. ;

• au Club EBIOS (communauté d'experts en gestion des risques), que l'un de ses agents préside ;

• au CESIN (communauté de responsables de la sécurité des systèmes d'information).

Innover dans le débat « Informatique et Libertés » : le PrivacyCamp

Pour la première fois, la CNIL a organisé, en association avec des acteurs du numérique, un événement participatif et ouvert sous la forme – innovante pour la CNIL – d'un Barcamp, c'est-à-dire d'une non-conférence ouverte à tous ceux qui le souhaitent.

Le 30 mars 2012, à l'invitation de la CNIL, et en association avec Mozilla, Owni et Silicon Sentier, la communauté du numérique a ainsi pris possession de La Cantine, lieu d'échanges et espace de *coworking*, pour une demi-journée de

▸▸▸

FOCUS

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.
Pour la 4e année consécutive, la CNIL a attribué le prix « Informatique et Libertés ». Le jury du Prix, présidé par M. Jean-Marie COTTERET, membre de la CNIL, a décidé de récompenser Mme Jessica EYNARD, docteur en droit privé (Université de Toulouse Capitole 1) et qualifiée aux fonctions de Maître de conférences par le Conseil National des Universités, pour son essai remarqué sur la donnée à caractère personnel. Son travail, particulièrement d'actualité, notamment dans le cadre de la révision de la législation européenne en la matière, fera l'objet d'une publication dans les mois à venir.

Le jury présidé par M. Jean-Marie COTTERET se compose de :
- **M. Daniel Le Metayer**, Directeur de recherches INRIA
- **Mme Nathalie Mallet-Poujol**, Directrice de recherches CNRS
- **M. Jean-Emmanuel Ray**, Professeur à l'Université Paris I – Panthéon – Sorbonne
- **M. Fabrice Rochelandet**, Maître de conférences à l'Université Paris Sud
- **M. Michel Riguidel**, Professeur émérite à Télécom ParisTech
- **Mme Sophie Vulliet-Tavernier**, Directrice des études, de l'innovation et de la prospective de la CNIL
- **M. Dominique Wolton**, Directeur de l'Institut des Sciences de la Communication du CNRS

Remise du prix de thèse 2012 à Madame Jessica EYNARD

rencontres et d'échanges autour de la question « comment contrôler ses données personnelles sur le web ? ».

Innovation dans la forme comme dans le fond pour la CNIL, cet événement a été un succès : une centaine de personnes se sont inscrites pour venir échanger autour des outils, des pratiques et des services permettant de maîtriser sa vie privée en ligne et de comprendre les flux et « fuites » de données personnelles en ligne.

Détecter les signaux faibles de l'innovation technologique

La Direction des études et de la prospective a aussi développé ses participations et interventions dans des événements autour de ses sujets de travail. Ainsi, elle était présente à la conférence LeWeb, conférence internationale qui se déroule à Paris tous les ans. Le thème central cette année était l'internet des objets. La tendance du *Quantified Self* était également à l'honneur.

Elle a également participé et est intervenue à la conférence annuelle de l'IDATE, le DiGiworld Summit qui avait pour thème cette année « *Game changers : mobile, cloud, big data* ».

LE LABORATOIRE D'INNOVATION

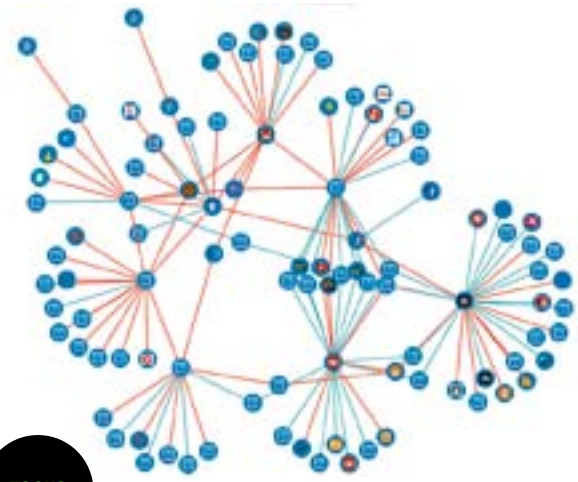
Ce laboratoire, créé en 2011, répond à la volonté de la CNIL de disposer en son sein de moyens informatiques dédiés permettant de tester et d'expérimenter, en réel, des produits et applications innovants. Il permet de disposer de nouveaux produits ou services afin d'en tester les fonctionnalités et d'en évaluer les impacts sur la protection de la vie privée.

Le laboratoire est donc pleinement opérationnel au plan technique depuis le début de l'année 2012 : une infrastructure associant des machines (serveurs, ordinateurs…) et un réseau informatique propre a été constitué et offre une plateforme technique sur laquelle de nombreux projets viennent s'appuyer. Tout au long de l'année, des tests sont donc réalisés grâce à ce matériel spécialement configuré : analyse des fuites de données sur des applications mobiles, étude sur les réseaux sociaux, tests de matériel biométrique…

De manière plus ambitieuse, le laboratoire porte des projets d'analyse et d'expérimentation qui sont en quelque sorte et toutes proportions gardées, à la CNIL ce que des projets de « Recherche & Développement » sont pour une entreprise. Ces projets prennent progressivement plus d'ampleur, et un premier projet lancé début 2012 montre l'ensemble des facettes de cette activité de laboratoire d'innovation.

Un autre projet a été lancé au second semestre 2012 et s'articule autour des « cookies » et de la traçabilité en ligne. Tout comme l'écosystème des smartphones, ce monde des cookies est marqué par une grande opacité : sauf à s'intéresser vraiment à la question, il est très difficile pour l'internaute de savoir quand et comment il est « tracé » par des programmes et outils aux finalités variées (analyses statistiques des visites, aide à l'achat en ligne, mais aussi et peut-être surtout ciblage publicitaire). La CNIL a donc décidé d'explorer ce monde au sein du laboratoire sous deux angles complémentaires : vu depuis la navigation de l'internaute, et vu depuis l'analyse macroscopique du web. Sous le premier angle, la CNIL dispose aujourd'hui d'un outil très pédagogique pour comprendre ce qu'est réellement un cookie et comment les cookies sont utilisés pour tracer les internautes. Cet outil, baptisé *CookieViz*, représente sur un graphe interactif et dynamique en temps réel au cours d'une navigation l'apparition de liens vers des sites tiers par des cookies ou autres codes. Il est pour le moment utilisé par les services lors de présentations publiques sur le thème des cookies et permet de faire mieux comprendre les recommandations du G29 et de la CNIL en la matière. Le laboratoire travaillera en 2013 sur une version web de cet outil pouvant éventuellement être mise à la disposition du public. Sous le second angle, un projet baptisé *CookieMiner* est en cours de développement depuis l'automne 2012 et vise à cartographier de la manière la plus exhaustive possible la présence de cookies et autres traqueurs dans le web français en « .fr ».

Progressivement, le laboratoire va donc élargir ses travaux pour aller vers plus d'expérimentations, d'essais et des développements d'outils. Le laboratoire pourra alors étendre son action pour porter les actions innovantes et expérimentales de la CNIL et cela en tout domaine : l'innovation doit pour la CNIL être technologique, mais aussi sociétale et juridique ! Le laboratoire sera un support essentiel dans la création d'une plateforme d'innovation ouverte au service de l'institution. ■



Outil « CookieMiner » développé par le laboratoire.

FOCUS

Mobilitics

Le laboratoire porte un projet de développement très concret lancé conjointement par la CNIL et l'INRIA dans le cadre de la convention de partenariat qui lie l'autorité à cet institut public de recherche, leader européen et mondial dans les recherches en informatique et sciences du numérique. Intitulé « *Mobilitics* », ce projet commun de recherche est tourné vers les smartphones et l'analyse de ce qui se passe à l'intérieur de ces « boîtes noires ». *Mobilitics* est ainsi une suite directe des travaux « smartphones et vie privée » pilotés en 2011 par la Direction des études, de l'Innovation et de la Prospective (voir rapport annuel 2011, pp : 23 à 27). Après un an de développement et d'échanges réguliers, une équipe de chercheurs INRIA[1] et la CNIL disposent à présent d'un outil qui permet de pousser très loin l'analyse du fonctionnement et des usages des smartphones et de la manière dont est géré l'accès aux données personnelles dans un téléphone (en particulier ce qui se passe lorsqu'une application cherche à accéder à un certain nombre de données personnelles : carnet d'adresses, localisation géographique, identifiant unique du téléphone, photographies...). À la fin de l'année 2012, le laboratoire a, pour la première fois, lancé une expérimentation *in vivo* avec l'aide de volontaires parmi les agents de la CNIL. Cette première expérimentation - qui consistait en l'utilisation, en condition réelle, de téléphones du laboratoire spécialement configurés - a permis de recueillir beaucoup de données qui sont en cours d'analyse et de valorisation. Certaines de ces analyses seront diffusées prochainement auprès des spécialistes par l'intermédiaire de publications dans des revues scientifiques ou techniques spécialisées. Cependant, l'ambition du laboratoire est plus large que de simplement valoriser des travaux auprès du monde de la recherche : il s'agit aussi d'explorer de nouvelles manières de diffuser une culture technologique et une pédagogie des usages en développant notamment des outils à destination du grand public. Le projet Mobilitics s'attachera en 2013 à se tourner ainsi vers l'extérieur, par exemple par la publication des enseignements tirés de l'analyse des données issues de l'expérimentation, mais aussi en explorant le prototypage de solutions techniques (par exemple permettant de tester la faisabilité de nouvelles solutions protectrices de la vie privée sur smartphones).

Ce projet Mobilitics est un bon prototype des futurs projets du laboratoire : ancrés dans un besoin d'approfondissement d'une thématique émergente et identifiée comme prioritaire par l'institution, ils devront se déployer à la fois vers le monde de la recherche, vers l'expérimentation réelle mais aussi vers la promotion d'outils concrets de maîtrise des données.

[1] *Équipe INRIA « Planete » http://planete.inria.fr/*

8.
LES SUJETS DE RÉFLEXION EN 2013

Big Data, tous calculés ?

Vers un droit à l'oubli numérique ?

La biométrie : une doctrine pragmatique et évolutive

BIG DATA, TOUS CALCULÉS ?

Jusqu'à récemment, les traitements massifs de données semblaient réservés à des acteurs disposant d'infrastructures informatiques importantes. La quantité exponentielle de données désormais disponibles et le cloud « démocratisent » aujourd'hui l'accès à ces traitements de masse et offrent des possibilités nouvelles de valorisation des données.

FOCUS

Les 3 V du Big Data

- **Le Volume : La masse de données informatiques et numériques produites en 2008 sur Internet représentait 480 milliards de gigaoctets. En 2010, ce furent 800 milliards soit l'équivalent de ce que l'humanité avait écrit, imprimé, gravé, ou enregistré jusqu'en 2003. 90 % des données ont ainsi été créées ces deux dernières années et on s'attend à une croissance annuelle de 40 % dans le monde entre 2011 et 2020[1].**
- **La Variété : le volume et la variété sont intrinsèquement liés à l'évolution des usages : les utilisateurs partagent des données issues de tout une diversité de contenus (photos[2], vidéos, billets de blog, micro-conversations, objets et capteurs connectés);**
- **La Vélocité : le traitement de grande masse de données est aujourd'hui simplifié. De nouvelles générations de technologies et d'algorithmes offrant toujours plus de puissance et d'analyse de calcul permettent de traiter de nouveaux types de données, en particulier non-structurées, et ont favorisé l'émergence d'une industrie qui pesait près de 700 milliards d'euros en 2012[3].**

Le concept de Big Data est certainement l'un des thèmes les plus en vogue lorsque l'on s'intéresse aux évolutions technologiques pouvant avoir le plus d'impact dans les 10 prochaines années, aussi bien sur un plan économique que sociétal. Le Big Data est souvent caractérisé par la formule dite des « trois V » : volume et variété dans un premier temps, car on amasse des sommes de données de plus en plus considérables par des moyens variés ; vélocité dans un second temps, car la masse des données recueillies doit être traitée en temps réel.

Ainsi, l'avènement du Big Data va-t-il permettre l'émergence d'une nouvelle forme de science, sans hypothèse ? Une nouvelle manière de prendre des décisions qui ne s'appuierait que sur du pur calcul, autour de modèles de comportements ? Quels enjeux nouveaux pose-t-il en termes « Informatique et Libertés » ?

NOUVELLES DONNÉES, NOUVEAUX CHAMPS, LE BIG DATA S'INVITE PARTOUT...

Les opportunités offertes par le Big Data sont aujourd'hui majoritairement valorisées dans le domaine du marketing et de la publicité pour des usages d'analyse des données sur le comportement des consommateurs dans le but de mieux anticiper leurs attentes. La publicité en ligne constitue sans doute la meilleure illustration au travers du développement de techniques permettant d'affiner le ciblage publicitaire en fonction du profil avec des adaptations en temps réel[4] du message affiché, ou le recours à des techniques de « re-targeting » ou reciblage publicitaire pour améliorer l'efficacité d'une campagne.

Les applications sont nombreuses dans le domaine scientifique : géologie, météorologie, par l'intermédiaire de capteurs pour surveiller et prévoir le déclenchement de phénomènes naturels. De la même manière on retrouve des applications dans des domaines d'intérêts publics comme l'aide au diagnostic médical ou la veille sanitaire.

De grandes sociétés informatiques développent aussi des projets pour accompagner des villes avec la promesse de les rendre plus « intelligentes », en adaptant les ressources aux besoins au moyen d'algorithmes de prévision de trafic par exemple. Dans le domaine de la sécurité publique, il s'agit d'agréger et d'analyser un ensemble de données dans le but de détecter les comportements « anormaux » et d'anticiper les menaces criminelles.

À une période où le coût d'accès à des ressources sur le cloud ne cesse de baisser, les technologies du Big Data s'étendent à de nombreux secteurs de l'économie, fort consommateurs de données, et sont principalement mobilisées pour leurs vertus prédictives.

[1] McKinsey 2011 / [2] Cf. gros plan du chapitre 1 La place des photos dans la vie numérique / [3] Étude IDATE Cloud et Big Data, mai 2012 / [4] On parle de RTB Real Time Bidding pour décrire les enchères en temps réel offertes aux annonceurs, et rendues possibles par la vélocité des systèmes de traitement.

TOUS GOUVERNÉS PAR DES ALGORITHMES ?

La « gouvernementalité algorithmique » est la thèse développée par certains chercheurs[5et6] pour lesquels ces systèmes de détection, de classification et d'évaluation anticipative des comportements structurent *a priori* le champ d'action possible des individus. L'extrême diversité des données susceptibles d'être analysées, la puissance de calcul permise par les technologies du Big Data, combinées aux capacités de stockage offertes par le cloud conduisent ainsi à s'interroger sur l'effectivité des principes « Informatique et Libertés » appliqués au Big Data. Qu'il s'agisse des principes de finalité, de pertinence des données, de loyauté de la collecte ou encore du concept même de donnée personnelle.

C'est la raison pour laquelle la Commission a souhaité engager une réflexion sur cette problématique, qui a d'ailleurs été le sujet d'une des tables rondes organisées dans le cadre de la journée d'études vie privée 2020.

TOUTES LES DONNÉES DEVIENNENT-ELLES IDENTIFIANTES ?

La démocratisation de l'accès à cette puissance de calcul autorise de telles potentialités de croisement et de recoupement de données (pour beaucoup cependant anonymes au départ) qu'elles ouvrent bien évidemment des possibilités infinies de profilage voire de ré-identification des personnes. L'eldorado du Big Data est constitué par ces informations qui ne sont pas nominatives a priori mais qui, grâce au volume de traces ou d'informations en réseaux combinées à d'autres sources, permettent de créer de nouvelles données directement ou indirectement nominatives[7]. En ce sens les technologies du Big Data questionnent l'effectivité des techniques d'anonymisation.

> Serons-nous tous calculés par le Big Data ?

[5] Antoinette Rouvroy et Thomas Berns, Le nouveau pouvoir statistique / [6] Cf. p.18-20 sur « La dictature des algorithmes : demain, tous calculés ? » dans le premier numéro des cahiers IP / [7] Les recherches de Latanya Sweeney, directrice du Data Privacy Lab à l'Université d'Harvard, ont montré que 87 % des américains pouvaient être identifiés à partir de la seule combinaison de 3 informations : le code postal, la date de naissance et le genre.

TOUTES LES DONNÉES DU CLOUD SONT-ELLES UTILISABLES ?

C'est un véritable sujet de débat parmi les chercheurs comme pour la CNIL qui s'interrogent sur le statut à accorder à ces informations considérées comme « publiques », parce qu'elles sont accessibles au travers des réseaux sociaux et donc facilement « agrégeables » avec les technologies du Big Data. Peuvent-elles être simplement utilisées, sans en demander la permission ? Des traitements et analyses peuvent-ils se faire à l'insu des personnes ?

L'analyse de micro-conversations peut par exemple permettre d'avoir des informations assez fines sur les orientations politiques d'un individu.

L'architecture en *cloud* pose également des questions sur la manière dont les données circulent, sur leur stockage et leur analyse en continu. Comment les sécuriser ? Est-il possible, souhaitable de limiter les recoupements, l'interconnexion et la centralisation de toutes ces données potentiellement sensibles ?

90 %
DES DONNÉES CRÉÉES L'ONT ÉTÉ CES 2 DERNIÈRES ANNÉES

FINALEMENT, TOUS PRÉVISIBLES ?

Toutes ces données sont *in fine* traitées par des algorithmes pour les transformer en informations capables de déduire ou de prédire des comportements. C'est d'ailleurs ce qui inquiète certains dans ce passage du déductif à un inductif purement statistique, une forme de nouvelle science sans hypothèse. Laisser ainsi des systèmes automatisés définir ce qui est suspect et ce qui ne l'est pas ne va pas sans poser des questions sérieuses sur un plan éthique.

En particulier, est-il acceptable de vouloir définir et détecter des comportements « anormaux » sur une logique statistique ?

Se pose également la question de la légitimité de la prise de décision sur la base d'un traitement automatique dont les individus ne connaissent pas la logique. Dans la mesure où ces algorithmes sont de véritables boîtes noires, comment les informer sur les conditions d'exploitation de données au départ anonymes et dont on ne connaît pas a priori l'usage qui en sera fait ? Comment assurer le respect de leurs droits ? Comment pourraient-ils contester la logique qui sous tend une décision prise sur la base d'un tel traitement ? Ou, à l'inverse les individus sont-ils susceptibles d'adopter certains comportements en anticipant des traitements de ce type ?

Au final, comment appliquer le principe de proportionnalité et de pertinence des données dans un contexte où il est de l'essence même du Big Data de recueillir toujours plus de données ?

Alors que les Big Data commencent à émerger en tant que champ de recherche et que ces technologies se diffusent à l'ensemble de l'économie, beaucoup de questions restent en suspens quant aux implications éthiques de leurs usages. L'intérêt pour ces questions a été appuyé par les experts rencontrés pour le premier numéro des Cahiers IP et lors de la journée d'études « vie privée 2020 ». Elles sont à l'ordre du jour du programme d'études de la CNIL en 2013. ■

Big Data : une nouvelle science sans hypothèse ?

VERS UN DROIT À L'OUBLI NUMÉRIQUE ?

Le droit à l'oubli numérique est la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie privée ou publique mise en ligne. Nécessité humaine et sociétale, ce droit ne doit, cependant, pas être interprété comme un impératif absolu d'effacement des données. Il est, en effet, nécessaire de trouver un équilibre entre le droit à l'oubli, d'une part et la nécessité de se ménager des preuves, le devoir de mémoire et la liberté d'expression, d'autre part.

LE DROIT À L'OUBLI SOUS L'ANGLE « INFORMATIQUE ET LIBERTÉS »

Le droit à l'oubli n'est pas en lui-même un concept juridique reconnu par le législateur, mais il résulte de l'application combinée de plusieurs principes issus de la loi « Informatique et Libertés » dans sa rédaction initiale comme dans celle résultant de la transposition de la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles, ainsi que dans la convention 108 du Conseil de l'Europe du 28 janvier 1981. Au-delà des principes de finalité, de loyauté, d'exactitude et de mise à jour des données, la Commission a ainsi toujours veillé à l'obligation de définir et de respecter des durées de conservation conformes à la finalité poursuivie et de prendre en compte les demandes de droit d'opposition en résultant.

La circulation d'informations personnelles concernant une personne peut en effet avoir de graves conséquences sur sa vie privée et professionnelle. Les plaintes adressées à la CNIL illustrent parfaitement ce risque d'atteinte à la vie privée des particuliers. **Celles liées aux problématiques de droit à l'oubli sur Internet (suppression de textes, photographies ou vidéos en ligne) sont en constante augmentation depuis plusieurs années.**

> Nécessité humaine et sociétale, le droit à l'oubli ne doit pas être interprété comme un impératif absolu d'effacement des données

LA NÉCESSITÉ DE SE DOTER DE SOLUTIONS JURIDIQUES ET TECHNIQUES INNOVANTES PERMETTANT D'ASSURER L'EFFECTIVITÉ DU DROIT À L'OUBLI

À la veille de l'adoption d'un nouveau règlement européen consacrant le droit à l'oubli, il est nécessaire de s'interroger collectivement sur l'effectivité réelle de ce droit à propos duquel s'exprime une demande sociale importante. Il s'agit d'examiner les solutions juridiques et techniques innovantes permettant d'assurer un meilleur respect de ce nouveau droit et offrant aux individus les moyens réels de maîtriser la diffusion de leurs données à caractère personnel.

Il serait par exemple possible d'offrir aux utilisateurs des fonctionnalités leur permettant de définir une date de « péremption » de leurs publications ou de gérer leurs propres publications en leur offrant directement la possibilité de les modifier ou de les supprimer.

Par ailleurs, l'effectivité du droit à l'oubli doit être complétée par une obligation juridique de déréférencement à la charge des moteurs de recherche. Ces derniers sont, en effet, devenus les principales clés d'entrée pour la recherche et la diffusion des données à caractère personnel sur Internet. Cette obligation s'avère utile, notamment, en cas de reproduction multiple d'une publication, en cas d'inaction du responsable de traitement initial (par exemple : l'éditeur du site internet) ou en cas d'impossibilité de contacter le responsable de traitement à la suite de son décès. Le droit au déréférencement, corollaire du droit à l'oubli, pourrait ainsi être consacré dans le règlement européen.

> Le droit au déréférencement, corollaire du droit à l'oubli, pourrait être consacré dans le règlement européen

La CNIL se félicite enfin que le projet de règlement prévoit un droit à la portabilité. Ce droit permet d'obtenir auprès du responsable du traitement une copie de ses données, dans un format électronique structuré couramment utilisé et permettant leur réutilisation. Le droit à la portabilité concourt donc au droit à l'oubli en autorisant les individus à récupérer leurs données et en leur évitant d'être captifs d'un service particulier.

Le développement des réseaux sociaux se manifeste, notamment, par une propension croissante des individus à exposer leur vie privée. Le caractère transnational du réseau Internet accentue la difficulté de maîtriser les informations publiées. Il apparaît alors essentiel que les autorités de protection des données, en concertation avec les professionnels, les acteurs de la société civile et les citoyens, agissent ensemble pour que le droit à l'oubli numérique puisse être effectif. ■

LA BIOMÉTRIE : UNE DOCTRINE PRAGMATIQUE ET ÉVOLUTIVE

Six ans après l'adoption des premières délibérations de la CNIL sur les dispositifs biométriques, la CNIL a constaté que l'évolution des technologies et des usages imposait une modernisation de sa doctrine en matière de biométrie.

UNE RÉFLEXION INSCRITE DANS LE PRINCIPE DE RÉALITÉ

À la suite de plus d'une dizaine d'auditions, notamment avec les syndicats de salariés ou patronaux, un consensus s'est clairement exprimé pour considérer comme disproportionnée l'utilisation de la biométrie aux fins de contrôle des horaires. Dès lors, en octobre 2012, la Commission a décidé de modifier l'AU-007 qui autorisait l'utilisation du contour de la main aux fins de gestion des horaires.

Fin 2012, la Commission a soulevé plusieurs questions de fond sur les usages de la biométrie pour accéder à des activités sportives ou de loisirs relevant de l'exercice d'une mission de service public. Au cours de ce travail, la Commission a constaté la nécessité d'approfondir sa réflexion.

En 2013, la CNIL souhaite mesurer l'impact de l'évolution des technologies biométriques et de leurs usages et favoriser une approche réaliste de nouveaux enjeux technologiques, économiques ou sociaux. La Commission a donc initié cette réflexion en auditionnant des experts du secteur, le 7 février 2013.

Ces experts représentaient la **communauté scientifique**, les **industriels du secteur** et la **société civile**.

Les discussions ont notamment porté sur :

- la relation entre le traitement de données biométriques (corporelles, irrévocables) et la protection du corps humain, sur la signification du critère de « proportionnalité »,
- un encadrement des finalités lors d'un stockage centralisé des empreintes digitales,
- la distinction des finalités de sécurité et de confort et sur la notion de « consentement préalable » des personnes concernées.

Aujourd'hui, la mise en œuvre de dispositifs biométriques à des fins de « souveraineté » (contrôle d'identité pour le compte de l'État) ne constitue plus qu'un des nombreux « marchés » de la biométrie. Les enjeux de cette technologie ne sont donc plus seulement sécuritaires mais deviennent également sociaux et ludiques (reconnaissance faciale en ligne par exemple). Dans ces conditions, la CNIL doit tenir compte d'un contexte économique et social en permanente évolution.

> La CNIL consulte la communauté scientifique, tient compte des propositions des fabricants et des représentants de la société civile

QUEL ENCADREMENT DE LA BIOMÉTRIE ?

Au-delà des aspects techniques et juridiques pris en considération par les délibérations de la CNIL, la Commission souhaite aujourd'hui s'interroger sur :

- **la perception par les utilisateurs de ces dispositifs biométriques** : entre, d'une part, le légitime besoin de sécurité ou l'utilité pratique et, d'autre part, le spectre de « Big brother » : quel est le ressenti réel de la société face à ces nouveaux instruments ?
- **le rôle de la CNIL face à l'essor de ces dispositifs** : la CNIL devrait-elle imposer une frontière claire entre les usages pertinents de la biométrie et ceux qui ne sont pas considérés comme acceptables car présentant trop de risques pour la vie privée eu égard à leur finalité ? Devrait-elle davantage développer une compétence pédagogique afin de sensibiliser chacun de nous aux risques relatifs à la vie privée, et nous permettre ainsi des choix plus éclairés ?
- **les instruments proposés par la CNIL à disposition des responsables de traitement** : la CNIL devrait-elle mettre à disposition des déclarants des outils leur permettant d'analyser la pertinence du dispositif biométrique envisagé au regard des critères de finalité, de proportionnalité, de sécurité et d'information des personnes en référence au modèle anglo-saxon et à la notion d'« *analyse d'impact relative à la protection des données* » (PIA en anglais) inscrite à l'article 33 du projet de règlement communautaire du 25 janvier 2012 ?
- modèles de supports d'information à diffuser auprès de tout éventuel client ?

La CNIL envisage de moderniser ses instruments d'aide à la décision sur l'usage des solutions biométriques, afin qu'ils soient utiles et fonctionnels pour l'ensemble des responsables de traitement, des utilisateurs et des industriels du secteur. ■

ANNEXES

LES MEMBRES DE LA CNIL

LE BUREAU

Présidente

Isabelle FALQUE-PIERROTIN, conseiller d'État
Membre de la CNIL depuis 2004 et vice-présidente de 2009 à 2011, Isabelle Falque-Pierrotin est élue présidente de la CNIL le 21 septembre 2011.

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

Jean-Paul AMOUDRY, sénateur de la Haute-Savoie
Secteur : Banques et crédit
Jean-Paul Amoudry est membre de la CNIL depuis janvier 2009, et vice-président depuis octobre 2011.

LES MEMBRES (COMMISSAIRES)

Jean-François CARREZ, président de chambre honoraire à la Cour des comptes
Secteur : Transports, élections
Jean-François Carrez est membre de la CNIL depuis janvier 2009.
Il est membre élu de la formation restreinte.

Dominique CASTERA, membre du Conseil économique, social et environnemental
Secteurs : 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 vice-président de la formation restreinte.

Claire DAVAL, avocate
Secteur : Justice
Claire Daval est membre de la CNIL depuis janvier 2009.
Elle a été élue Présidente de la formation restreinte.

Claude DOMEIZEL,
sénateur des Alpes-de-Haute-Provence
Secteur : Développement durable, énergie et logement
Claude Domeizel est membre de la CNIL depuis décembre 2008.
Il est membre élu de la formation restreinte.

Laurence DUMONT,
députée du Calvados
Secteur : Questions sociales et fiscales
Laurence Dumont est membre de la CNIL depuis octobre 2012.

Didier GASSE, conseiller maître honoraire à la Cour des comptes
Secteurs : Télécommunications et internet – sécurité – vote électronique
Didier Gasse est membre de la CNIL depuis janvier 1999.

Gaëtan GORCE, sénateur de la Nièvre
Secteur : Libertés publiques et e-administration
Gaëtan Gorce est membre de la CNIL depuis décembre 2011.

Sébastien HUYGHE, député du Nord
Secteur : Identité, défense et affaires étrangères
Sébastien Huyghe est membre de la CNIL depuis juillet 2007.

Jean MASSOT, président de section honoraire au Conseil d'État
Secteurs : Santé et assurance maladie – archives et données publiques
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. Elle est membre élue de la formation restreinte.

Éric PERES, membre du Conseil économique, social et environnemental
Secteur : Éducation et enseignement supérieur
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
Secteurs : Affaires culturelles et sportives – vidéoprotection
Dominique Richard est membre de la CNIL depuis janvier 2009.
Il est membre élu de la formation restreinte.

Commissaires du gouvernement

Jean-Alexandre SILVY
Catherine POZZO DI BORGO, adjointe

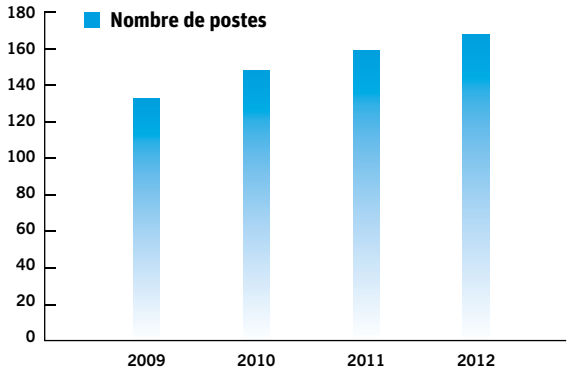
LES MOYENS DE LA CNIL

LE PERSONNEL

Afin de faire face à l'augmentation soutenue de ses missions traditionnelles ainsi qu'à l'extension de son périmètre d'intervention par l'entrée en vigueur de nouveaux textes législatifs, la CNIL connaît une croissance continue et significative de ses moyens humains.

Ainsi, en 2012, elle a été dotée de 12 postes supplémentaires, passant ainsi de 159 postes à 171, soit une augmentation de 7,5 % de ses effectifs.

Ces nouveaux emplois ont permis notamment le renforcement des moyens humains en matière d'expertise informatique et d'investigation



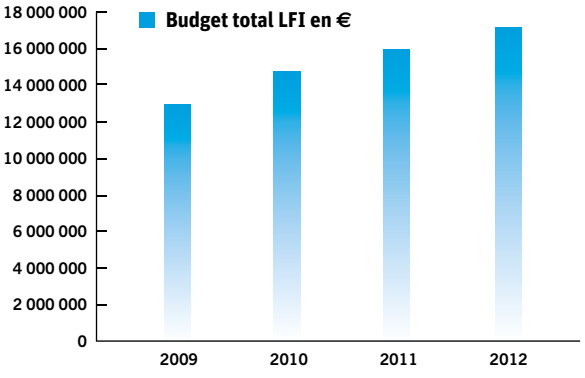
La croissance soutenue de l'activité des services de la Commission, tant dans ses missions premières de conseil, d'examen des formalités préalables obligatoires (demandes d'avis et d'autorisation), d'instruction des plaintes, de contrôles, de sanctions et d'animation du réseau des CIL, que dans les dernières confiées par le législateur (contrôle de la vidéoprotection - loi n°2011-267 du 14 mars 2011 dite LOPPSI 2 et enregistrement des notifications des failles de sécurité -, loi n°2011-302 du 22 mars 2011) conduit à maintenir cette phase de croissance des effectifs a minima tout au long du triennal 2013-2015. 7 créations de postes ont de ce fait été actées pour chacune des trois prochaines années.

LES CRÉDITS

En 2012, la CNIL a été dotée d'un budget total de 17,2 millions d'euros répartis à hauteur de 11,3 millions pour le personnel et 5,9 millions d'euros pour le fonctionnement. Le budget alloué au personnel croît ainsi d'un million d'euros entre 2011 et 2012. Cette augmentation de 10 % du budget est inhérente à l'accroissement du nombre de postes ouverts à la CNIL.

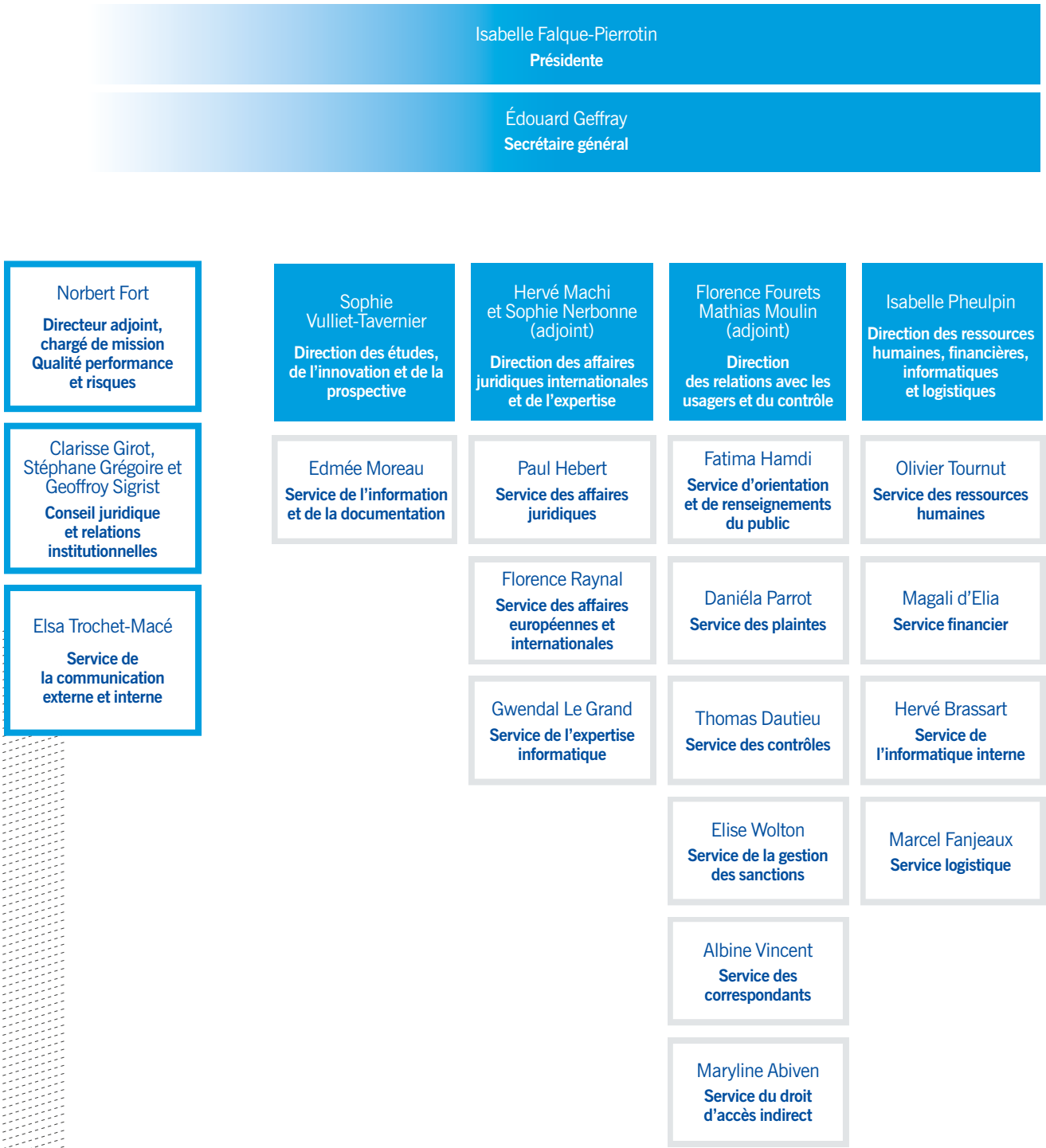
Le budget de fonctionnement augmente également mais dans une moindre mesure (+180 000 euros par rapport à 2011).

Dans ce contexte de maîtrise actuelle des finances publiques, le budget de fonctionnement fait donc l'objet d'une utilisation contrôlée et d'une optimisation des fonds mis à disposition. Les dépenses de fonctionnement courant sont donc particulièrement surveillées et maximisées afin de pourvoir à l'équipement des postes de travail des nouveaux arrivants sans augmenter significativement les budgets alloués par famille



d'achats. Dans cette optique, la CNIL recourt depuis 2012 à des dispositifs d'achats mutualisés, notamment les marchés passés par le Service d'Achats de l'État, en vue de réaliser des économies structurelles sur des dépenses de fonctionnement courant obligatoires telles que les fournitures de bureau, la papeterie, les achats de documentations ou d'abonnements. ■

ORGANIGRAMME DES DIRECTIONS ET SERVICES



LISTE DES ORGANISMES CONTRÔLÉS EN 2012

ASSURANCE

APRIL PARTENAIRES
MAIF
MUTEX

BANQUE

BANQUE TRAVELEX SA
CRCAM DES SAVOIE CREDIT AGRICOLE DES SAVOIE

COLLECTIVITES LOCALES

COMMUNAUTE D'AGGLOMERATION DE RENNES
COMMUNE DE CHELLES
COMMUNE DE CHOISY-LE-ROI
COMMUNAUTE DE COMMUNES DE RUFFEC
COMMUNE DE PARIS
COMMUNE DE RENNES
COMMUNE DE VILLERS-SUR-MER
CONSEIL GENERAL DE LA CHARENTE MARITIME
CONSEIL GENERAL DU VAL D'OISE
SERVICE DEPARTEMENTAL D'INCENDIE ET DE SECOURS DES BOUCHES DU RHONE

COMMERCE

ADIDAS CHAMPS ELYSEES
AMAZON.FR
APPLE FRANCE
ARNELLL
AUCHAN E-COMMERCE FRANCE
AUCHAN LA DEFENSE
BOULANGER
BOURSE IMMOBILIERE
BOUYGUES TELECOM
CANAL + FRANCE
CASINO CANNES BALNEAIRE PALM BEACH
CASINO DE PANTIN
CASINO DE TROUVILLE
CARREFOUR MARKET VERSAILLES
CASH CONVERTERS
CEE DIRECTE
CELIO FRANCE VINCENNES
CENTRE DE RESSOURCES INTERACTIF
CHAUSPORT REIMS
CHRISTIE'S FRANCE SAS
COGEMEX
COMMUNICATION DIRECTE EXTERNALISEE DE L'ENTREPRISE (C.DIRECTE)
CORA MONDELANGE
CORA
COURIR FRANCE
CRITEO
DALKIA FRANCE
DECATHLON MONTREUIL SOUS BOIS
DECATHLON SAINT DENIS
DIA NANTERRE
DROUOT MONTMARTRE HOLDING
EBSCO
EDF
EGEYS
EMAILVISION
EMB SERVICE
EOREZO
ERDF
ETAM CRETEIL
EURODIF
EURO PACTE
FIA-NET
FNAC DIRECT
FONEX
FRANCE TELECOM
FRANPRIX NEULLY SUR SEINE
GAP
GALERIES LAFAYETTE LILLE
GALERIES LAFAYETTE REIMS
GDF-SUEZ
GFK RETAIL AND TECHNOLOGY FRANCE
GO SPORT
GOOGLE Inc.
GRDF
GROUPE CONCOURSMANIA
GROUPE D.S.E. FRANCE
GUCCI FRANCE
HEMA FRANCE EVRY
HITEX
INTERMARCHE COMPIEGNE
INTRINSEC
JDC

▸▸▸

▸▸▸

JENNYFER CRETEIL
JIVE SQUAD
JUST AROUND US
LA FRANCAISE DES EAUX
LA HUTTE FRANCE SPORT REIMS
LEADER PRICE NANTERRE
LE FURET DU NORD
LEROY MERLIN
LIDL EVRY
LYONNAISE DES EAUX FRANCE
OBJECTIF TERRAIN
OMER TELECOM LIMITED
OPINION-WAY
PANDIS DISTRIBUTION PANTIN
PAYBOX SERVICES
P COMME PERFORMANCE
P2H INVESTISSEMENT
PIXMANIA
POWEO
PRISMA PRESSE
MARIONNAUD PARFUMERIE
MESSAGE BUSINESS
MEUBLES IKEA FRANCE SNC
MOBEO
MONOPRIX CONVENTION
MONOPRIX ROUEN
MONOPRIX TERNES
NANTAISE DES EAUX SERVICES
NOVEX
RUE DU COMMERCE
SHALISO
SENSEE
S.F.I.G.
SIMONPLAST
SMART & CO
SOCIETE FRANCAISE DE RADIOTELEPHONE (SFR)
SOGETI FRANCE
SOCIETE DE PROTECTION ELECTRONIQUE ET MECANIQUE
SOTHEBY'S FRANCE
SWATCH STORE
TMB
TRIDENT MEDIA GUARD
TOTAL RAFFINAGE MARKETING
TRAVELEX PARIS SAS
TUTO4PC.COM
UNITEAD
VEOLIA EAU – COMPAGNIE GENERALE DES EAUX
VERSAILLES VOYAGES
VENTE-PRIVEE.COM
VIA2S
ZONG SAS

CULTURE

CENTRE NATIONAL D'ART ET DE CULTURE GEORGES POMPIDOU
OPERA NATIONAL DE PARIS
THEATRE DU CAVEAU DE LA REPUBLIQUE

EDUCATION

CENTRE REGIONAL DE DOCUMENTATION PEDAGOGIQUE
COLLEGE HENRI BARBUSSE
COLLEGE GEORGES CLEMENCEAU
LYCEE HENRI IV
LYCEE MARCELIN BERTHELOT

IMMOBILIER

AGENCE NATIONALE POUR LA RENOVATION URBAINE (ANRU)
EIFFAGE IMMOBILIER ATLANTIQUE
FRANCE HABITATION
GREEN POINT (BE PREM'S)
IMMOBILIERE 3 F
OFFICE PUBLIC DE L'HABITAT DU TERRITOIRE DE BELFORT
OPH-PARIS HABITAT

POLICE - JUSTICE

AGENCE NATIONALE DES TITRES SECURISES (ANTS)
CONSEIL NATIONAL DES ACTIVITES PRIVEES DE SECURITE (CNAPS)

MINISTERE DE L'INTERIEUR :

EURODAC
CIRCONSCRIPTION DE SECURITE PUBLIQUE DE COMPIEGNE
CIRCONSCRIPTION DE SECURITE PUBLIQUE DE STRASBOURG
DIRECTION DEPARTEMENTALE DE LA SECURITE PUBLIQUE DE LYON
SERVICE CENTRAL DE DOCUMENTATION CRIMINELLE
PREFECTURE DU BAS–RHIN
PREFECTURE DE GIRONDE
PREFECTURE DE L'OISE
PREFECTURE DU RHONE
PREFET DELEGUE CHARGE DE LA SECURITE ET DE LA SURETE DES PLATEFORMES AEROPORTUAIRES DE ROISSY ET DU BOURGET
SERVICE DEPARTEMENTAL D'INFORMATION GENERALE DE BORDEAUX

MINISTERE DE LA JUSTICE :

MAISON D'ARRET DE CHALONS-EN-CHAMPAGNE
TRIBUNAL DE GRANDE INSTANCE DE BOBIGNY
TRIBUNAL DE GRANDE INSTANCE DE BORDEAUX
TRIBUNAL DE GRANDE INSTANCE DE LYON
TRIBUNAL DE GRANDE INSTANCE DE SENLIS
TRIBUNAL DE GRANDE INSTANCE DE STRASBOURG

MINISTERE DES AFFAIRES ETRANGERES :
MISSION POUR LA POLITIQUE DES VISAS
DIRECTION DES SYSTEMES D'INFORMATION
CONSULAT GENERAL DE FRANCE D'ISTANBUL
CONSULAT GENERAL DE FRANCE DE LONDRES
CONSULAT GENERAL DE FRANCE DE MOSCOU

SANTE - SOCIAL

AIMSU
AMBULANCE LA MALOUINE
AMEDIM
BEBE VIEW
BIOSYNERGIE
CAISSE NATIONALE D'ALLOCATIONS FAMILIALES
CAISSE PRIMAIRE D'ASSURANCE MALADIE DE TOULOUSE
CENTRE COMMUNAL D'ACTION SOCIALE DE RENNES
CENTRE HOSPITALIER COCHIN (CECOS)
CENTRE MEDICO CHIRURGICAL DE READAPTATION DES MASSUES
CEGEDIM
CLINIQUE GERIATRIQUE CHATEAU GOMBERT
CONSEIL GENERAL DE L'HERAULT
ECHOGRAFILM
FONDATION DES APPRENTIS D'AUTEUIL
FONDATION HOSPITALIERE SAINTE-MARIE
FRANCE TELECOM – ORANGE BUSINESS SERVICES
GRANDE PHARMACIE BAILLY
GRANDE PHARMACIE BROCHANT
GROUPE HOSPITALIER JEAN-VERDIER (CECOS)
HOPITAL PRIVE GERIATRIQUE LES MAGNOLIAS
HOSPICES CIVILS DE LYON
I-DISPO
INSERM
LABORATOIRE ALPHA
LABORATOIRE BEAUHAIRE ET BIENVENU
LABORATOIRE CENTRAL 92
LABORATOIRE DUBREUIL
LABORATOIRE DU VAL-AKNOUCHE
LABORATOIRE GENDRAULT-TALLOBRE MANCY
LA PHARMACIE BLEUE
LINK CARE SERVICES
MAISON D'ENFANTS A CARACTERE SOCIAL MAISON JEAN XXIII
MEGABUS INTERNATIONAL
NCS NORD DE FRANCE
OVH
PHARMACIE ALIMI SOFIYAT
PHARMACIE COULAND REGINE ISABELLE
PHARMACIE D'ALBRET
PHARMACIE DE LA REPUBLIQUE
PHARMACIE DE L'HOTEL DE VILLE ET DE ST ANDRE
PHARMACIE DES GRANDS HOMMES
PHARMACIE DU CHATEAU
PHARMACIE DU FOUR-BONAPARTE
PHARMACIE EDGAR QUINET
PHARMACIE MONTPARNASSE
REGISTRE FINISTERIEN DES TUMEURS DIGESTIVES
REGIME SOCIAL INDEPENDANTS AQUITAINE
RESEAU DE CANCEROLOGIE ONCOBOURGOGNE
RESIDENCE LA GUILBOURDERIE
SEDAD
SIAO 67
S.M.A.I.O

SECURITE PRIVEE – RECOUVREMENT DE CREANCES

ASSISTANCE RISQUE CLIENT (ARCA CONSEIL)
BUREAU EUROPEEN D'INFORMATIONS COMMERCIALES –BEIC
CRISTAL RISK MANAGEMENT
GENERALE D'EDITION ELECTRONIQUE
MES CONSEILS
OFFICE JURIDIQUE NATIONAL DE RECOUVREMENT (OJNR)

SPORT

CONSORTIUM STADE DE FRANCE
FEDERATION FRANCAISE D'ATHLETISME
FEDERATION FRANCAISE DE FOOTBALL
FEDERATION FRANCAISE DE TENNIS
FEDERATION FRANCAISE DE WUSHU ARTS ENERGETIQUES ET MARTIAUX CHINOIS
GOLF INTERNATIONAL DE GRENOBLE
LIGUE DE FOOTBALL PROFESSIONNEL
LIGUE REGIONALE DE TIR DE LA COTE D'AZUR
PARIS SAINT-GERMAIN FOOTBALL
PISCINE SAINT-CHARLES

TRAVAIL - RECRUTEMENT

AFPA RENNES
PROFESSIONAL SERVICE CONSULTING
ROLESCO
START PEOPLE

TRANSPORT

KEOLIS BORDEAUX
SANEF
SOCIETE DES AUTOROUTES ESTEREL, COTE D'AZUR, PROVENCE, ALPES (ESCOTA)
VEOLIA TRANSPORT MONT-SAINT-MICHEL
VINCI PARK

LISTE DES ORGANISMES CONTRÔLÉS EN 2012 DISPOSITIFS DE VIDÉOPROTECTION/VIDÉOSURVEILLANCE

ASSOCIATION

AUTOMOBILE CLUB DE FRANCE

BANQUE

BANQUE DE FRANCE
BARCLAYS BANK
CAISSE REGIONALE DE CREDIT AGRICOLE MUTUEL DE NORMANDIE
CREDIT MUTUEL BRESSAN
SOCIETE GENERALE

COLLECTIVITES LOCALES

COMMUNAUTE URBAINE DE STRASBOURG
COMMUNE D'ALLONNE
COMMUNE D'ARGENTEUIL
COMMUNE DE BRY-SUR-MARNE
COMMUNE DE CAGNES-SUR-MER
COMMUNE DE CHELLES
COMMUNE DE LYON
COMMUNE DE MORANCE
COMMUNE DE NOGENT-SUR-MARNE
COMMUNE DE PANTIN
COMMUNE DE ROUEN
COMMUNE DE SAINT-GERMAIN-EN-LAYE
COMMUNE DE SAINT-MANDE
COMMUNE DE TOULOUSE
COMMUNE DE VILLENEUVE-LA-GARENNE

COMMERCE

ALKERN NORD
ANASUN
AOCT
BATI DOLE
BIJOUTERIE LEPAGE
BOUCHERON
MAGASINS BOULANGER
BOUTIQUE BODY'MINUTE
CABINET DOUCET-KORHEL
CARLTON'S HOTEL
CENTRES E. LECLERC
CHOCOLATERIE DE BEUSSENT LACHELLE
DALLOYAU
GARAGE BOURBON GENLIS
GENTILE MOTO SPORT
GRANDE PHARMACIE DU MARCHE
GROUPE MARIE-CLAIRE
GUESS
HANDINAMYC
HERMINE DE PASHMINA
HOTEL BRIGHTON
HOTEL CRILLON
HOTEL DE FRANCE
HOTEL FROCHOT
HOTEL GALANT
HOTEL IBIS GRENOBLE GARE
HOTEL LE BRISTOL
HOTEL MERCURE
HOTEL MERCURE PARIS AUSTERLITZ
HOTEL PELETIER OPERA
HOTELS & SPA SAINT-JAMES & ALBANY
INCOGNITO
INSTITUT KARITE
MAGASINS INTERSPORT
JLC OPTICIEN LUNETIER
KEEP COOL
LA FERME DU LAC
LA MODE EST A VOUS
AGENCES LA POSTE
LE MATELY'S
LE PANETON
M'SPORTS
MADE IN V
MAN DIESEL SAS
MAGASINS CARREFOUR
MAGASINS CONFORAMA
MAGASINS DARTY
MAGASINS DECATHLON
MAGASINS GO SPORT
MAGASINS FNAC
MAGASINS JULES
MAGASINS KIABI
MAGASINS LA CHAISE LONGUE
MAGASINS YVES ROCHER
MAP
MARQUES VICTOR
MAUBOUSSIN
MONTRES SUISSES SA
NCT - NOUVELLE COMMUNICATION TELEPHONIQUE
NETTO
NOVOTEL
OPTIQUE CALAS
ORGAPHARM

PATHE GRENOBLE-CHAVANT
PEAU D'ANE
PHARMACIE DE LA GARE
PHARMACIE DU HOHBERG
PHARMACIE HASSAN
PLESSIS GRAND HOTEL
PROLIVAL
PROMOCASH
PRONUPTIA
PROVIDIS LOGISTIQUE SA
RESTAURANTS MC DONALD'S
RESTAURANTS SUBWAY
ROGER CDB
SALMA STORE
SEPHORA
SERGE BLANCO
STARBUCKS COFFEE
SOCIETE D'EXPLOITATION DE LA TOUR EIFFEL
SOCIETE D'AMENAGEMENT TOURISTIQUE ET D'EXPLOITATION LA CLUSAZ (SATELC)
SOCIETE COMMERCIALE DES HOTELS ECONOMIQUES
SOCIETE HOTELIERE MANAGEMENT
SOGIDUN
SUPERMARCHES FRANPRIX
TABAC LE PRESSE BOOK
TABAC LOTO BERTHO
TABAC MERLICO
UGC CINE CITE
UGC GEORGE V
VCASH
VAN CLEEF ET ARPELS

CULTURE

LA MAISON DU LIMOUSIN
MUSEE D'ANGOULEME
MUSEE DE LA MARINE
MUSEE DES ABATTOIRS DE TOULOUSE
MUSEE DES BEAUX ARTS DE DIJON
MUSEE DU LOUVRE
MUSEE JULES VERNE DE NANTES
MUSEE MUNICIPAL D'ORANGE
MUSEE NATIONAL DE LA VOITURE ET DU TOURISME DE COMPIEGNE
THEATRE DU NORD-EST DE THIONVILLE

EDUCATION

ASSSOCIATION DE GESTION « LA DOCTRINE CHRETIENNE »
ECOLE ELEMENTAIRE SERMET
ENSEN (ECOLE SUP. DE L'EDUCATION NATIONALE)

IMMOBILIER

CITYA SAINT-HONORE CANNES
SYNDICAT DES COPROPRIETAIRES ARCADES DES CHAMPS-ELYSEES

POLICE - JUSTICE

DIRECTION DEPARTEMENTALE DES FINANCES PUBLIQUES DES HAUTS DE SEINE
PREFECTURE DE POLICE DE PARIS

SANTE/SOCIAL

CENTRE CARDIOLOGIQUE DU NORD
CLINIQUE LA PERGOLA
EHPAD ORPEA
HOPITAL EUROPEEN DE PARIS GVM CARE & RESEARCH
RESIDENCE ORPEA « LES MARINIERS »

SPORT

FITNESS PARK
PISCINE LEO LAGRANGE (TOULOUSE)

TRANSPORT

RATP
VEOLIA TRANSPORT

▸▸▸

LEXIQUE

AFAPDP
L'Association francophone des autorités de protection des données personnelles (AFAPDP) a été créée en 2007, à Montréal, à l'initiative d'une trentaine de représentants d'autorités de contrôle et représentants d'États francophones.
Elle a pour objectif de :
• **Promouvoir le droit à la protection des données personnelles**, dans les États non encore dotés d'une législation (la majorité des États dans le monde), et également au niveau international (pour encourager l'établissement d'un instrument juridique international contraignant) ;
• **Développer et valoriser l'expertise francophone** en matière de protection des données personnelles.

ACCOUNTABILITY
L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

BCR
BCRs signifie « Binding Corporates Rules » ou règles d'entreprise contraignantes. Ces règles internes applicables à l'ensemble des entités du groupe contiennent les principes clés permettant d'encadrer les transferts de données personnelles, de salariés ou de clients et prospects, hors de l'Union européenne.
Ces BCRs sont une alternative au Safe Harbor (qui ne vise que les transferts vers les États-Unis) ou aux Clauses Contractuelles Types adoptées par la Commission européenne.
Elles garantissent qu'une protection équivalente à celle octroyée par la directive européenne de 1995 s'applique aux données personnelles transférées hors de l'Union européenne.

Big data
On parle depuis quelques années du phénomène de « Big Data », que l'on traduit souvent par « données massives ». Avec le développement des nouvelles technologies, d'internet et des réseaux sociaux ces vingt dernières années, la production de données numériques a été de plus en plus nombreuse : textes, photos, vidéos, etc. Le gigantesque volume de données numériques produites combiné aux capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiquées offre aujourd'hui des possibilités inégalées d'exploitation des informations.

Biométrie
La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.
Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales…).

Bring your own device (BYOD)
Pratique qui consiste à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel

CASSIOPEE (Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants)
Le traitement CASSIOPEE, mis en œuvre dans les tribunaux de grande instance, permet l'enregistrement d'informations relatives aux plaintes et dénonciations reçues par les magistrats, dans le cadre de procédures judiciaires, afin d'améliorer le délai de traitement des procédures, et d'assurer l'information des victimes.

Cloud Computing
Le Cloud Computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (Cloud) composé de nombreux serveurs distants interconnectés.

CNIL
Autorité administrative indépendante, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers, 4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1), par le Président du Sénat (1), par le conseil des ministres (3). Le mandat de ses membres est de 5 ans.

Conférence mondiale des Commissaires à la protection des données et à la vie privée
Cette conférence se tient chaque année à l'automne. Elle réunit l'ensemble des 81 autorités et commissaires à la protection des données et à la vie privée de tous les continents. Elle est ouverte aux intervenants et participants du monde économique, des autorités publiques, et de la société civile. Une partie de la Conférence est réservée aux représentants des autorités accréditées par la Conférence, durant laquelle sont adoptées les résolutions et déclarations.

Correspondant « Informatique et Libertés »
La principale mission du correspondant est de s'assurer que l'organisme qui l'a désigné auprès de la CNIL, respecte bien les obligations issues de la loi Informatique et Libertés. Il a un rôle de conseil et de diffusion de la culture Informatique et Libertés auprès de ses collaborateurs, supérieurs hiérarchiques et collègues. À ce titre, le correspondant

est devenu l'acteur incontournable pour toute entité soucieuse de sa responsabilité sociale, de ses valeurs et respectueuse des droits et libertés des usagers, clients et salariés.

Donnée personnelle
Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale…).

Donnée sensible
Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Droit à l'oubli numérique
Le droit à l'oubli numérique est la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie privée ou publique mise en ligne. Nécessité humaine et sociétale, ce droit ne doit, cependant, pas être interprété comme un impératif absolu d'effacement des données. Il est, en effet, nécessaire de trouver un équilibre entre le droit à l'oubli, d'une part et la nécessité de se ménager des preuves, le devoir de mémoire et la liberté d'expression, d'autre part.

Droit d'accès direct
Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'accès indirect
Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.

Droit d'opposition
Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

Droit de rectification
Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

FICOBA (Fichier national des comptes bancaires et assimilés)
FICOBA sert à recenser les comptes de toute nature (bancaires, postaux, d'épargne…), et à fournir aux personnes habilitées des informations sur les comptes détenus par une personne ou une société.

Formation restreinte
Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi « Informatique et Libertés », la CNIL siège dans une formation spécifique, composée de six membres appelée « formation restreinte ». À l'issue d'une procédure contradictoire, cette formation peut notamment décider de prononcer des sanctions pécuniaires pouvant atteindre 300 000 euros.

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 rassemblant les représentants de chaque autorité indépendante de protection des données nationale. Cette organisation réunissant l'ensemble des CNIL européennes 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 G 29 se réunit à Bruxelles en séance plénière tous les deux mois environ.

IaaS / PaaS
IaaS (« Infrastructure as a Service ») désigne la fourniture d'infrastructures de calcul et de stockage en ligne.
PaaS (« Platform as a Service ») désigne la fourniture d'une plateforme de développement d'applications en ligne

NIR
Le Numéro d'Inscription au Répertoire ou numéro de sécurité sociale est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.

Open data
L'Open data désigne un mouvement, né en Grande-Bretagne et aux États-Unis, d'ouverture et de mise à disposition des données produites et collectées par les services publics (administrations, collectivités locales…).

PNR (« Passenger Name Record »)
Il s'agit des informations collectées auprès des passagers aériens au stade de la réservation commerciale. Elles permettent d'identifier, entre autres : l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que des préférences alimentaires spécifiques (végétarien, asiatique, cascher, etc.) ou des services liés à l'état de santé du passager. Des informations du

▸▸▸

▸▸▸

type « tarif pèlerin » « missionnaire » « clergé » telles qu'elles figurent dans les champs « libres » des rubriques « remarques générales ». Ces données étant susceptibles de faire apparaître indirectement une origine raciale ou ethnique supposée, des convictions religieuses ou philosophiques, ou l'état de santé des personnes, sont considérées par la directive européenne comme des données sensibles, à exclure ou à protéger.

Quantified self

Le Quantified Self désigne la pratique de la « mesure de soi » et fait référence à un mouvement né en Californie qui consiste à mieux se connaître en mesurant des données relatives à son corps et à ses activités

RFID (Radio Frequency Identification)

Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micro-puce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution, leur coût est d'environ 5 centimes d'euros.
D'autres puces communicantes, plus intelligentes ou plus petites font leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi-invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm^2, possèdent une capacité de stockage de 512 Ko (kilo octets) et échangent des données à 10 Mbps.(méga bits par seconde).

Séance plénière

C'est la formation qui réunit les 17 membres de la CNIL pour se prononcer sur des traitements ou des fichiers et examiner des projets de loi ou de décrets soumis pour avis par le Gouvernement.

SIS (Système d'information Schengen)

Le système d'information Schengen (SIS) est composé d'une base centrale située à Strasbourg et, dans chaque pays participant à l'espace Schengen, de bases nationales. Les informations concernent essentiellement des personnes :
- recherchées pour arrestation aux fins d'extradition ;
- étrangères, signalées aux fins de non-admission dans l'espace Schengen à la suite d'une décision administrative ou judiciaire ;
- signalées aux fins de surveillance discrète ou de contrôle spécifique.

Smart Grids

Le compteur communicant est une des composantes des réseaux de distribution d'énergie intelligents (également désignés sous les termes anglais de « smart grids »). Ces réseaux utilisent des moyens informatiques évolués afin d'optimiser la production et l'acheminement de l'électricité, notamment grâce à la télétransmission d'informations relatives à la consommation des personnes. Cette télétransmission aura notamment pour conséquence de supprimer la relève physique des compteurs.

STIC (Système de traitement des infractions constatées)

Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées. Il facilite la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il permet également d'élaborer des statistiques.

Traitement de données

Collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation de fichiers ou bases de données, notamment des interconnexions.

Transfert de données

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Vidéoprotection

Les dispositifs dits « de vidéoprotection » filment la voie publique et les lieux ouverts au public sont soumis aux dispositions du code de la sécurité intérieure

Vidéosurveillance

Les dispositifs dits de « vidéosurveillance » concernent des lieux non ouverts au public (locaux professionnels non ouverts au public comme les bureaux ou les réserves des magasins) sont soumis aux dispositions de la loi « Informatique et Libertés ».

Violation de données à caractère personnel

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

Commission nationale de l'informatique et des libertés
8, rue Vivienne - 75083 Paris Cedex 02 / www.cnil.fr / Tél. 01 53 73 22 22 / Fax 01 53 73 22 00

Conception & réalisation graphique EFIL 02 47 47 03 20 / www.efil.fr
Impression La documentation Française / Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr, imprimé en France
Crédit photo Fotolia, istockphoto / **Diffusion** Direction de l'information légale et administrative

Commission nationale de l'informatique et des libertés
8, rue Vivienne
75083 Paris Cedex 02
Tél. 01 53 73 22 22
Fax 01 53 73 22 00

www.cnil.fr

Diffusion
Direction de l'information légale et administrative

La Documentation française
Tél. 01 40 15 70 10
www.ladocumentationfrançaise.fr

ISBN : 978-2-11-009349-3
DF : 5 HC33610
Prix : 15 €

CNIL
Commission Nationale de l'Informatique et des Libertés