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

2078
DÉCISIONS ET DÉLIBÉRATIONS ADOPTÉES
(+ 5,5% par rapport à 2011)

316
AUTORISATIONS, DONT 3 AUTORISATIONS UNIQUES

113
AVIS

3
DISPENSES

2
RECOMMANDATIONS PORTANT SUR LA COMMUNICATION POLITIQUE ET LES COMPTEURS COMMUNICANTS

MISES EN DEMEURE ET SANCTIONS

43
MISES EN DEMEURE

4
SANCTIONS FINANCIÈRES

9
AVERTISSEMENTS

2
RELAXES

PLAINTES ET DEMANDES DE DROIT D'ACCÈS INDIRECT

6017
PLAINTES
(+ 4,9 % par rapport à 2011)

3682
DEMANDES DE DROIT D'ACCÈS INDIRECT
(+ 75 % par rapport à 2011)

INTERVENTIONS EXTÉRIEURES

160
INTERVENTIONS

FORMALITÉS PRÉALABLES

8946
DÉCLARATIONS RELATIVES À DES SYSTÈMES DE VIDÉOSURVEILLANCE
(+49,3 % par rapport à 2011)

5483
DÉCLARATIONS RELATIVES À DES DISPOSITIFS DE GÉOLOCALISATION
(+ 22,3 % par rapport à 2011)

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

CONTRÔLES

458
CONTRÔLES
(+19 % par rapport à 2011)

173
CONTRÔLES VIDÉOPROTECTION

CORRESPONDANTS

10709
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.

▸▸▸

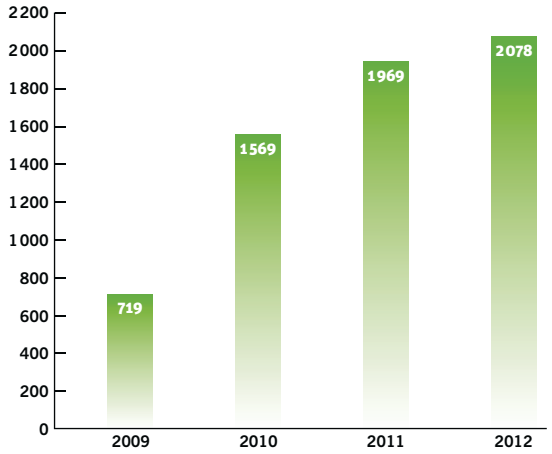
Accompagnement, ensuite, des acteurs publics ou privés : l'enjeu n'est pas seulement, en effet, d'effectuer telle ou telle formalité auprès de la Commission. L'enjeu est bien, pour les responsables de traitements, de s'assurer de la conformité permanente de leurs traitements aux exigences légales et 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

L'éducation numérique :
une priorité pour la CNIL

Les réponses au public

GROS PLAN
La place des photos et vidéos dans la vie numérique

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.).

LE SITE INTERNET WWW.CNIL.FR

41 860
ABONNÉS À LA LETTRE INFOCNIL

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.

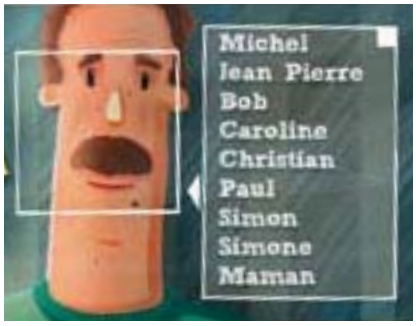
> Les technologies de reconnaissance faciale pourraient transformer la photo en nouvel identifiant numérique

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

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.

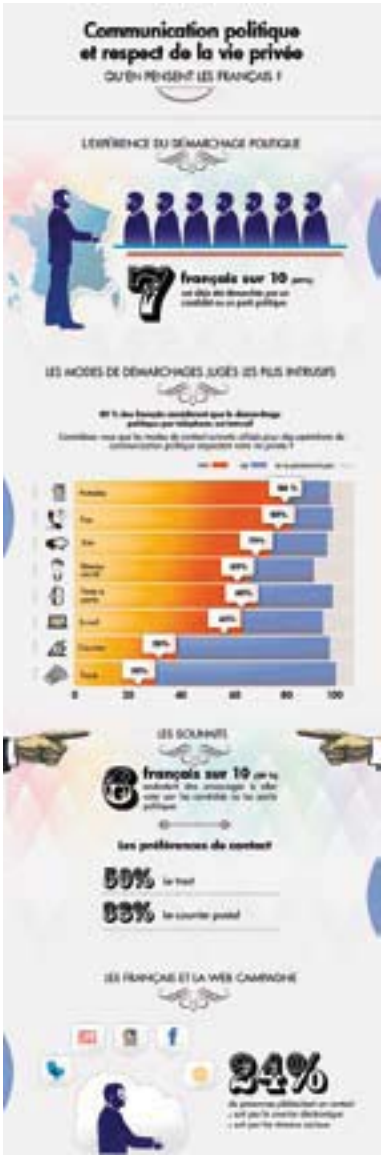
La CNIL a adressé au Gouvernement diverses propositions de modification du cadre juridique actuel tirant les enseignements des travaux de l'Observatoire.

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. ■



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 %.**

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).

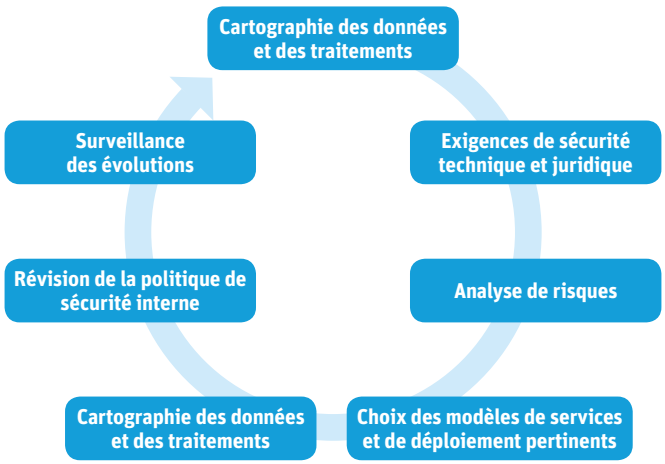
3 **Analyser les risques nouveaux engendrés par le passage dans le cloud** : réfléchir à l'impact sur les personnes concernées et sur l'organisme d'un passage des données et traitements identifiés dans le cloud, par exemple en ce qui concerne la perte de gouvernance sur le traitement, la dépendance technologique 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.

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.

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

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

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.

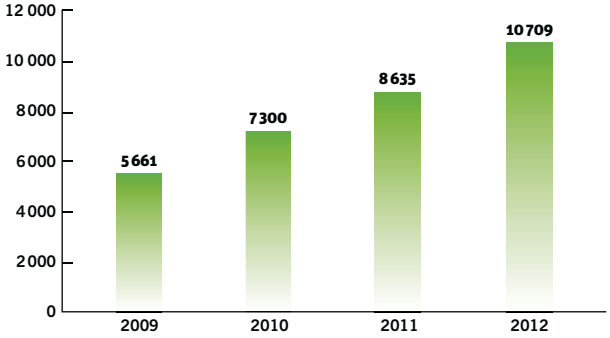
nelles devra être en accord avec la nature des traitements concernés (importance, sensibilité). En outre, le futur délégué à la protection des données aura l'obligation d'être régulièrement formé dans le cadre de ses fonctions.

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

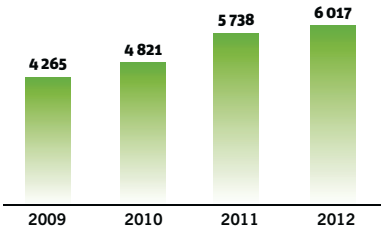
Des agents de sécurité d'un immeuble parisien saisissent la CNIL pour dénoncer la présence d'une caméra qui les filme en continu (PC sécurité). Le syndicat de copropriétaires utilisait la caméra pour surveiller l'activité et la présence des salariés en se prévalant d'une finalité liée à la protection 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.**

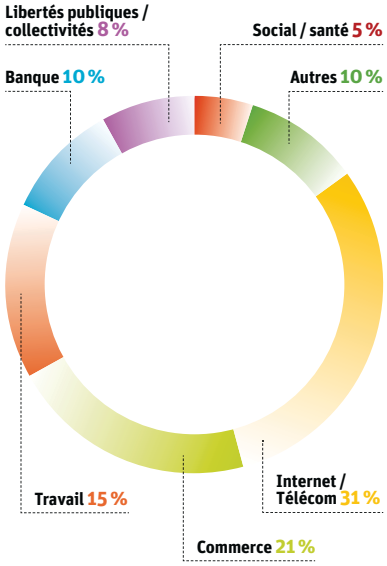
Le secteur du commerce représente 21 % des plaintes reçues (radiation de fichiers publicitaires, conservation des coordonnées bancaires, gestion des fichiers clients, défaut de confidentialité des données…)

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.

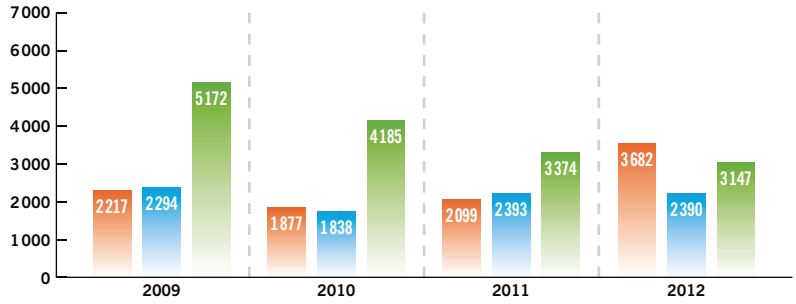
L'année 2012 a été marquée par une forte progression du nombre de demandes de droit d'accès indirect, puisque la CNIL a reçu 3 682 demandes, soit une augmentation de 75 % par rapport à 2011. Cette augmentation résulte principalement de l'importance des demandes (1 829 demandes) portant sur le fichier 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).

▸▸▸

3 682
DEMANDES DE DROIT D'ACCÈS INDIRECT
SOIT + 75 % PAR RAPPORT À 2011

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

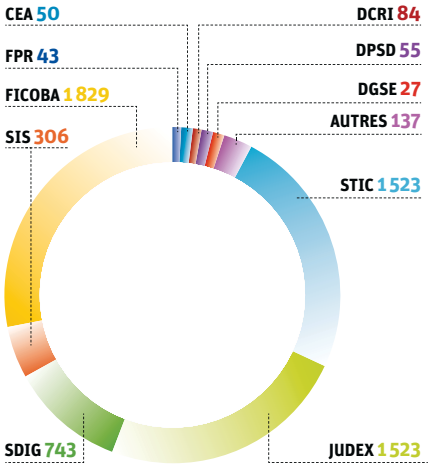


INFOS +

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.