rapport d'activité 2011

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS




CNIL
Commission Nationale de l'Informatique et des Libertés

La documentation Française

COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

RAPPORT D'ACTIVITÉ **2011**

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

LES CHIFFRES CLÉS DE 2011

DÉCISIONS ET DÉLIBÉRATIONS

1 969
DÉCISIONS ET DÉLIBÉRATIONS ADOPTÉES
(+ 25,5% par rapport à 2010)

249
AUTORISATIONS, DONT 6 AUTORISATIONS UNIQUES

11
REFUS D'AUTORISATION

2
DISPENSES

93
AVIS, DONT 1 AVIS SUR UN RÈGLEMENT UNIQUE

1
RECOMMANDATION PORTANT SUR LA COMMUNICATION POLITIQUE

MISES EN DEMEURE ET SANCTIONS

65
MISES EN DEMEURE

5
SANCTIONS FINANCIÈRES

13
AVERTISSEMENTS

2
RELAXES

FORMALITÉS PRÉALABLES

5 993
DÉCLARATIONS RELATIVES À DES SYSTÈMES DE VIDÉOSURVEILLANCE
(+37% par rapport à 2010)

4 483
DÉCLARATIONS RELATIVES À DES DISPOSITIFS DE GÉOLOCALISATION
(+ 33,5% par rapport à 2010)

744
AUTORISATIONS DE SYSTÈMES BIOMÉTRIQUES
(+5,4% par rapport à 2010)

PLAINTES ET DEMANDES DE DROIT D'ACCÈS INDIRECT

5 738
PLAINTES
(+ 19% par rapport à 2010)

2 099
DEMANDES DE DROIT D'ACCÈS INDIRECT AUX FICHIERS DE POLICE ET DE RENSEIGNEMENT
(+ 12% par rapport à 2010)

CONTRÔLES

385
CONTRÔLES
(+25% par rapport à 2010)

151
CONTRÔLES VIDÉOPROTECTION

CORRESPONDANTS

8 635
ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT « INFORMATIQUE ET LIBERTÉS »
(+25% par rapport à 2010)

SOMMAIRE

> Face à la complexité de l'écosystème numérique, l'enjeu du régulateur est de construire des relais"

AVANT-PROPOS DE LA PRÉSIDENTE

UNE CNIL DE COMBAT

La CNIL est aujourd'hui à une étape décisive de son évolution. Elle fait face à des mutations structurelles liées au développement de la société numérique ; elle est au cœur d'un débat international sur la protection des données au XXIème siècle. Cette période exceptionnelle nous invite à renouveler notre action.

Mutations structurelles tout d'abord car il s'agit bien d'un changement d'ère du fait du numérique. En quelques années, le numérique est devenu ambiant : avec la dématérialisation croissante des industries et des services, nous sommes passés d'un monde plutôt statique et national de fichiers à un univers de données, international, fluctuant et aux acteurs multiples. Les données sont partout, produites et consommées par les individus, les entreprises, les acteurs publics ; elles concerneront même demain de plus en plus les objets. Elles constituent désormais une valeur marchande considérable au cœur des enjeux économiques du XXIème siècle.

Face à ce nouvel écosystème, ma priorité est de consolider une adaptation déjà engagée et faire entrer la CNIL dans l'ère numérique. Ce nouvel environnement ne peut plus être régulé comme avant. Nous devons donc repenser notre action et nos outils d'intervention pour pouvoir traiter ces flux de données et s'adresser à des interlocuteurs toujours plus variés.

Certes, nos pouvoirs de contrôle et de sanction sont puissants et nous n'hésitons pas à y avoir recours en cas de besoin. Pour autant, ces instruments coercitifs ne peuvent suffire à mettre ce nouvel univers en état de droit. Nous ne pouvons plus en effet seulement affirmer des principes généraux et les contrôler *a posteriori*. Face à la complexité de l'écosystème numérique, l'enjeu du régulateur est de construire des relais. Des relais permettant d'associer et de responsabiliser les acteurs, publics et privés ou individus afin, *in fine*, de partager la charge de la régulation avec eux.

Pour ce faire, il nous faut nous rapprocher du terrain, de ces différents acteurs et de leurs spécificités métier. Cette approche nouvelle conduit à mettre à leur disposition des outils leur permettant de mettre en œuvre

Isabelle Falque-Pierrotin,
présidente de la CNIL

concrètement et le plus en amont possible les principes « Informatique et Libertés ». Cette boîte à outils existe déjà mais nous devons la compléter et la renouveler en collaboration avec les professionnels. Qu'il s'agisse de codes de bonne conduite, de chartes, labels ou correspondants « Informatique et Libertés », tous ces leviers sont au service de la mise en conformité des entreprises avec la loi « Informatique et Libertés ». C'est le pilotage de la conformité qui est au cœur du métier de la CNIL pour les années à venir.

Cette évolution correspond aussi, me semble-t-il, à une phase nouvelle de maturité des acteurs eux-mêmes. Sous la pression des consommateurs et des jeunes, la protection des données commence à ne plus être seulement perçue sous le prisme réducteur de la contrainte légale mais aussi comme un avantage concurrentiel, voire social. Les entreprises sont certes soucieuses de limiter le risque juridique, mais elles souhaitent également susciter la confiance de leurs publics interne (employés) et externes (clients, internautes) et, en cas de problème, limiter les préjudices en termes d'image.

Progressivement, la question de la protection des données dépasse le domaine de la direction juridique ou informatique pour investir le marketing, le commercial ou les ressources humaines.

Elle devrait cependant aussi investir les directions générales car l'innovation et la croissance de demain apparaissent de plus en plus liées au traitement de données.

Que l'on pense à la voiture, aux compteurs intelligents, à la domotique… beaucoup de secteurs devront en effet considérer la gestion des données personnelles comme un outil d'appropriation de leurs produits et services par leurs clients et, donc, un moyen de développement durable de leurs activités.

De la même manière, les individus ont mûri : même si beaucoup ne mesurent pas vraiment par qui et comment leurs données personnelles sont réellement utilisées, consommateurs ou internautes, qui représentent une population volatile et exigeante, revendiquent plus de transparence de la part des entreprises. Ils veulent savoir, voire maîtriser cette utilisation ! Les entreprises, et plus généralement, les acteurs du numérique sont donc confrontées à ces nouvelles demandes ; elles ne peuvent les décevoir au risque de perdre le contact et la confiance de leurs clients.

La CNIL doit elle aussi s'adapter à cette demande sociale nouvelle et proposer au grand public une pédagogie des solutions en lui donnant des clés pour un usage maîtrisé et responsable. La CNIL doit jouer pleinement son rôle d'accompagnateur de la vie numérique. C'est une des raisons pour laquelle nous avons mené une étude sur les smartphones, nouveaux outils du quotidien, qui renferment de très nombreuses données personnelles, y compris sensibles, sans sécurité particulière. À la suite de cette étude, nous avons élaboré 10 conseils pour mieux sécuriser son smartphone sous la forme d'un tutoriel vidéo didactique. C'est aussi dans cet esprit de pédagogie des bonnes pratiques que la CNIL a innové en réalisant une vidéo interactive, intitulée *Share the Party*, pour responsabiliser les jeunes aux vidéos ou photos qu'ils publient sur les réseaux sociaux.

Pour être capable d'anticiper les nombreux usages, nous pouvons de plus nous appuyer désormais sur les initiatives et les travaux de la Direction des études, de l'innovation et de la prospective. Les nombreux échanges que celle-ci a initiés témoignent de notre volonté d'ouverture et de dialogue auprès d'un public très divers qui enrichit nos réflexions et nous invite parfois à repenser nos modèles.

> “Le pilotage de la conformité est au cœur du métier de la CNIL pour les années à venir”

Ces évolutions structurelles se déroulent dans un contexte international de fortes turbulences ce qui ne simplifie pas le processus d'adaptation.

Europe, États-Unis et Asie se font face pour élaborer le cadre juridique de la protection des données personnelles qui soit le plus efficient en termes de croissance. Au niveau européen, je veux parler ici du projet de règlement réformant la directive européenne de 1995 sur la protection des données. Une proposition a été faite par la Commission le 25 janvier dernier et la CNIL s'est très fortement mobilisée. Nous vivons un moment historique dont il faut prendre la pleine mesure car le nouveau texte dessinera le nouveau paysage de la protection des données du XXIème siècle en Europe. L'essor du numérique et le contexte de globalisation rendent nécessaire la révision du cadre juridique européen existant. Le projet de règlement tel qu'il existe à l'heure où j'écris ces lignes, présente des avancées substantielles qui étaient attendues et nécessaires. Les droits des citoyens sont ainsi en grande partie renforcés : reconnaissance d'un droit à l'oubli, d'un droit à la portabilité de leurs données et clarification des règles relatives au recueil du consentement et à l'exercice de leurs droits. Dans le même temps, les entreprises bénéficient d'une simplification en matière de formalités administratives tout en étant soumises à des obligations accrues.

Mais, ce projet comporte aussi des points qui nous inquiètent et qui posent la question du fonctionnement même du dispositif proposé. À travers le critère de l'« établissement principal », le traitement des plaintes s'éloigne de l'internaute puisque celui-ci pourra être opéré par une autorité étrangère ; de plus, la coopération entre les autorités de protection des données apparaît trop restreinte et assez lourde alors même que c'est la clé pour peser dans les négociations avec les grands acteurs de l'internet. À ce titre, l'audit des nouvelles règles de confidentialité de Google, lancé en février dernier et réalisé par la CNIL pour le compte des 27 autorités européennes du G29 est un bon exemple d'une crédibilité renforcée par une action collective volontariste.

Dans ce contexte de forte concurrence internationale, le monde se tourne vers l'Europe et regarde ses capacités à moderniser son modèle tout en réaffirmant effectivement la vie privée en tant que droit fondamental. Car tout n'est pas seulement question de croissance ! Il s'agit de concilier celle-ci avec une vision humaniste des droits fondamentaux, approche qui a fait la spécificité de l'Europe et qui trouve de larges échos dans la francophonie notamment.

Pour qu'elle existe et pèse réellement sur l'échiquier international, l'Europe doit donc faire preuve d'audace, d'innovation, ne pas hésiter à mettre en avant ses nombreux atouts et à changer ses habitudes tout en restant fidèle à ses principes fondamentaux.

> “L'Europe doit moderniser son modèle tout en réaffirmant la vie privée en tant que droit fondamental”

La CNIL est donc face à un environnement national et international mouvant et compliqué. Je ne doute pas de sa capacité à réinventer son action et peser dans la négociation européenne. Ses équipes et ses membres sont armés et motivés pour affronter ces changements. En tant que Présidente de la CNIL, je suis particulièrement heureuse et enthousiaste de participer et d'orchestrer cette formidable aventure ! ■

“Une nouvelle extension des compétences de la CNIL : voici le phénomène le plus marquant de l’année 2011”

MOT DU SECRÉTAIRE GÉNÉRAL

Une nouvelle extension des compétences de la CNIL : voici, à mes yeux, le phénomène le plus marquant de l’année 2011. Cette extension procède d’abord du Législateur. En effet, il a confié à notre Commission deux nouvelles missions.

La première a été introduite par l’article 18 de la loi n° 2011-267 du 14 mars 2011 dite LOPPSI 2, qui attribue à la CNIL la compétence pour contrôler tous les systèmes de vidéoprotection installés sur la voie publique en application de la loi du 21 janvier 1995. Rappelons qu’avant l’adoption de cette loi, la CNIL était uniquement compétente en ce qui concerne les dispositifs de vidéosurveillance installés dans des locaux n’accueillant pas du public (une entreprise par exemple). Ces dispositifs relevant de la seule loi de 1978, et déclarés à la CNIL, sont au nombre de 35 000. Or, selon le rapport annuel des commissions départementales de la vidéoprotection de 2011, 897 750 caméras sont installées en France en application de la loi de 1995. En outre, le Gouvernement a annoncé un plan ambitieux de déploiement de la vidéoprotection avec un objectif de 45 000 caméras supplémentaires d’ici la fin de la Législature.

Cette nouvelle mission de contrôle des dispositifs de vidéoprotection (loi de 1995) concerne donc un nombre de caméras près de 25 fois supérieur à celui relevant de la loi de 1978. L’ampleur de cette nouvelle mission prévue par la Législateur nécessitera un renforcement conséquent des moyens de la CNIL. Sans attendre ceux-ci, notre Commission a exercé sa nouvelle compétence en contrôlant, en 2011, 150 systèmes de vidéoprotection. Ces contrôles se sont ajoutés aux 235 autres concernant l’application de la loi de 1978 modifiée. Avec 385 contrôles au total, contre 308 en 2010 (+ 25 %), notre Commission poursuit son effort de vérification concrète et *in situ* du respect des libertés individuelles à l’ère du numérique.

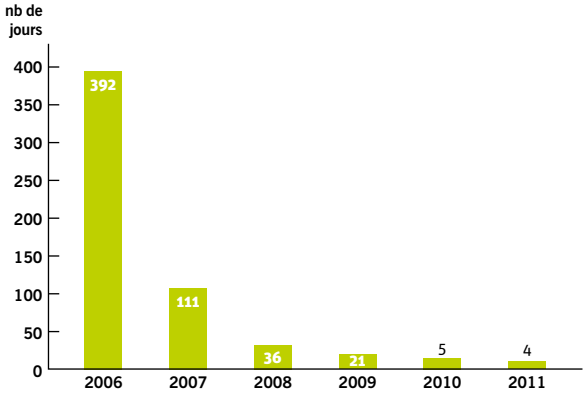
Yann Padova,
secrétaire général de la CNIL

La seconde procède de la transposition de la directive révisant le « paquet télécom » qui introduit l’obligation de notifier les violations de données à caractère personnel à la CNIL (article 38 de l’ordonnance n° 2011-1012 du 24 août 2011). Les responsables de traitements de données à caractère personnel du secteur des télécommunications sont désormais obligés d’informer la CNIL « en cas de violation » de l’intégrité ou de la confidentialité de ces données. La CNIL pourra ensuite, en cas d’atteinte portée aux données d’une ou plusieurs personnes physiques, d’une part, exiger que les responsables de traitement

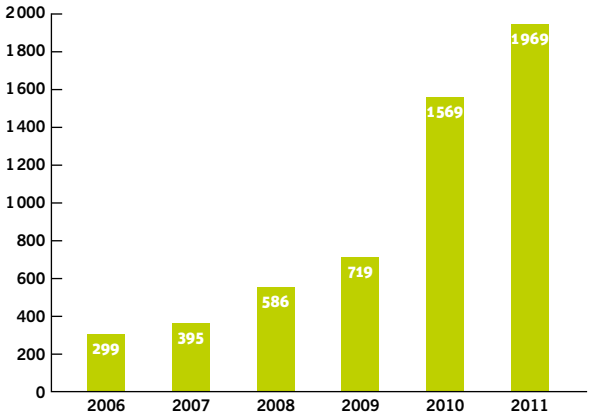
avertissent les intéressés et, d'autre part, diligenter des contrôles, mettre en demeure ces responsables de prendre les mesures correctrices, voire engager des procédures de sanction en cas de manquement aux obligations de sécurité qui leur incombe. Là encore, il s'agit d'une nouvelle mission, certes prévue par un texte européen obligatoire, mais qui va, de façon inéluctable bien qu'inconnue dans son ampleur, fortement modifier l'activité de la CNIL et exiger de sa part une réactivité et une expertise technologique encore renforcées.

À cet égard, la CNIL a engagé depuis plusieurs années une diversification du profil de ses agents en réorientant ses recrutements vers davantage d'ingénieurs. Ainsi les experts informatiques (hors service informatique interne) représentaient moins de 3,5 % de notre effectif en 2006. Ils sont aujourd'hui près de 10 %. Ce véritable investissement nous a permis en 2011 de créer notre propre laboratoire afin de tester des nouveaux matériels technologiques et de développer nos propres programmes. Il convient de souligner que notre Commission est la seule parmi ses homologues européens et étrangers à s'être dotée d'une telle capacité d'expertise technologique, indispensable dans le monde numérique. C'est également grâce à cette singularité qu'a été créée, au début 2011, la direction des études, de l'innovation et de la prospective (DEIP) qui peut, précisément, solliciter cette nouvelle capacité d'expertise du laboratoire. Tournée vers l'analyse pluridisciplinaire des usages, des nouvelles technologies, la DEIP dispose également d'un budget d'études lui permettant d'éclairer la Commission sur les enjeux de ces usages : tel a été le cas de l'étude menée par l'institut Médiamétrie sur les Smartphones, rendue publique en décembre 2011[1], et dont les conclusions ont nourri, notamment, l'un des axes du programme des contrôles de notre Commission pour 2012.

Les délais moyens de délivrance des récépissés des déclarations (2006 à 2011)



Le nombre des décisions et délibérations depuis 2006



L'extension des compétences de notre Commission découle, enfin, de la mise en œuvre de son pouvoir de labellisation. En effet, le 6 octobre 2011, notre Commission a adopté les deux référentiels (publiés au JO le 3 novembre 2011) permettant d'attribuer aux entreprises qui en feront la demande des « labels ». Ces labels, pour l'instant limités aux domaines de l'audit et de la formation, sont une façon, pour ces entreprises, de différentier, de singulariser, leurs produits par leur conformité à la loi « Informatique et Libertés ». Les premiers labels devraient être délivrés au cours du 1er semestre 2012. Très attendue par les entreprises, la labellisation fait entrer notre Commission dans un nouveau métier, celui de la régulation par la « qualité », fort différente de la régulation par la norme qu'elle pratique depuis sa création.

On le voit, l'année 2011 a été riche en nouveautés et nouvelles missions.

Pour autant, notre Commission a poursuivi l'amélioration de sa productivité, donc du service rendu à l'usager. En effet, en 2011, la CNIL a adopté 1 969 décisions et délibérations, contre 1 569 en 2010 (+ 25,5 %). Par ailleurs, les délais de délivrance des récépissés aux organismes qui déclarent leurs fichiers à la CNIL sont désormais de 4 jours. Ils étaient de 13 mois en 2006. Cette amélioration est donc pérenne en dépit de l'augmentation des flux concernés puisque le nombre des déclarations faites à la CNIL est passé de 70 797 en 2010 à 82 243 en 2011. Ces bons résultats sont à mettre au crédit des équipes de la CNIL dont la motivation mérite d'être saluée ici. ■

[1] *Cette étude est présentée plus en détail page 23 du présent rapport*

1. LES NOUVELLES MISSIONS

Les contrôles de la vidéoprotection : bilan et plan d'action

Les labels

La notification des violations de données à caractère personnel

La prospective : premiers travaux, premières publications

GROS PLAN

Smartphone et vie privée, une priorité d'analyse et d'action

LES CONTRÔLES DE LA VIDÉOPROTECTION : BILAN ET PLAN D'ACTION

La loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 (LOPPSI 2) a notamment modifié l'article 10 de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, afin de permettre à la CNIL de contrôler les dispositifs dits « de vidéoprotection ». La compétence de la Commission est donc désormais expressément reconnue pour le contrôle tant des dispositifs de « vidéoprotection » soumis à la loi de 1995 (pour la voie publique et les lieux ouverts au public) que pour les dispositifs de « vidéosurveillance » soumis à la loi de 1978 (pour les lieux non accessibles au public telles que les zones réservées aux salariés).

150
CONTRÔLES SUR DES LIEUX VARIÉS DU TERRITOIRE NATIONAL

75%
DES CONTRÔLES EFFECTUÉS AUPRÈS DU SECTEUR PRIVÉ

LA MISE EN ŒUVRE DES CONTRÔLES : MÉTHODOLOGIE ET TYPOLOGIE DES ORGANISMES CONTRÔLÉS

Cette extension de sa compétence a été prise en compte par la Commission dès l'adoption de son programme annuel de contrôle pour l'année 2011 puisque, lors de sa séance du 24 mars 2011, celle-ci s'est fixée pour objectif de réaliser 150 contrôles sur les dispositifs de vidéoprotection. Cet objectif a été atteint. Ces 150 contrôles ont été effectués sur des lieux variés du territoire national.

75% de ces contrôles ont concerné le secteur privé (magasins, hôtels, restaurants, entreprises, banques, etc.) ; 25% le secteur public (gares écoles, musées, collectivités locales, etc.).Les organismes contrôlés ont été choisis afin de s'assurer de l'application de la loi dans l'ensemble des situations où un système vidéo peut être déployé. Ainsi, les organismes contrôlés ont été identifiés en fonction de leur taille – et donc du nombre de personnes filmées (par exemple, des contrôles ont été diligentés aussi bien dans des commerces de petite taille que dans des grands magasins parisiens), de leur localisation (centres commerciaux et centres villes) et, également, parfois, en fonction de l'actualité (article de presse soulignant la mise en œuvre d'un dispositif).

Les principaux points vérifiés par la CNIL sont les suivants :

- le respect de l'autorisation préfectorale délivrée quant à la finalité du dispositif et l'orientation des caméras ;
- la durée de conservation des images ;
- l'information des personnes filmées ;
- les mesures de sécurité entourant le dispositif.

Environ **15% des contrôles** ont été effectués dans le cadre de l'instruction de plaintes. On doit en effet rappeler que la loi du 21 janvier 1995 prévoit expressément que « *Toute personne intéressée peut saisir […] la Commission nationale de l'informatique et des libertés de toute difficulté tenant au fonctionnement d'un*

système de vidéoprotection ». Ainsi, la CNIL a, par exemple, été saisie par des salariés s'interrogeant sur la légalité de caméras placées dans leur entreprise ou encore de clients ayant remarqué un dispositif de vidéoprotection en l'absence d'information à destination du public, etc.

On doit aussi relever que la CNIL a été saisie d'une demande de la SNCF souhaitant que des contrôles soient réalisés afin de vérifier la conformité des dispositifs de vidéoprotection installés dans ses gares. La loi de 1995 permet en effet à un responsable d'un système de vidéoprotection de saisir la CNIL afin que celle-ci effectue un contrôle sur ses installations. Ce « partenariat » a ainsi conduit la CNIL à effectuer plus d'une vingtaine de contrôles portant sur les systèmes de vidéoprotection installés dans des gares réparties sur l'ensemble du territoire national.

> Toute personne peut saisir la CNIL de toute difficulté portant sur un système de vidéoprotection

INFOS +

La Commission nationale de l'informatique et des libertés peut, sur demande de la commission départementale prévue au premier alinéa du présent III, du responsable d'un système ou de sa propre initiative, exercer un contrôle visant à s'assurer que le système est utilisé conformément à [l'autorisation préfectorale le concernant] **et, selon le régime juridique dont le système relève, aux dispositions de la présente loi ou à celles de la loi n° 78-17 du 6 janvier 1978 précitée[1].**

[1] LOPPSI 2/14 mars 2011

LES PRINCIPAUX CONSTATS EFFECTUÉS LORS DES CONTRÔLES

▸ **Les responsables contrôlés ont parfaitement identifié la compétence de la CNIL** en matière de contrôle des systèmes de vidéoprotection.
Les contrôles ont permis de constater qu'aucun des dispositifs vérifiés par la Commission – à l'exception d'un seul – n'avait fait l'objet d'un contrôle de la part d'une autre autorité (forces de police, préfectures, etc.). L'activité de la CNIL comble donc bien un « vide » en termes de contrôle de dispositifs potentiellement intrusifs pour la vie privée des personnes.

40%
DES CONTRÔLES RÉVÈLENT UNE INFORMATION DES PERSONNES INEXISTANTE OU INSUFFISANTE

▸ **Environ 50 % des dispositifs contrôlés relèvent à la fois de la loi de 1995** (caméras filmant des zones ouvertes au public : espace « clients ») **et de la loi « Informatique et Libertés »** (zones non ouvertes au public : espace « réservés » aux salariés).
Or, les préfectures, lorsqu'elles délivrent des autorisations, ne mentionnent jamais, à titre d'information, la loi de 1978 au nombre des dispositions légales devant être respectées. Tout au plus, certaines autorisations préfectorales mentionnent-elles l'interdiction, pour le responsable du système, de constituer un traitement à partir des images enregistrées.
Pour autant, la circulaire du 14 septembre 2011 relative au cadre juridique applicable à l'installation de caméras de vidéoprotection reconnaît l'application de la loi « Informatique et Libertés » aux dispositifs installés dans des lieux non ouverts au public. La CNIL va donc se rapprocher des préfectures afin que celles-ci rappellent les dispositions de la loi « Informatique et Libertés ».

▸ **Un manque d'homogénéité dans les autorisations délivrées par les différentes préfectures a été constaté**, que ce soit concernant leur compétence (application ou non de la loi de 1995 à des lieux tels que des crèches ou des espaces non ouverts au public dans des maisons de retraite) ou quant aux zones pouvant être filmées (par exemple, certaines préfectures refusent que les zones où se restaurent les personnes soient filmées, d'autres l'acceptent).

Les principaux manquements concernant les conditions de mise en œuvre effective des dispositifs vidéo, relevés à l'occasion des contrôles sont les suivants :

▸ **Une absence d'autorisation ou absence de renouvellement préfectoral** (environ 30 % des contrôles). Les absences d'autorisation préfectorale sont le plus souvent des cas constatés lorsqu'un contrôle est effectué pour apprécier la régularité d'un dispositif soumis à la loi de 1978 et qu'il fait apparaître un dispositif filmant également des lieux ouverts au public ;

▸ **Une absence de déclaration à la CNIL** pour les parties de dispositifs relevant de la loi de 1978 (environ 60 % des cas) ;

▸ **Une information des personnes inexistante ou insuffisante** (environ 40 % des contrôles) ;

▸ **Une mauvaise orientation des caméras** (environ 20 % des contrôles). Certains contrôles ont permis de constater des caméras « cachées », notamment dans les détecteurs de fumées ;

▸ **Une durée de conservation excessive** (environ 10 % des contrôles) ;

▸ **Des mesures de sécurité insuffisantes** (environ 20 % des contrôles).

La CNIL a ainsi adopté, sur la base de l'article 10 III de la loi de 1995, **trois mises en demeure** concernant les dispositifs de vidéoprotection. Les préfectures territorialement compétentes en ont été informées.

Les contrôles ont également permis de constater parfois l'utilisation de caméras factices et les dysfonctionnements pouvant affecter les dispositifs vidéo (absence d'enregistrement, mauvaise qualité de l'image, etc.).

Enfin, les contrôles ont permis de constater que les responsables de dispositifs de vidéoprotection/vidéosurveillance ont, bien souvent, des difficultés à comprendre l'articulation entre la loi « Informatique et Libertés » et la loi du 21 janvier 1995. ■

FOCUS

Les perspectives pour l'année 2012

Sur le même modèle de partenariat que celui développé avec la SNCF, la CNIL va engager en 2012 le contrôle du système de vidéoprotection mis en œuvre par la RATP. Ce contrôle permettra à la CNIL de s'assurer que le système de la RATP respecte les dispositions issues de la loi de 1995. Ces contrôles seront effectués sur l'ensemble du réseau RATP au cours du premier trimestre de l'année 2012. La CNIL poursuivra sa politique de contrôle des dispositifs de vidéoprotection au cours de l'année 2012 en privilégiant, notamment, ceux qui concernent un nombre important de personnes (on pense ici aux dispositifs mis en œuvre au sein des collectivités locales ou au sein de structures accueillant un nombre important de personnes), et les dispositifs de vidéoprotection utilisés également à des fins accessoires telles la « vidéoverbalisation ».

LES LABELS

La loi du 6 août 2004 a introduit la possibilité pour la CNIL de délivrer des labels à des produits ou des procédures. La Commission a procédé en septembre 2011 à la modification de son règlement intérieur conformément aux dispositions de l'article 13-II de la loi du 6 janvier 1978 modifiée afin de préciser « les modalités de mise en œuvre de la procédure de labellisation ».

Pour les entreprises, le Label CNIL est un facteur de différenciation qui leur permet d'attester de la qualité de leurs produits ou de leurs services. Pour leurs clients ou leurs usagers, c'est un indicateur de qualité, donc un facteur de confiance qui garantit un haut niveau de protection des données. Pour la CNIL, c'est un vecteur de diffusion de la culture « Informatique et Libertés » et un moyen de garantir une meilleure application de la loi. Il s'agit donc d'un enjeu stratégique pour la Commission qui s'inscrit d'ailleurs pleinement dans le projet de révision de la Directive 95/46 (article 39 du projet de règlement européen).

La Commission a choisi de labelliser dans un premier temps des procédures d'audits de traitements et des formations « Informatique et Libertés ». L'adoption de deux premiers référentiels en octobre 2011 marque le lancement des Labels CNIL.

INFOS +

Le Comité de labellisation assure le pilotage des Labels

Il regroupe trois commissaires de la CNIL (M. Jean-François CARREZ, M. Bernard PEYRAT et M. Dominique RICHARD) en charge de proposer des orientations relatives à la politique de labellisation, d'élaborer les projets de référentiel et de superviser l'évaluation des demandes de labels.

LA PROCÉDURE DE LABELLISATION

La création du référentiel

Dans un premier temps, une organisation professionnelle ou une institution regroupant des responsables de traitements adresse à la Commission une demande de création de label relatif à des produits ou des procédures. Cette demande initiale permet à la Commission d'engager une réflexion sur l'opportunité d'adopter un référentiel pour une nouvelle catégorie de produits ou de procédures. Dans le cadre de cette réflexion, la Commission peut rencontrer les parties prenantes (administrations, autorités de certification…) afin de s'assurer de la cohérence de ses objectifs avec les besoins et le niveau de maturité du marché.

Si, à la suite de ces travaux, elle juge opportun de délivrer un label pour cette catégorie de produits ou de procédures, elle élabore un référentiel adopté en séance plénière sous la forme d'une délibération. Une fois ce texte publié au Journal officiel, toute entreprise souhaitant obtenir le label peut adresser une demande à l'aide du formulaire disponible sur le site de la CNIL.

Deux entreprises ayant des activités distinctes (par exemple un cabinet d'avocat et un prestataire informatique) peuvent choisir de s'associer pour procéder à une demande de label. On parle alors de « *label conjoint* ». Dans ce cas, les demandeurs s'engagent à collaborer pendant la durée de validité du label.

L'instruction d'une demande de label

L'instruction se déroule en deux phases : l'examen de la recevabilité et l'évaluation de la conformité du produit ou de la procédure.

L'examen de la recevabilité permet de s'assurer que la demande est formellement complète et que le produit ou la procédure correspond à l'objet défini dans le référentiel. À défaut de réponse de la Commission dans un délai de deux mois, la demande est réputée irrecevable.

Si la demande est recevable, les services de la Commission procèdent à **l'évaluation du produit ou de la procédure**. Il s'agit de s'assurer que le produit ou la procédure satisfait à l'ensemble des exigences du référentiel, sur la base de justifications appropriées (formulaire, procédures, curriculum vitae…). Afin de procéder à cette évaluation, les services de la CNIL peuvent demander communication de toute pièce ou document pertinent et auditionner le demandeur. Une fois l'évaluation terminée, la Commission réunie en séance plénière décide de l'octroi ou non du label. En cas de délivrance du label, la décision emporte autorisation d'utilisation du logo « Label CNIL ».

▸▸▸

La vie du label

Le label est délivré pour une durée de trois ans. Le titulaire devra donc procéder à une demande de renouvellement, au plus tard six mois avant la date d'échéance du label.

En cas de modification des caractéristiques du produit ou de la procédure labellisé avant la date d'échéance, le titulaire est tenu d'en informer la Commission par courrier. Ces modifications seront analysées par les services afin d'évaluer leur importance. Dans le cas où celles-ci seraient identifiées comme substantielles, une nouvelle évaluation sera réalisée. Dans le cas contraire, la durée initiale de trois ans continue à courir.

Si des faits ou circonstances de nature à remettre en cause la conformité d'un produit ou d'une procédure sont portés à la connaissance de la Commission, la CNIL peut, à l'issue d'une procédure contradictoire, décider de retirer le label.

Les référentiels peuvent imposer aux titulaires d'un label des obligations spécifiques permettant de s'assurer que les conditions de délivrance du label sont maintenues en permanence pendant toute sa durée de validité (par exemple, transmission à la Commission d'un rapport d'activité annuel).

INFOS +

Qu'est qu'un référentiel ?

Il s'agit d'une liste d'exigences ou de spécifications à laquelle le produit ou la procédure doit répondre afin d'obtenir le label. Ces exigences correspondent aux critères permettant d'évaluer la conformité du produit ou de la procédure aux dispositions de la loi « Informatique et Libertés ».

LES DEUX PREMIERS RÉFÉRENTIELS D'ÉVALUATION

Les procédures d'audit de traitement de données personnelles

L'audit « Informatique et Libertés » est un audit dont les critères permettent d'évaluer la conformité à la loi de traitements de données à caractère personnel. Son champ concerne les traitements de données à caractère personnel mis en œuvre par un responsable de traitement dans un périmètre délimité. Ce périmètre peut être très large et englober l'ensemble des traitements mis en œuvre par une entreprise ou seulement un secteur, par exemple les traitements de ressources humaines.

Le référentiel d'évaluation de procédures d'audit de traitements de données à caractère personnel (cf. : délibération n°2011-316 du 6 octobre 2011) fixe les critères qui devront être satisfaits selon les catégories suivantes :

▸ **Les critères relatifs à la démarche d'audit de traitements.** Ils comprennent principalement des exigences relatives à la compétence des auditeurs et à la procédure de mise en œuvre de l'audit (préparation, réalisation et finalisation). Ils s'inspirent de ceux utilisés dans les normes internationales, en particulier la

FOCUS

Des exigences fortes pour l'accès aux données

Afin d'assurer la préservation de l'intérêt et des droits fondamentaux des personnes concernées en application des principes de proportionnalité et de sécurité, le référentiel pose deux limites importantes à l'accès des auditeurs aux données à caractère personnel :

• toute donnée collectée pendant l'audit doit être anonymisée dès lors qu'elle sort des locaux de l'organisme audité. Ainsi, les preuves figurant dans le rapport d'audit devront être présentées sous une forme anonymisée sauf si ce document est entièrement conçu et consulté dans les locaux de l'organisme audité ;

• la confidentialité des données à caractère personnel doit être garantie par une clause insérée dans le contrat entre l'auditeur et l'audité. Cette clause doit notamment rappeler le principe d'anonymisation précédemment mentionné.

norme ISO 19011 *(« Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental », norme conçue pour s'adapter à d'autres types d'audit)*, compte tenu des spécificités de la loi du 6 janvier 1978 modifiée et de la sécurité des systèmes d'information.

▸ **Les critères sur le contenu de l'audit de traitements.** Ils ont été élaborés de telle manière qu'ils s'adaptent aux différentes approches des professionnels. Ces critères sont vérifiables : les demandeurs doivent apporter des preuves dont la forme est libre (extraits de méthodologie, questionnaires types, documentation interne…). Ces exigences requièrent de l'auditeur qu'il démontre la mise en œuvre d'une démarche méthodologique, systématique et documentée, permettant de vérifier la conformité effective des traitements audités aux dispositions de la loi.

Les formations « Informatique et Libertés »

Une formation « Informatique et Libertés » est une procédure destinée à produire et à développer les connaissances et les savoir-faire nécessaires au respect de la loi « Informatique et Libertés ». La formation peut se dérouler sur plusieurs jours et comprendre plusieurs modules indépendants. Le label est attribué à un organisme et à un contenu, et non à un ou des formateurs particuliers.

Le référentiel d'évaluation de formations (cf. délibération n°2011-315 du 6 octobre 2011), fixe les critères qui devront être satisfaits selon les deux catégories suivantes :

▸ **Les critères sur l'activité de formation.** Ils permettent d'évaluer le respect par l'organisme de la loi « Informatique et Libertés », la compétence des formateurs, et les conditions dans lesquelles le contenu pédagogique est notamment créé, délivré et mis à jour. Ils s'inspirent de ceux utilisés dans la norme internationale ISO 29990 (« *Service de formation dans le cadre de l'éducation et de la formation non formelle – Exigences de base pour les prestataires de services* »). L'objectif poursuivi par le référentiel est d'identifier, pour chacune des phases de l'activité de formation, les points à respecter pour créer les conditions permettant d'offrir une formation de qualité, tant sur la forme que sur le fond.

▸ **Les critères sur le contenu de la formation.** Ils fixent les points qui devront être abordés lors de la formation. Le référentiel reprend le contenu et l'architecture de la loi « Informatique et Libertés », afin de couvrir la plus grande partie du champ d'application de la loi. La plupart des exigences requièrent de l'organisme qu'il prouve que la formation et le formateur sont en mesure de permettre aux apprenants de comprendre et de connaître les aspects de la loi figurant au programme de la formation. Outre la remise du support pédagogique, la CNIL se réserve la possibilité, le cas échéant, d'auditionner les formateurs et d'assister à une formation. On distingue :

▸ **Des exigences sur un module principal** composé des fondamentaux de la loi (principes et définitions, droits des personnes concernées…). Ces points doivent nécessairement être traités lors de la formation. Toutefois, une formation peut être constituée de plusieurs jours ou modules. Il suffit que les exigences précitées soient satisfaites dans l'un des modules ou l'une des journées de formation pour être éligible au label ;

▸ **Des exigences sur des modules optionnels.** Ces modules peuvent aborder par exemple le rôle du correspondant à la protection des données, l'encadrement des traitements dans le domaine de la santé, ou encore le pouvoir de sanction de la CNIL. Ils sont facultatifs et ne seront évalués que lorsque la formation en prévoit l'enseignement. ■

FOCUS

La nécessité d'effectuer des vérifications

L'évaluation ne doit pas se limiter pas à une revue documentaire réalisée par des experts juridiques, mais elle doit s'appuyer également sur des vérifications effectuées par des experts informatiques sur les systèmes d'information utilisés. Par exemple, les durées de conservation des données doivent faire l'objet d'une appréciation de l'auditeur, qui devra être complétée par une vérification dans le système d'information afin d'en constater la réalité.

> Les premiers labels seront délivrés en 2012. Une liste des procédures d'audit de traitements et de formations labellisées sera ensuite disponible sur le site de la CNIL.

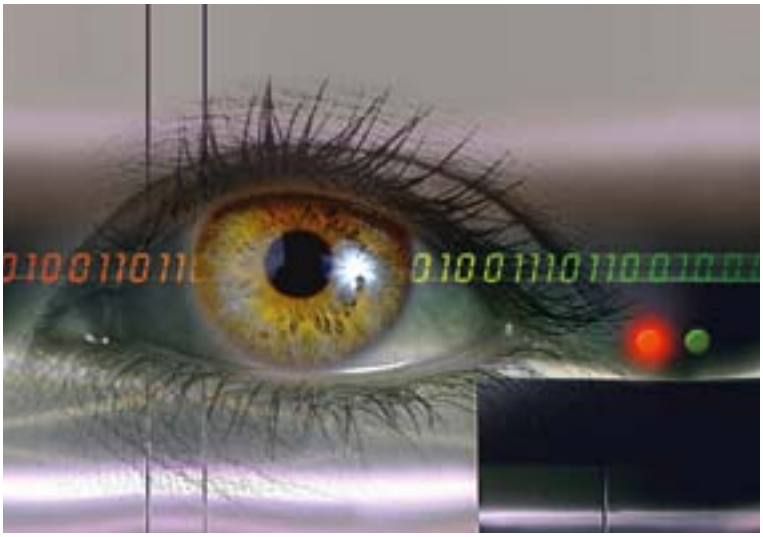
FOCUS

Un pré-requis : une démarche « Informatique et Libertés » chez le candidat

Dans la mesure où les organismes de formation traitent les données à caractère personnel des apprenants, il est apparu nécessaire de fixer des exigences relatives au respect par l'organisme de la loi « Informatique et Libertés ». Il ne saurait être envisageable de délivrer un label CNIL à un organisme qui ne présenterait pas des garanties minimales de conformité à la loi du 6 janvier 1978 modifiée.

LA NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

Régulièrement, les médias se font l'écho de comptes clients dérobés lors d'attaques informatiques ou dévoilés sur internet en raison d'une mauvaise configuration du site web. De telles erreurs se multiplient, souvent au détriment des personnes dont les données sont perdues, volées, divulguées, ou détruites.



Dans de telles circonstances, la loi ne préconisait aucune forme d'alerte particulière. La seule obligation légale des responsables de traitements était de garantir la sécurité des données. Mais que faire quand la sécurité a fait défaut et que l'erreur a été commise ?

UNE NOUVELLE OBLIGATION DÉFINIE AU NIVEAU EUROPÉEN

« Prévenir plutôt que guérir »

C'est en 2002, dans l'État de Californie qu'est né le principe d'obliger les acteurs économiques détenant des données sensibles à informer une autorité, ainsi que les personnes dont ils traitent les données, des atteintes à la confidentialité qui ont été perpétrées. La grande majorité des États américains a, depuis, adopté des lois similaires.

Prévenir plutôt que guérir, tel pourrait être le fondement de cette nouvelle obligation. Du côté du consommateur, il s'agit de prévenir pour qu'il puisse agir (ex : changer de carte bancaire) plutôt que de risquer une usurpation d'identité ou une fraude sur son compte bancaire.

Du côté des acteurs économiques, il leur incombe de prévenir les violations en renforçant les mesures de sécurité interne plutôt que de réaliser des notifications coûteuses et préjudiciables à leur image de marque.

De nombreux pays ont repris ce principe comme l'Allemagne, l'Espagne ou bien encore l'Irlande.

En France, cette nouvelle responsabilité avait déjà été proposée par les sénateurs Anne-Marie ESCOFFIER et Yves DETRAIGNE dans une proposition de loi « visant à mieux garantir le droit à la vie privée à l'heure du numérique » ; mais elle n'avait pas été adoptée de manière définitive par le Parlement.

De Bruxelles à Paris : l'adoption d'une nouvelle obligation

La Commission européenne s'est donc inspirée de ces dispositifs et a retenu le principe d'une telle obligation à l'occasion de la révision des directives « Paquet télécom ».

Toutefois, le « Paquet télécom » constituant le cadre européen des communications électroniques, l'obligation de notifier les failles de sécurité a été limitée aux fournisseurs de services de communications électroniques.

Les autorités de protection des données regroupées au sein du « G29 » (qui regroupe les autorités de protection des données des États membres de l'Union) ont exprimé leur point de vue en produisant deux avis avant l'adoption définitive de la directive, puis en se prononçant sur

l'encadrement des violations de données à caractère personnel. Le G29 a fait part de son souhait de voir cette obligation généralisée à tous ceux qui utilisent des données personnelles, et en particulier les sites d'e-commerce, ou les banques en ligne.

Cette demande n'a pas été suivie en raison de l'aspect sectoriel du « Paquet télécom » (qui se cantonne aux communications électroniques). Le projet de règlement révisant la directive de 1995 généralise cette obligation à tous les responsables de traitement.

Le 26 août 2011, l'ordonnance « Paquet Télécom » a permis d'adopter en droit français l'obligation de notification qui a été inscrit dans la loi « Informatique et Libertés » à l'article 34 bis.

UNE NOUVELLE MISSION POUR LA CNIL

Une mission complexe

Toutes les violations de données à caractère personnel concernant des fournisseurs de service de télécom doivent désormais être systématiquement notifiées à la CNIL, et ce, quelle que soit leur gravité.

La CNIL devra analyser de nombreuses situations au regard de la définition particulièrement étendue des « violations ».

Une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel constitueront une violation de données à caractère personnel. Cette violation résultera soit d'un acte malveillant : par exemple, en cas de piratage informatique. Soit d'une erreur commise par un salarié qui détruirait ou divulguerait un fichier client après une fausse manipulation.

La CNIL va donc devoir gérer ce nouveau flux d'informations et vérifier que les personnes ont bien été informées quand la loi l'exige.

En effet, la notification des violations aux personnes n'est pas systématique à la différence de celle à la CNIL. Si toutes les violations, y compris celles sans conséquence, étaient notifiées aux personnes, ces dernières seraient submergées par ces alertes et elles n'y prêteraient plus attention. Une telle attitude irait à l'encontre de la raison d'être du dispositif. C'est la raison pour laquelle seules les violations qui peuvent porter atteinte aux personnes doivent leur être notifiées. La directive 2009/136/CE précise bien qu'*« une violation devrait être considérée comme affectant les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier lorsqu'elle est susceptible d'entraîner, par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation »*.

En pratique, la destruction d'un fichier client qui, préalablement, aurait été sauvegardé, n'apparaît pas préjudiciable pour les personnes. De même, si un fichier client subit une attaque informatique mais qu'il ne peut être lu qu'après décodage avec un mot de passe confidentiel, qui n'a pas été piraté, les risques pour les personnes apparaissent également comme limités.

▸▸▸

INFOS +

Le Paquet Télécom, qu'est-ce que c'est ?

L'expression « Paquet Télécom » désigne un ensemble de textes communautaires adoptés en 2002 et définissant un cadre juridique commun pour la réglementation et la régulation des réseaux et des services de communications électroniques.
Il s'agit donc d'un outil sectoriel qui n'a pas vocation à s'appliquer à tous les acteurs de l'Internet.
Cette législation a pour principal objectif de réglementer la gestion des réseaux nationaux ouverts au public et d'obliger les grands opérateurs historiques à s'ouvrir à la concurrence.
Ce cadre réglementaire a fait l'objet d'une vaste révision qui a abouti le 25 novembre 2009, lorsque le Parlement et le Conseil européen ont adapté ces dispositions. L'un de leurs objectifs était d'améliorer la protection des données à caractère personnel et de la vie privée des individus dans le secteur des communications électroniques.
Les États membres avaient l'obligation de transposer ces dispositions uniquement dans leur droit national avant le 25 mai 2011.

C'est ces cas de figure que la loi a visé en exemptant les fournisseurs de leur obligation d'information des personnes lorsque des mesures de protection ont été prises.

Dans l'hypothèse où ces mesures s'avéraient insuffisamment efficaces pour garantir que les données ne sont pas exploitables par un tiers, la Commission pourra mettre en demeure le fournisseur de notifier la violation aux personnes.

Cette procédure vise à inciter les responsables de traitement à adopter en amont des mesures de sécurité efficaces.

INFOS +

Faille de sécurité ou violation de données à caractère personnel, quelle différence ?

L'expression « faille de sécurité » est souvent utilisée comme synonyme de « violation de données à caractère personnel ». Or, une faille de sécurité (ou une violation de sécurité) ne concerne pas toujours des données à caractère personnel. Par exemple, la violation de consignes de sécurité par un employé qui aurait mal utilisé l'outil informatique ne signifie pas nécessairement que les données personnelles stockées ont été compromises.
L'expression anglo-saxonne *data breach* a le mérite d'être plus explicite puisqu'elle fait référence à la faille et aux données.

Toujours plus de sécurité

La CNIL va donc devoir mettre en œuvre en 2012 cette nouvelle mission qui lui est confiée par le législateur. Elle devra notamment accompagner les fournisseurs de services de communications électroniques dans l'appréciation et la mise en œuvre de mesures de protection efficaces.

La CNIL interpellait déjà régulièrement les responsables de traitements sur leurs obligations de sécurité et leur proposait des bonnes pratiques à mettre en œuvre tant lors de l'examen de demandes d'autorisation, que lors de l'instruction de demandes de conseil. Un guide « sécurité des données personnelles » a même été publié en 2010.

Vers plus de transparence

Cette nouvelle obligation s'inscrit dans un processus de responsabilisation accrue des acteurs en charge des données personnelles.

Il ne s'agit plus d'attendre que les victimes portent plainte, et que la CNIL contrôle et sanctionne. Le responsable du traitement doit assumer pleinement la responsabilité des erreurs commises en amont afin de permettre aux personnes d'éviter de devenir victime.

Cette obligation permettra à la CNIL d'avoir une meilleure vision du niveau de sécurité mise en œuvre, mais également d'offrir un meilleur accompagnement. ■

FOCUS

Dernière minute : notification des failles de sécurité

Le décret d'application de l'ordonnance Paquet Télécom a été publié le 31 mars 2012, modifiant ainsi le décret « Informatique et Libertés » de 2005 (les articles 91-1 et suivants y ont été ajouté). Ces dispositions permettent de préciser les modalités de mise en œuvre du nouvel article 34 bis de la loi « Informatique et Libertés ». Elles décrivent comment la CNIL doit être notifiée ainsi que les cas où les personnes doivent également être informées.

LA PROSPECTIVE : PREMIERS TRAVAUX, PREMIÈRES PUBLICATIONS

Créée en janvier 2011, la direction des études, de l'innovation et de la prospective (DEIP) a été mise en place pour développer la réflexion prospective au sein de la CNIL.
Centre de ressources de prospective et de veille pour l'ensemble de la Commission cette direction, en liaison avec les autres directions, contribue à l'identification et l'analyse des usages innovants des technologies et leurs évolutions de notre mode de régulation.

L'analyse des usages est au cœur du travail prospectif de la DEIP. En 2011, la direction s'est donc intéressée aux comportements des jeunes sur les réseaux sociaux (cf chapitre 2) et aux pratiques d'utilisation du smartphone. Ces études sont conduites selon une approche qui se veut résolument pluridisciplinaire- notamment économique et sociologique- et non uniquement technologique ou juridique.
Le recrutement, en juillet 2011, d'un chargé d'études prospectives a permis d'engager les premiers chantiers de prospective décidés par la Commission.

LES PREMIERS CHANTIERS

La Commission, sur proposition de la direction de la prospective (DEIP) a décidé le lancement en 2011 de deux grandes études prospectives, actuellement en cours.

Les smartphones et leur écosystème

Le smartphone est devenu le centre nerveux de la vie numérique. La DEIP a donc souhaité explorer les tendances à l'horizon 5-10 ans autour de l'objet smartphone : acteurs économiques, évolutions des techniques de profilage et de personnalisation, formes possibles de régulations…

Première étape : dresser un état des lieux des pratiques. Un sondage a ainsi été réalisé pour mieux connaître et comprendre les usages quotidiens des utilisateurs de smartphones et évaluer leur niveau de perception des enjeux de protection des données personnelles. Les résultats de ce sondage, fort éclairants, ont été rendus publics en décembre 2011 et ont fait l'objet d'une analyse approfondie présentée dans ce rapport annuel. Les constats dégagés, à savoir une très forte perception d'opacité sur ces données qui « sortent » des smartphones et une sécurisation insuffisante du smartphone ont conduit la Commission à décider d'un plan d'action axé en particulier autour du développement d'une véritable pédagogie des usages.

Parallèlement, une étude technico-économique sur l'utilisation des smartphones a été confiée, en octobre 2011, à une société d'études et de conseils, associée avec un consultant spécialisé en droit des technologies de l'information et une société de conseils en sécurité informatique. Le premier travail consiste à dresser un panorama des technologies et services liés au mobile, comme par exemple les différents capteurs ou la géolocalisation, mais sous un angle prospectif : à quelles

▸▸▸

évolutions pouvons-nous nous attendre d'ici 5 à 10 ans ? Il s'agit également d'établir un état des lieux et d'analyser l'évolution des modèles et stratégies économiques des acteurs (Apple, Google, Amazon, SFR, Nokia etc.). Ces technologies et stratégies sont simultanément évaluées en termes de sécurité et évaluation des risques. Puis, à la lumière de ces informations, une analyse de la régulation existante et de ses possibles évolutions sera faite afin d'aboutir à 4 ou 5 scénarii de régulation pour les smartphones, d'ici 5 à 10 ans. Les résultats de ces travaux devraient être disponibles au printemps 2012.

Le chantier « vie privée 2020 »

Ce travail ambitieux est relatif à « *la vie privée, les libertés et les données personnelles à l'horizon 2020. Quels enjeux pour la régulation et la CNIL ?* ». Pour conduire ce chantier stratégique pour l'institution, la CNIL a choisi une démarche résolument ouverte. Elle consiste à interroger des experts et acteurs relevant de différents domaines : économistes, sociologues, historiens, philosophes, représentants d'instituts de recherches, du monde associatif, *think tanks*, acteurs économiques, etc. L'objectif de ces entretiens est de recueillir leur perception des évolutions futures dans le champ de la vie privée, des libertés et des données personnelles. Il s'agit aussi de connaître leur lecture des formes de régulation à venir et du rôle de la CNIL demain. C'est aussi l'occasion pour la Commission de renforcer sa visibilité auprès de certains acteurs et de développer un réseau d'experts dans le monde académique, prélude d'un *think tank* de prospective « Informatique et Libertés ».

Lancés en septembre 2011, ces travaux conduits sous la forme d'une trentaine d'entretiens semi-directifs feront l'objet d'une restitution globale et devraient donner lieu, courant 2012, à un séminaire de réflexion.

Enfin, la Commission a décidé la mise en place d'un comité de la prospective qui verra le jour en 2012. Organe consultatif de conseil, placé auprès de la direction des études, de l'innovation et de la prospective (DEIP) il sera notamment chargé d'émettre un avis sur le programme d'études de la DEIP et contribuera à l'évaluation des résultats de ces études. Comité mixte, il sera composé de deux commissaires et de six experts extérieurs, compétents notamment dans les domaines de l'économie et de la sociologie.

LA LETTRE IP

La lettre d'information IP pour « Innovation et Prospective », a été créée en septembre 2011. Conçue par la direction de la prospective de la CNIL, diffusée en version électronique et papier, cette newsletter, trimestrielle, a vocation à informer un large réseau d'experts, de parties prenantes et d'interlocuteurs de tous horizons qui s'intéressent aux questions liées aux technologies, aux usages et à la vie privée. C'est une manière de nourrir la réflexion prospective sur le débat et la réflexion sur les enjeux prospectifs en matière de protection des données personnelles et de la vie privée et d'échanger avec ces experts et acteurs.

D'autres publications seront accessibles progressivement, notamment sur le site de la CNIL. Ainsi, la DEIP prévoit de publier des « cahiers de la prospective », rendant compte des résultats de ses chantiers et travaux.

Par ailleurs, la veille prospective interne a été fortement développée. Une base documentaire de veille sur les thématiques prospectives intéressant la protection des données personnelles est en cours de constitution. Une rubrique prospective, créée sur le réseau intranet de l'institution, permet de diffuser des notes d'alerte et d'analyse.

À cet égard, la CNIL devrait être dotée d'ici la fin de l'année 2012 d'un nouveau système d'information documentaire permettant ainsi la mise en place d'une nouvelle politique de gestion de la connaissance, indispensable à la veille prospective.

PARTENARIATS ET COOPÉRATION

Au cours de l'année 2011, la CNIL a développé des actions de coopération avec le monde de la recherche et de l'enseignement et engagé à cet effet plusieurs partenariats. C'est une façon pour la CNIL d'être plus au cœur des process d'innovation et de recherche. Il s'agit aussi d'être plus à l'écoute des chercheurs et des entreprises et de mieux comprendre leurs préoccupations et besoins.

La Commission a renforcé sa coopération avec l'ANR au travers de plusieurs actions :

▸ **La participation à des comités de pilotage de programmes de recherche.**
La direction de la prospective participe aux comités de pilotage du :

- programme « Concepts systèmes et outils pour la sécurité globale » ;
- programme de recherche interdisciplinaire en sécurité ;
- programme « contenus et interactions (CONTINT) qui a pour objet de financer des projets innovants en matière de contenus numériques pour tous types de médias (cinéma, web, contenus personnels,…) et en matière robotique.

Outre l'intérêt de mieux faire connaître la CNIL dans le monde de la recherche, cette participation présente l'avantage d'identifier les projets porteurs d'enjeux en termes de protection des données, de faire intégrer le plus en amont possible la réflexion éthique en la matière et de permettre ensuite un accompagnement « Informatique et Libertés » des projets.

▸ Par ailleurs, **elle fait partie d'un comité de revue de l'ANR pour un projet de recherche multidisciplinaire intéressant l'usage des données sur internet**.

La CNIL s'est engagée dans un partenariat avec l'INRIA qui s'est traduit d'abord par la signature en juillet 2011 d'une convention, puis par le lancement conjoint fin 2011 d'un projet de recherche à visée pédagogique : le projet **Mobilitics**. Ce projet vise à comprendre et expliquer les risques pour la vie privée liée à l'utilisation des smartphones par une analyse en profondeur des données enregistrées, stockées et diffusées par ces appareils. Les premiers résultats devraient être disponibles au printemps 2012.

Une convention de partenariat entre la CNIL et la Conférence des Grandes écoles (CGE) a été signée en décembre 2011. Elle a notamment pour objet de sensibiliser élèves, corps enseignant et personnels administratifs à nos problématiques par différentes actions de communication, de développer les CIL et d'envisager des projets de recherche en commun.

Par ailleurs, d'autres actions de coopération sont actuellement en cours ou envisagées, selon des modalités différentes, avec certaines grandes écoles sur des projets de recherche précis.

Enfin, des partenariats ponctuels ont été noués tel celui conclu avec l'UNAF en partenariat avec Action Innocence sur la réalisation du sondage lancé en juin 2011 sur l'usage des réseaux sociaux chez les jeunes *(voir chapitre 2)*.

FOCUS

Le Prix de thèse « Informatique et Libertés »

Le Prix de thèse « Informatique et Libertés » reconnaît la valeur de certains travaux et incite donc au développement des recherches universitaires concernant la protection de la vie privée et des données personnelles.
Ce prix s'adresse à de très nombreuses disciplines telles que les sciences humaines, le droit, les sciences politiques, l'économie mais aussi les disciplines techniques. Un montant de 7 000 euros est alloué au lauréat afin de faciliter la publication de sa thèse.
Le jury, présidé par Jean-Marie COTTERET, membre de la CNIL, a décerné le prix de thèse 2011 à Monsieur Jean-Raphaël DEMARCHI, Chercheur au Centre d'Études et de Recherches en Droit Privé (CERDP) et Maître de conférences à l'Université de Nice-Sophia Antipolis, pour sa thèse intitulée « La preuve scientifique et le procès pénal ». Ses travaux feront très prochainement l'objet d'une publication.

LE LABORATOIRE

La CNIL a souhaité créer, en son sein, un laboratoire, doté de moyens informatiques dédiés, pour tester et expérimenter des produits et applications innovantes ; Il s'agit ainsi de :

- disposer des nouveaux produits le plus en amont possible de leur commercialisation ou récemment mis sur le marché afin de tester leurs fonctionnalités, et d'évaluer leurs impacts sur la protection de la vie privée ;
- diffuser une culture technologique et une pédagogie des usages en développant des outils à destination du grand public pour mieux protéger la vie privée et tester la faisabilité de solutions nouvelles protectrices de la vie privée ;
- renforcer la mission de conseil auprès des entreprises en matière d'intégration des exigences de protection des données personnelles dans leur processus de développement technologique dans une logique de *privacy by design* ;
- contribuer au développement de solutions technologiques protectrices de la vie privée ;

> La CNIL doit comprendre et accompagner l'innovation technologique, sociale et juridique

- renforcer la crédibilité technique et la capacité d'influence de la CNIL, notamment dans les communautés techniques et scientifiques ;
- réaliser des analyses techniques poussées sur des sujets précis à des fins par exemple de publication dans des revues spécialisées. ■

FOCUS

Labo : des investigations techniques... et des expérimentations

Le « labo » installé et piloté conjointement par la Direction des études, de l'Innovation et de la Prospective et le Service de l'Expertise s'est mis progressivement en place en 2011. Dès l'installation d'une plateforme technique, le labo a commencé à multiplier des investigations techniques et des analyses telles que celle réalisée sur la question de la transmission d'informations de géolocalisation par les iPhones (voir p 58). Dans ce cas précis, un iPhone 3Gs a été « mis sous surveillance » afin d'en tirer un certain nombre de conclusions sur les données transmises.

Le laboratoire a mené des analyses rapides lorsque les médias se sont fait l'écho de la découverte du logiciel dit « Carrier IQ », intégré par des fabricants de smartphones à la demande des opérateurs américains. Le matériel du laboratoire a permis de vérifier si des traces de ce logiciel étaient visibles sur des appareils français ou non. La CNIL a constaté qu'aucune trace du logiciel en question n'était présente sur les appareils android OS du laboratoire, et que si une trace semblait présente sur des appareils Apple iOS, le logiciel y semblait inactif dès le départ.

De telles investigations vont se multiplier à l'avenir, afin de réagir très rapidement aux nouveaux produits et services.

Dans le même temps, le laboratoire va prendre plus d'ampleur, à la fois du point de vue technique par la mise en place de projets plus lourds, en particulier dans le cadre du partenariat avec INRIA.

Progressivement, le laboratoire va élargir ses travaux pour aller vers des expérimentations, des essais et des développements d'outils. Le laboratoire pourra alors élargir ses activités pour porter les actions innovantes et expérimentales de la CNIL et cela en tout domaine.

GROS PLAN

SMARTPHONE ET VIE PRIVÉE, UNE PRIORITÉ D'ANALYSE ET D'ACTION POUR LA CNIL

19 millions
DE MOBINAUTES EN FRANCE

48 %
UTILISENT LEUR SMARTPHONE POUR UN RÉSEAU SOCIAL

> 65 % des mobinautes estiment que leurs données ne sont pas bien protégées ”

La CNIL a choisi l'analyse prospective et l'expérimentation concrète d'outils afin d'étudier dans la durée les enjeux de données personnelles liés à ces compagnons numériques mobiles qui ne nous quittent plus. Ces derniers sont devenus en quelques années l'interface principale de la « communication nomade permanente » et le centre nerveux de la vie numérique d'utilisateurs connectés partout et tout le temps. Or, le smartphone reste une « boîte noire » pour son propriétaire.

Une utilisation des données personnelles opaques

L'inquiétude monte autour de l'impression – largement justifiée – qu'ont les utilisateurs d'être incapables d'avoir une idée claire sur les enregistrements, stockage et « fuites » vers l'extérieur de données personnelles liées à l'utilisation des fonctions, services et applications disponibles. La quantité de données susceptibles d'être ainsi diffusées est considérable et va du carnet de contacts, à la géolocalisation, en passant par toutes sortes de données d'identification.

Cette situation n'est acceptable ni pour les utilisateurs ni pour la CNIL. Elle n'est pas non plus soutenable dans la durée pour les acteurs économiques. Des améliorations devront avoir lieu dans ce domaine, au risque de scandales et polémiques à répétition. La CNIL veut donc renforcer son rôle de prescripteur de « bonnes pratiques », en coopérant avec les acteurs économiques et au profit de la protection des droits des utilisateurs. Dans cette optique plusieurs initiatives ont été lancées durant le second semestre 2011. Elles ont permis de mieux comprendre les enjeux autour des smartphones et de poser les bases d'un plan d'action 2012 centré en particulier sur les actions de son laboratoire.

▸▸▸

UN SONDAGE POUR MIEUX COMPRENDRE LA FRANCE DU SMARTPHONE

À la demande de la CNIL, l'institut Médiamétrie a, entre le 4 et 14 novembre 2011, interrogé par internet 2 315 personnes dont un échantillon spécifique de 198 individus âgés de 15 à 17 ans[1]. Les objectifs de ce sondage étaient de :

- déterminer les types de smartphones utilisés par les Français, et les usages réalisés au quotidien ;
- mesurer la perception des utilisateurs de smartphones sur les contenus et les données personnelles stockées sur leur téléphone ;
- décrire et comprendre les risques perçus par l'utilisateur, et les protections mises en place ;
- proposer des conseils pratiques aux utilisateurs de smartphones.

Les principaux résultats, présentés à la presse le 12 décembre 2011, sont également disponibles sur le site de la CNIL.

Le smartphone : un compagnon de tous les instants

La population équipée est certes encore spécifique (plus masculine, plus CSP+, plus citadine…), mais cette différence s'estompe rapidement avec la démocratisation des appareils : selon l'institut GFK, 11,4 millions de Smartphones ont été vendus en 2011, et selon Médiamétrie il y avait fin 2011 19 millions de mobinautes en France.

Le sondage permet cependant d'identifier des différences de perception de la place du smartphone en fonction des âges : simple téléphone « avancé » pour les 50 ans et + (« outil de communication » à 35 %), il est un terminal indispensable du jeune *always on* (« outil de connexion permanente » pour 30 % des 15-17 ans).

Si les jeunes ont des usages spécifiques (jeux, réseaux sociaux, messagerie instantanée), l'offre de services est tellement large que chaque profil y trouve ses usages intensifs (exemple pour les 50 ans et plus : gestion de données médicales). Ainsi, ce sont 48 % des possesseurs de smartphones l'utilisent pour un réseau social (69 % des 15-17 ans), et 67 % de ceux qui le font tous les jours. Ce sondage montre qu'au fur et à mesure que l'outil est apprivoisé, les usages se densifient : les personnes interrogées équipées d'un smartphone depuis plus de 2 ans sont ainsi plus nombreuses à consulter leur compte bancaire. L'appétit pour les applications très intensives en données personnelles semble fort et croit avec la confiance.

Au départ, le smartphone a été un outil professionnel : l'image classique était alors celle de l'homme d'affaires ou du cadre équipé de son « blackberry ». Ce n'est plus du tout le cas aujourd'hui. En effet 74 % des personnes dotées d'un smartphone utilisent leur téléphone à titre avant tout personnel. On assiste même à un renversement de tendance : ces appareils personnels sont si importants, si pratiques et si utiles que les individus veulent pouvoir l'utiliser dans le cadre professionnel, éventuellement avec une contrepartie. Les entreprises sont obligées de s'adapter à cette demande, dans le cadre de ce que l'on appelle le BYOD, pour *bring your own device* (« apportez votre appareil ») : les entreprises cherchent à fournir des solutions et applications professionnelles utilisables sur un appareil personnel. Notre sondage montre ainsi que 56 % des personnes ont une utilisation partiellement professionnelle de leur smartphone principal[2], et que 36 % des CSP+ disent avoir un usage « autant professionnel que personnel » (21 % de la population générale) *(voir graphique ci-contre).*

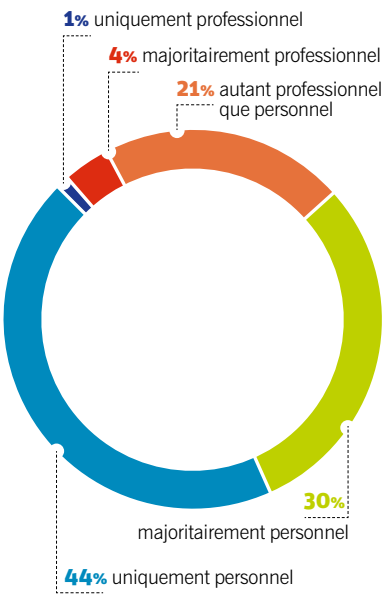
Une utilisation des données personnelles opaque

La conscience de la présence de données personnelles sur les smartphones est largement partagée. Le sondage ne montre ni décalage majeur entre les perceptions intuitives des utilisateurs et la réalité des informations enregistrées, ni réelle négligence vis-à-vis des données personnelles. Cependant, il convient de relever que 15 % des personnes interrogées déclarent ne stocker aucune information personnelle, ce qui est impossible dans les faits. Cela dénote pour cette partie de la population (ce chiffre est plus fort chez les plus de 50 ans et les personnes équipées d'un smartphone depuis moins de 6 mois) une faible connaissance des enjeux liés à ces informations et à l'usage de ces appareils.

En revanche, l'opacité règne en tout cas sur les « sorties » ou « fuites » de données personnelles (diffusion vers l'opérateur, le fabricant, les éditeurs d'application ou vers des tiers). En effet, la moitié des personnes interrogées pensent que leurs données ne peuvent pas être transmises sans leur accord préalable,

Quel type d'usage faites-vous du téléphone mobile que vous utilisez le plus souvent ?

Base : ensemble des équipés smartphone de 18 ans et plus (2 117 rép.)



l'autre moitié des répondants pensant que cela est possible. Dans toutes les questions de ce type, les individus expriment en tout cas à la fois leur méconnaissance et leur souhait de mieux comprendre ce qui peut être fait en termes de stockage et transmission de données personnelles par des applications ou services mobiles. Cette tension est particulièrement flagrante en ce qui concerne la géolocalisation, qui est bel et bien une nouvelle donnée sensible.

Par ailleurs, un manque de clarté persiste dans l'esprit des utilisateurs quant à ce que les acteurs économiques font de leurs données et quant à leurs droits : ils sont 51 % à penser que leurs données ne peuvent être enregistrées ou transmises sans leur accord, ce qui témoigne d'une méconnaissance de la réalité.

Le monde des applications *(apps)* qui devient le quotidien des utilisateurs de smartphones renforce encore cette opacité : les *apps* sont en effet omniprésentes… et parfois trop curieuses ! 63 % des individus qui ont déjà téléchargé une application ont d'ailleurs déjà refusé d'en installer une à cause des conditions d'utilisation. Et ce chiffre augmenterait si les utilisateurs savaient réellement ce qu'ils autorisent (les autorisations étant parfois rédigées dans des termes insuffisamment explicites). De nombreuses études, dont celles réalisée par le *Wall Street Journal* à partir des applications les plus populaires sur smartphones aux États-Unis (par exemple *What they know – mobile*)[4], montrent que beaucoup de données personnelles sont aujourd'hui transmises à l'insu des utilisateurs. Cette méconnaissance est en partie due au fait que les conditions d'utilisation des services et applications, peu lisibles et compréhensibles, sont rarement lues (71 % ne les lisent pas systématiquement), mais est surtout due au fait que les acteurs ne font pas œuvre de transparence en ce domaine.

▸▸▸

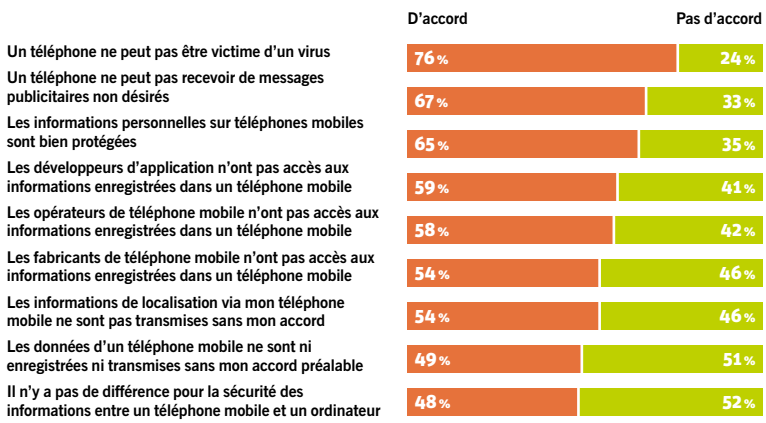
FOCUS

La géolocalisation : nouvelle donnée sensible ?

L'usage des services de géolocalisation est probablement la fonction qui se répand actuellement le plus rapidement. Plus de 55 % des possesseurs de smartphone utilisent des services de géolocalisation : bien sûr, la recherche d'itinéraire ou de plan, mais aussi très largement le repérage de lieux autour de soi, ou la recherche de recommandations sur des lieux. Le fait d'indiquer sa présence en un lieu ou de vérifier la localisation de ses proches est encore très minoritaire, mais concerne d'ores et déjà entre 10 et 25 % des utilisateurs des services de géolocalisation.
La réaction des personnes interrogées est sans équivoque : plus de 90 % des répondants souhaitent sélectionner les moments où ils sont localisés, contrôler à qui la localisation est communiquée, savoir comment ces données sont utilisées et pouvoir refuser la transmission.
Ces résultats sont cohérents avec le focus réalisés par le CREDOC dans la dernière livraison en octobre 2011 de son étude sur la « diffusion des TIC dans la société française »[4]. Selon cette étude, 81 % des possesseurs d'un téléphone mobile souhaiteraient avoir la possibilité d'interdire la transmission de leur localisation à des entreprises commerciales.
Le CREDOC ajoute d'ailleurs que « le plus intéressant est sans doute le changement intervenu auprès des plus jeunes : relativement sereins en 2008, ils sont désormais 75 % à vouloir mettre un véto à la transmission de données de géolocalisation à des tiers (+ 21 points en trois ans, la plus forte progression) ». La géolocalisation doit probablement être considérée comme une nouvelle donnée sensible, utilisable et diffusable par les acteurs économiques dans un cadre de régulation cohérent avec les attentes, fortes, des individus.

Quel est votre degré d'accord avec les affirmations suivantes ?

Base : ensemble des équipés smartphone de 15 ans et plus (2 315 rép.)



[1] Pour cette cible, les réponses ont été recueillies avec l'accord des parents. / [2] Une minorité d'entre eux ayant certes probablement pour téléphone principal un téléphone fourni et financé par l'entreprise, mais le cas reste minoritaire. Ainsi, seul 25 % des cadres disposent d'un smartphone fourni par l'entreprise selon le dernier baromètre du stress des cadres Opinion Way pour la CFE CGC (Mai 2011). / [3] Source : CREDOC - La diffusion des TIC dans la société française - (2011). / [4] http://blogs.wsj.com/wtk-mobile/

40 % des personnes stockent des données à caractère secret

LES
15-17 ANS,
UN EXEMPLE
À SUIVRE ?

30%
DÉCLARENT N'AVOIR AUCUN CODE DE PROTECTION

65%
DES PARENTS D'ENFANTS DE MOINS DE 18 ANS UTILISERAIENT LA FONCTION DE LOCALISATION DE LEURS ENFANTS

Le smartphone, une boîte noire que l'on ne sait pas protéger

Les possesseurs de smartphone négligent, probablement par ignorance technique ou pour des questions de commodité, les protections. Ainsi, **plus d'un quart des répondants affirment n'avoir aucun code de verrouillage**. Dans le même temps, nouveau *privacy paradox*, ils sont pourtant 65 % à estimer que leurs données ne sont pas bien protégées.

Le sondage montre aussi très clairement que les possesseurs de smartphones n'ont pas tous la même perception à la fois des protections mises en œuvre et des risques encourus. Très peu sont réellement « confiants », moins d'un quart peuvent être en quelque sorte qualifiés de « paranos », mais les deux grandes « familles » de smartphoneurs français qui ressortent de l'étude sont bels et bien des nonchalants (28 %) et des insouciants (34 %) qui ne s'intéressent pas réellement à la protection de leurs données sur smartphone, car cela ne leur parait pas important soit parce qu'ils ne souhaitent pas y consacrer d'efforts, soit car ils ne pensent pas que le risque associé soit important[1].

Qui plus est, plusieurs résultats du sondage montrent **des 15-17 ans « relativement » prudents**. En effet, ils utilisent plus de codes de verrouillage que la moyenne, et sont plus méfiants vis-à-vis des données enregistrées. Comment expliquer ce résultat ? Tout d'abord, le smartphone est souvent l'objet le plus précieux qu'ils possèdent « en propre ». Qui plus est, ils cherchent probablement avant tout à limiter la surveillance des parents. Enfin, leur « expérience d'utilisateur » est dense et multiforme, elle leur sert donc d'apprentissage et d'acculturation au numérique. Ce sondage ne fait que confirmer que les plus jeunes ne consomment plus de l'internet « comme avant » et que le rôle des parents dans l'éducation numérique ne peut être uniquement une affaire de contrôle technique (par des logiciels de contrôle parental par exemple) ou de gestion du temps de connexion. Pourtant, le sondage révèle qu'à la question : **« Pourriez-vous utiliser la fonction de localisation de vos enfants si celle-ci était accessible simplement ? », 65 % des parents d'enfants de moins de 18 ans répondent oui**. Il faut, à côté de la surveillance de leurs enfants, que les parents jouent pleinement leur rôle d'éducation numérique et parlent des usages réels et concrètement avec leurs enfants. D'autant que l'étude montre qu'ils peuvent eux-mêmes en retirer des leçons quant à leur propre pratique !

> 30 % des équipés smartphones identifient la CNIL comme un acteur pour informer sur la sécurisation

PLAN D'ACTION 2012

La CNIL a commencé à tirer des résultats du sondage un certain nombre de conseils aux utilisateurs.

Ces conseils ont ensuite été illustrés dans un tutoriel vidéo, disponible sur le site de la CNIL.

Forte de ce constat, la CNIL compte elle-même développer des projets et outils permettant de mieux saisir cette « économie cachée » des données personnelles sur smartphones, et ce en particulier en mobilisant son nouveau laboratoire.

La CNIL va donc dans les mois qui viennent recenser les bonnes pratiques des acteurs en termes d'information et de maîtrise des données personnelles par l'utilisateur. La question est d'importance pour l'ensemble de l'écosystème économique du mobile, comme le montrent les initiatives prises par le GSMA (l'organisme international de défense des intérêts des opérateurs et acteurs du mobile) autour de « *mobile and privacy*[2] » depuis 2011 (définition de principes et de lignes directrices de design) ainsi que les récentes polémiques autour des accès illégitimes d'applications à des données à caractère personnel (par exemple le carnet de contacts).

Le programme annuel de contrôle de la CNIL prendra également en compte cette priorité liée à l'écosystème des smartphones. ■

10 conseils aux utilisateurs

1. **N'enregistrez pas d'informations confidentielles (codes secrets, codes d'accès, coordonnées bancaires…) dans votre smartphone (vol, piratage, usurpation d'identité…).**
2. **Ne désactivez pas le code PIN et changez celui proposé par défaut. Choisissez un code compliqué. Pas votre date de naissance !**
3. **Mettez en place un délai de verrouillage automatique du téléphone. En plus du code PIN, il permet de rendre inactif (verrouiller) le téléphone au bout d'un certain temps. Cela empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol.**
4. **Activez si possible le chiffrement des sauvegardes du téléphone. Pour cela, utilisez les réglages de la plate-forme avec laquelle vous connectez le téléphone. Cette manipulation garantira que personne ne sera en mesure d'utiliser vos données sans le mot de passe que vous avez défini.**
5. **Installez un antivirus ou une solution de sécurité quand cela est possible… en vous informant sur leur efficacité.**
6. **Notez le numéro « IMEI » du téléphone pour le bloquer en cas de perte ou de vol.**
7. **Ne téléchargez pas d'application de sources inconnues. Privilégiez les plateformes officielles.**
8. **Vérifiez à quelles données contenues dans votre smartphone l'application que vous installez va avoir accès.**
9. **Lisez les conditions d'utilisation d'un service avant de l'installer. Les avis des autres utilisateurs peuvent également être utiles !**
10. **Réglez les paramètres au sein du téléphone ou dans les applications de géolocalisation (Twitter, Foursquare,…) afin de toujours contrôler quand et par qui vous voulez être géolocalisé. Désactivez le GPS ou le WiFI quand vous ne vous servez plus d'une application de géolocalisation.**

[1] Pour en savoir plus sur cette typologie, consulter la 2ème lettre « innovation et prospective » de la DEIP, disponible sur www.cnil.fr/ip. / [2] www.gsma.com/mobile-and-privacy/

2. INFORMER

La CNIL vous informe au quotidien

GROS PLAN
Réseaux sociaux : quelles sont les pratiques de nos enfants ? Quel peut être le rôle des parents ?

Les réponses au public

Les correspondants

LA CNIL VOUS INFORME AU QUOTIDIEN

La CNIL est investie d'une mission générale d'information des personnes des 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 en même temps s'informer.

PARTENARIAT FRANCE INFO

Ce partenariat débuté en 2007 a été renouvelé en 2011. 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 : les caméras dans les écoles, les achats depuis un smartphone, le *cloud computing*, la reconnaissance faciale, les commentaires sur des salariés, le *phishing*, etc.

Chaque vendredi, la CNIL intervient sur France Info

SENSIBILISER AUX BONNES PRATIQUES SUR INTERNET

Dans la continuité des actions menées les années précédentes auprès des élèves et du personnel enseignant de primaire et du collège, la CNIL a poursuivi en 2011 son engagement pour sensibiliser les jeunes aux bonnes pratiques sur Internet.

En juin 2011, elle a ainsi investi l'univers des communautés virtuelles, en créant une opération spéciale sur Habbo Hotel, le site de « Social Game » des 13-18 ans[1]. L'objectif était de s'adresser directement aux enfants et adolescents, à travers une plate-forme qu'ils utilisent quotidiennement. L'opération consistait en différentes activités (concours vidéo, quiz, chat…) permettant de faire découvrir aux jeunes

[1] *www.habbo.fr/ Habbo est un site de « Social Game » pour les 13-18 ans. Il s'agit d'une communauté virtuelle dans laquelle les membres peuvent discuter, se rendre visite, visiter leurs appartements, acheter des objets pour meubler leurs appartements, habiller leurs avatars ou encore faire des échanges d'objets. Créé en Finlande en 2000, Habbo est le 2ème réseau social dans le monde après Facebook. Le site est présent dans 37 pays et compte 200 millions de membres. L'âge moyen est de 14,4 ans (78 % de 13-18 ans).*

80

VIDÉOS ONT ÉTÉ RÉALISÉES DANS LE CADRE DU CONCOURS SUR HABBO

Le Tutoriel CNIL #1 Créer des listes d'amis sur Facebook[4].

de manière ludique les conseils et astuces de la CNIL pour mieux protéger leur vie privée sur Internet. Les membres de la communauté Habbo ont par exemple été invités à exprimer leur créativité en réalisant des vidéos illustrant les principaux conseils de la CNIL.

Les thèmes des vidéos étaient les suivants : « Réfléchis avant de publier ! », « Attention aux photos ! », « Sécurise tes comptes ! ». Les vidéos des gagnants du concours ont été mises en ligne sur le site Jeunes et sur le compte Dailymotion de la CNIL[2]. Un quiz spécial « Internet et Vie privée » permettait également aux membres de gagner des badges et des vignettes Habbo exclusives à s'échanger. Cette opération a été un succès. Elle a généré 2 000 clics vers le site jeunes de la CNIL, 80 vidéos ont été reçues dans le cadre du concours et certaines ont dépassé les 1 000 vues sur Youtube. Enfin, 3 356 personnes ont répondu au quiz.

En investissant pour la première fois un réseau virtuel dédié aux jeunes, la CNIL a montré qu'elle était un acteur majeur de l'univers numérique et qu'elle pouvait s'associer aux entreprises du web pour promouvoir un internet maîtrisé et respectueux des valeurs essentielles que sont l'identité et l'intimité.

La CNIL s'est ensuite adressée aux collégiens ainsi qu'à leurs enseignants en leur envoyant un numéro spécial de l'actu, le journal des 14-18 ans, consacré à la géolocalisation. En effet, ces dernières années, la géolocalisation a connu un développement considérable. Avec le développement des smartphones on assiste à une multiplication des applications dans tous les usages de la vie quotidienne. Pourtant, 72 % des français pensent que la diffusion sur Internet de la localisation en temps réel est risquée[3]. La CNIL considère qu'il est indispensable de faire prendre conscience aux futurs citoyens de demain, des incidences de la géolocalisation sur leur vie privée.
Ce numéro spécial a été envoyé aux 20 000 enseignants d'histoire-géographie, souvent en charge de l'enseignement de l'instruction civique, des classes de 4ème ainsi qu'à tous les CDI (centres de documentation et d'information) des collèges de France. Il permet aux enseignants d'engager un dialogue avec les élèves sur la géolocalisation et ses enjeux : « La géolocalisation sur mobile : état des lieux » ; « Qu'est-ce que la réalité augmentée ? » ; « Géolocalisation et publicité » ; « Le droit d'aller et venir librement »…

LES TUTORIELS VIDÉO

Il peut être est parfois difficile pour un internaute de s'y retrouver dans le paramétrage de ses comptes. La CNIL a souhaité montrer de manière pédagogique comment maîtriser les informations publiées sur les réseaux sociaux. Pour cela, elle a réalisé un tutoriel vidéo, présentant comment créer des listes d'amis sur le réseau Facebook. Facebook permet en effet de répartir ses contacts dans des listes correspondant aux membres de sa famille, à ses amis proches, à ses collègues… puis d'adopter les paramètres de confidentialité en fonction des informations que l'on souhaite partager avec chaque catégorie de personnes. Ce tutoriel montre, étape par étape, comment créer des listes d'amis.

[2] www.jeunes.cnil.fr/internet-vie-privee/la-cnil-sur-habbo/ et www.dailymotion.com/cnil. / [3] Source: Observatoire sociétal du téléphone mobile, 6e édition, Afom/TNS Sofres. (2010). / [4] www.dailymotion.com/video/xg5ulc_tutoriel-cnil-1-creer-des-listes-d-amis-sur-facebook_tech#from=embed

LES PUBLICATIONS À L'ATTENTION DES PROFESSIONNELS

En 2011 la CNIL a publié deux nouveaux guides.

Dans le cadre d'une convention de partenariat conclue avec le Conseil National des Barreaux, la CNIL a publié un guide pratique à destination des avocats. Ce guide apporte des réponses concrètes aux questions que les avocats peuvent se poser quant à l'application de la loi « Informatique et Libertés », que ce soit en qualité de responsable de traitement ou de conseil auprès de leurs clients. Il a été distribué aux participants de la Convention Nationale des Avocats en octobre 2011.

À l'heure du développement de l'informatisation des dossiers médicaux et des échanges dématérialisés de données de santé, la CNIL met à disposition des acteurs de santé un guide pratique. Il les informe sur les mesures à adopter pour gérer leurs fichiers dans le respect de la loi « Informatique et Libertés ». Ce guide donne également des conseils pour mettre en place des mesures permettant de respecter l'intégrité et la sécurité des données de santé et garantir les droits des patients. Ce guide a été adressé à l'ensemble des établissements de santé.

LE SITE INTERNET WWW.CNIL.FR

Version mobile de cnil.fr

En 2011, **212 actualités** ont été publiées sur le site. Depuis janvier 2011, la version anglaise est désormais enrichie mensuellement d'une nouvelle actualité. La lettre Infocnil comptait 36 661 abonnés fin 2011 (contre 33 000 en 2010).

En décembre 2011 à l'occasion de la présentation du sondage « smartphones et vie privée », la CNIL a mis en ligne une version mobile de son site internet. Il permet d'accéder à l'ensemble de l'actualité, des fiches pratiques actualités et des questions réponses dans une version optimisée pour la lecture sur mobile.

La nouvelle démo des traces

Destinée à sensibiliser les internautes à la problématique des traces de navigation qu'ils laissent à leur insu, la rubrique vos traces existe depuis la première version du site de la CNIL. En juin 2011, elle a été entièrement repensée et enrichie de nouvelles démonstrations. La rubrique propose d'expérimenter, à travers cinq démonstrations, quelques-unes des techniques mises en œuvre par les différents acteurs du web : géolocalisation vie l'adresse IP, cookies et flash cookies, historique des sites visités, publicité ciblée.

36 661
ABONNÉS À LA LETTRE INFOCNIL

LES RÉSEAUX SOCIAUX

En 2011, la CNIL a confirmé sa présence sur les réseaux sociaux Facebook, Twitter, Dailymotion et les réseaux professionnels Viadéo et LinkedIn. Avec maintenant 11 600 abonnés sur Twitter et 3 223 fans sur Facebook, ces nouveaux canaux de communication prennent de l'importance dans la diffusion des messages de l'institution. La CNIL arrive en cinquième position dans le classement des institutions françaises sur Twitter, effectué par l'agence de communication La Netscouade[1].

11 600

ABONNÉS SUR TWITTER

L'IMAGE DE LA CNIL

Depuis 2004, la CNIL mesure sa notoriété ainsi que la connaissance qu'ont les personnes de leurs droits « Informatique et Libertés ». 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 23 au 28 novembre 2011.

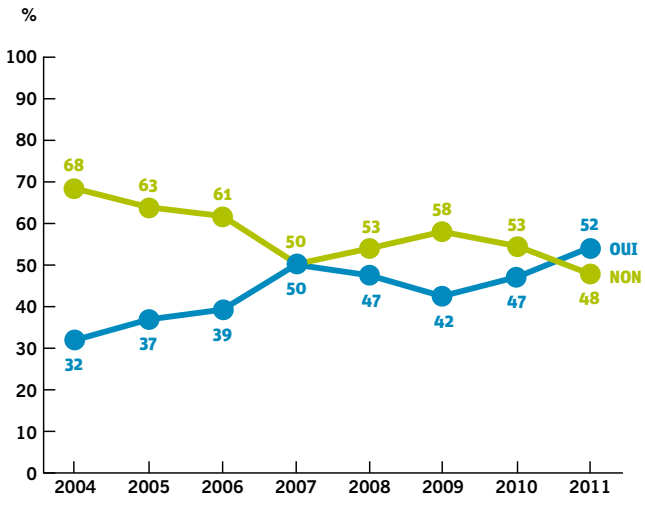
52 % des personnes connaissent la CNIL contre 32 % en 2004 et 47 % en 2010. C'est la première fois que la notoriété de la CNIL franchit la barre des 50%.

37 % des personnes ont le sentiment d'être suffisamment informées à propos de leurs droits en matière de protection des informations personnelles contre 21 % en 2004 et 34 % en 2010. ■

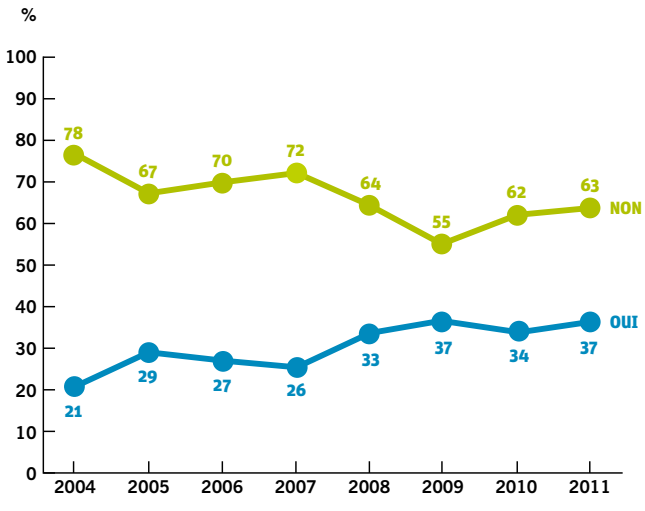
52 %

DES PERSONNES CONNAISSENT LA CNIL

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



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



[1] *www.lanetscouade.com/fr/article/le-top-20-des-institutions-francaises-sur-twitter*

GROS PLAN

RÉSEAUX SOCIAUX : QUELLES SONT LES PRATIQUES DE NOS ENFANTS ? QUEL PEUT ÊTRE LE RÔLE DES PARENTS ?

18 % DES MOINS DE 13 ANS ONT UN COMPTE

33 % DES MOINS DE 13 ANS N'UTILISENT PAS LES PARAMÈTRES DE CONFIDENTIALITÉ

> "60 % des moins de 18 ans sont présents sur les réseaux sociaux"

Les moins de 18 ans sont massivement présents sur les réseaux sociaux, en particulier sur Facebook (au moins 60 % s'y connectent quotidiennement). Mais qu'y font-ils ? Qu'échangent-ils ? Avec qui ? Leurs pratiques sont-elles toujours « amicales » ? Se sentent-ils protégés ? Quelle place ont pris les réseaux sociaux dans leur vie et celle de leur famille ?

Pour répondre à ces questions et aider les parents à jouer leur rôle éducatif, l'UNAF, Action Innocence et la CNIL ont demandé en juin 2011 à TNS SOFRES de réaliser une étude auprès de 1 200 jeunes. Ce sondage a été effectué par téléphone du 10 au 17 juin 2011 auprès d'un échantillon national représentatif d'enfants et adolescents âgés de 8 à 17 ans.

Les résultats de cette étude ont permis l'élaboration de conseils destinés aux parents et la diffusion d'une plaquette d'information.

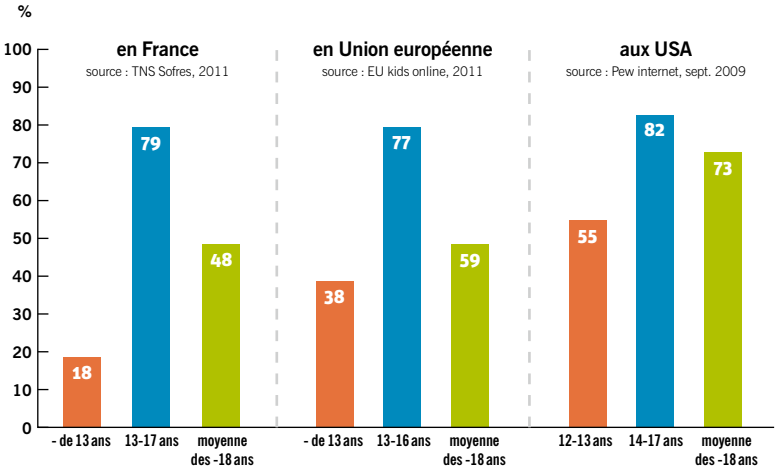
LES PRINCIPAUX CONSTATS DU SONDAGE

Quels sont les constats les plus significatifs ? Les résultats de cette étude montrent-ils une spécificité française dans ce domaine ? Afin de répondre à ces questions, la Direction des Études, de l'Innovation et de la Prospective (DEIP) a analysé et comparé ces résultats à ceux d'une étude européenne réalisée en 2011 par IPSOS[1]. Des différences entre pays existent.

Près de 20 % des moins de 13 ans ont un compte

Si, sans surprise, près de la moitié (48 %) des enfants français de 8-17 ans sont connectés à un réseau social (Facebook), - ce qui est légèrement moins que la moyenne européenne - 18 % des moins de 13 ans sont déjà connectés, et ce malgré l'interdiction - théorique - de s'y connecter avant 13 ans. Mais la France est en fait le pays d'Europe dans lequel les moins de 13 ans sont le moins présents sur les réseaux sociaux : ainsi, aux Pays-Bas, 70 % des 9-12 ans sont sur un réseau social, et la moyenne européenne s'établit à 38 %. À titre de comparaison, selon des chiffres datant de fin 2009, 55 % des 12-13 ans américains étaient membres d'un réseau social[2] *(voir graphique)*.

Pourcentage de mineurs membres d'au moins un réseau social par tranche d'âge



Les enfants et les adolescents livrent leurs identités et beaucoup d'informations personnelles

Pour les enfants et les adolescents, la relation sur le réseau n'est pas virtuelle. Ils sont dans la vraie vie : 92 % utilisent ainsi leur vraie identité et livrent beaucoup d'informations personnelles. Leurs activités sont notamment les commentaires et la publication de photos (surtout pour les filles à 88 %).

Le réseau d'amis est souvent large et ouvert, parfois à des inconnus : les jeunes interrogés ont en moyenne 210 « amis » (un chiffre qui augmente avec l'âge), mais 30 % d'entre eux ont déjà accepté en « amis » des gens qu'ils n'avaient pas rencontrés pour de vrai. Peut-on alors considérer qu'ils sont vraiment « entre amis » ?

Un tiers des jeunes ont été choqués ou gênés par des contenus

Le réseau social est un espace plutôt civilisé mais les risques y sont démultipliés par la résonance d'internet. 18 % des 8-17 ans y ont déjà été insultés et plus d'un tiers (36 %) a déjà été choqué par certains contenus. Spontanément, ils citent d'abord les contenus à caractère sexuel, puis les contenus violents ou racistes et homophobes. Quand ils ont été choqués, seuls 10 % d'entre eux en ont parlé à leurs parents : ils en parlent plus facilement quand le sujet des réseaux sociaux est abordé en famille.

Des jeunes conscients des risques

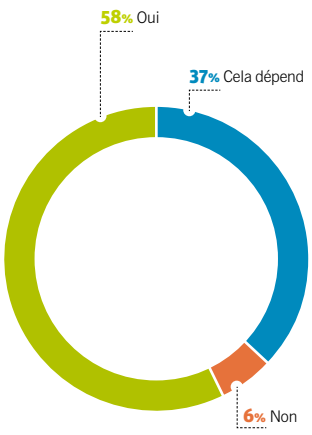
Les 8-17 ans semblent plutôt sensibilisés aux risques pour la vie privée : 57 % déclarent que l'inscription sur un réseau social comporte des risques.

Au niveau européen, entre 12 et 15 % seulement des jeunes livrent leur adresse ou leur numéro de téléphone sur un réseau social. Ils semblent donc conscients de la sensibilité de ces informations. La France se situe d'ailleurs plutôt en dessous de cette moyenne (moins de 8 %).

Globalement, si les jeunes semblent donc conscients des risques pour la vie privée associés à l'utilisation des réseaux sociaux (57 %), les comportements imprudents sont répandus. Les jeunes français ne font pas figure d'exceptions : les comportements à risques se concentrent partout sur les publics les plus jeunes et les moins bien informés. ▸▸▸

Des enfants plutôt sensibilisés aux risques des réseaux sociaux

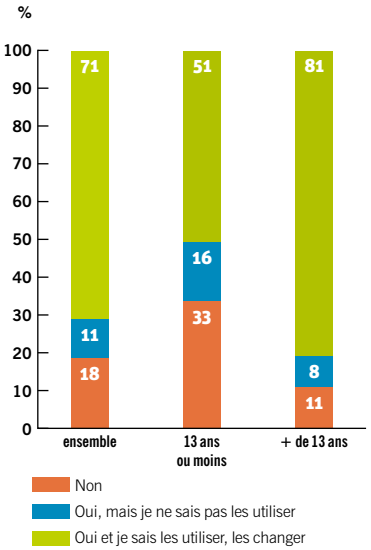
Dirais-tu que s'inscrire sur un réseau social comporte des risques pour la vie privée ?



[1] Dans le cadre du programme EU kids online, 27 000 enfants internautes de 9 à 16 ans et leurs parents ont été interviewés dans 27 pays. Plus d'informations sur : www.eukidsonline.net / [2] Source : Pew Research Center's Internet & American Life Project. Données : septembre 2009. Plus d'informations sur : http://pewinternet.org/

Un quart des jeunes européens ont en effet un profil totalement public sur leur réseau social (un cinquième seulement en France, et seulement un sur 10 au Royaume Uni et en Irlande). Mais l'étude européenne montre aussi que ce sont les enfants qui ont leur statut réglé sur « public » qui « postent » le plus d'informations personnelles (un sur cinq, soit le double du chiffre moyen).

Il existe des paramètres de confidentialité pour limiter la diffusion des informations que tu publies. Est-ce que c'est quelque chose que tu connais ?



La France est le pays où la supervision parentale parait a priori la plus forte, mais celle-ci est plus quantitative que qualitative

Les parents imposent souvent des règles d'utilisation : au niveau européen, un tiers des parents interdiraient à leurs enfants d'avoir un profil sur un réseau social, et c'est en France que cette interdiction serait la plus présente : 45%. En réalité, le contrôle des parents s'exerce peu sur le contenu, mais plutôt sur la quantité et la fréquence d'utilisation : la plupart des parents se contentent de réguler le temps passé à utiliser l'ordinateur, comme le montre l'étude française TNS Sofres.

Certes les parents semblent être au courant à 97% du fait que leurs enfants sont sur les réseaux sociaux (une moitié (49%) d'entre eux serait « amis » avec leurs parents). Et la moitié des enfants (55%) se disent surveillés dans leur utilisation de Facebook, la vigilance des parents étant plus marquée pour les plus jeunes (77%) et les filles (63%).

Mais le sondage montre aussi que les jeunes se connectent souvent seuls : depuis leur ordinateur personnel (50%) et de plus en plus depuis leur mobile (23%)…

En outre, seule la moitié (55%) des 8-17 ans interrogés déclare en discuter avec leurs parents et ce, principalement pour le temps qui y est passé plutôt qu'en termes d'usages… Les parents sont donc assez peu associés.

Enfin, 40% des enfants français exposés à un contenu choquant en parlent en priorité à leurs amis et ils sont à peine plus de 15% à se tourner vers leurs parents selon les résultats TNS Sofres.

Ces résultats, comme ceux concernant l'usage du smartphone chez les jeunes (cf chapitre 1), montrent clairement que le rôle des parents dans l'éducation numérique de leurs enfants est essentiel mais ne peut se limiter à un contrôle quantitatif, d'ailleurs le plus souvent inefficace. Cela passe d'abord par leur propre éducation numérique. Ceci suppose donc que les parents aient à tout le moins le même niveau d'information (voire de pratique) que leurs enfants sur les réseaux sociaux de façon à pouvoir en discuter en pleine connaissance de cause et à favoriser ainsi la prise d'autonomie et la responsabilisation des jeunes dans la gestion de leur réseau et de la confidentialité de leur vie privée.

Ces études montrent qu'informer les jeunes et leurs parents est un enjeu crucial. Elles témoignent aussi du fait que la restriction à l'inscription en fonction de l'âge n'est que partiellement efficace, voire parfois contre-productive (car elle pousse certains jeunes à déclarer un âge faux). Des mécanismes spécifiques de réglage stricts de vie privée « par défaut » pour les plus jeunes pourraient être plus efficaces, d'autant que l'essor de l'internet mobile rend la supervision parentale beaucoup plus difficile que lorsque l'accès se faisait via un ordinateur familial.

Quelques bonnes pratiques

Face à ces constats, l'UNAF, ACTION INNOCENCE et la CNIL ont proposé quelques bonnes pratiques aux parents qui se sentent souvent démunis sur ce sujet.

Un guide pratique destiné aux parents a ainsi été diffusé via les UDAF et ACTION INNOCENCE. Il est aussi disponible sur les sites de la CNIL et de l'UNAF. ■

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.

La dématérialisation des procédures, mise en place en 2010, confirme son succès en 2011, puisque 92 % des formalités sont effectuées en ligne.

- 48 726 déclarations simplifiées
- 29 645 déclarations normales
- 1 808 demandes d'autorisation
- 869 demandes d'avis
- 556 demandes d'autorisation de recherche médicale
- 205 demandes d'autorisation évaluation de soins
- Il faut ajouter 434 demandes de modification effectuées par courrier.

Le SORP est chargé de la validation des déclarations. En 2011, il a délivré les récépissés dans **un délai moyen de 48 h pour les déclarations simplifiées et de 4 jours ouvrés pour les déclarations (soit 27 530 récépissés de déclarations délivrés par le SORP). Ces délais étaient de 13 mois en 2006 et de 3 semaines en 2010.**

Le SORP 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 (5 720 courriers adressés en 2011 contre 4 400 en 2010) et par téléphone. La permanence de renseignements juridiques est assurée par 6 téléconseillers, du lundi au vendredi (de 10 h à 12 h et de 14 h à 16 h). Cette permanence juridique a pris en charge 69 620 appels en 2011 contre 63 125 en 2010. ■

32 743
COURRIERS REÇUS
CONTRE 28 490 EN 2010

138 979
APPELS TÉLÉPHONIQUES
CONTRE 132 806 EN 2010

82 243
DOSSIERS DE FORMALITÉS
CONTRE 70 797 EN 2010

FOCUS

Les usagers sont-ils satisfaits ?

- **93 % sont satisfaits de l'accomplissement des formalités préalables contre 96 % en 2010**
- **79 % sont satisfaits du contact avec la CNIL contre 87 % en 2010**

Source : Enquête de satisfaction réalisée par l'IFOP fin septembre 2011 auprès de 1 013 usagers.

LES CORRESPONDANTS

L'année 2011 a été particulièrement riche pour les Correspondants « Informatique et Libertés » (CIL). Les actions menées par la CNIL auprès d'eux peuvent se résumer en quatre temps forts, ou quatre mots clés : **fédérer, accompagner, promouvoir et évaluer**.

Depuis la modification de la loi « Informatique et Libertés » en août 2004, les entreprises et les administrations peuvent désigner un Correspondant « Informatique et Libertés » (CIL). Avec l'introduction des pouvoirs de sanction et de labellisation de la CNIL, le correspondant est le symbole des nouveaux outils créés par le législateur français pour garantir l'effectivité de la protection des données.

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

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

FÉDÉRER

Pour la première fois depuis leur création en 2004, la CNIL a organisé une journée dédiée aux CIL. Elle s'est déroulée le 8 avril 2011, au Palais du Luxembourg à Paris et a réuni 200 correspondants. L'objectif principal était de permettre aux CIL et à la CNIL d'échanger sur les six années passées et d'envisager ensemble l'avenir de cette profession. À cet égard, deux tables rondes ont été organisées, l'une consacrée aux réseaux de CIL, l'autre au rôle des correspondants et de la CNIL face aux innovations technologiques. Cela a également été l'occasion pour des CIL français et étrangers de témoigner de leurs expériences et de leurs travaux. Devant le succès rencontré par cette manifestation et les attentes exprimées par les correspondants, la CNIL a décidé de pérenniser cette action et d'organiser un événement similaire tous les deux ans.

ACCOMPAGNER

Les correspondants manifestent régulièrement leur souhait d'être accompagnés par la CNIL dans le cadre d'actions de communication au sein de leur organisme afin d'expliquer les enjeux de la loi « Informatique et Libertés » et de leur métier. Ce besoin est particulièrement récurrent à la veille de la journée européenne de la protection des données, organisée chaque 28 janvier depuis 2007. C'est pourquoi, la CNIL a réalisé un « kit de communication » à destination exclusive des correspondants. Il a été adressé en décembre 2011 à chaque correspondant et comprenait des affiches, des autocollants et des cartes postales axés sur les missions du CIL et la journée européenne du 28 janvier, ainsi qu'un dépliant sur la vie privée au quotidien. Ce type d'action doit permettre aux CIL de renforcer leur visibilité au sein de leurs organismes et leur permettre de

27
SESSIONS DE FORMATION RÉUNISSANT **719 PARTICIPANTS**
CONTRE 25 SESSIONS EN 2010 RÉUNISSANT 530 PARTICIPANTS

sensibiliser les différentes personnes de leur entourage (collègues, clients, famille ou amis) à la protection des données, de manière interactive et ludique.

PROMOUVOIR : LA RECONNAISSANCE D'UN MÉTIER

Au sein de son organisme, le CIL agit en tant qu'expert de la protection des données dans sa mission de régulation et de conseil. Les connaissances particulières dont il doit disposer en droit et en informatique ont conduit à la professionnalisation de cette fonction. D'ailleurs, il occupe souvent ce poste à temps plein et dirige parfois un service comprenant plusieurs personnes chargées de veiller à la conformité de son organisme à la loi. C'est dans ce contexte que la CNIL a sollicité Pôle emploi pour que la fonction de CIL soit inscrite au Répertoire Opérationnel des Métiers (ROME - référentiel regroupant les métiers par fiches et par domaines professionnels).
Cette demande s'est traduite par l'insertion du métier de CIL dans la fiche intitulée « défense et conseil juridique » (K 1903). Ce rattachement fonctionnel à un métier juridique résulte du fait que l'objet même du rôle de CIL est de veiller au respect de la loi. Cependant, cela n'exclut en rien d'autres profils professionnels de l'exercice de cette fonction. En pratique, de nombreux CIL exercent des métiers différents : déontologues, auditeurs, informaticiens, responsables qualité, etc. La reconnaissance officielle du métier de correspondant par un acteur essentiel de la politique de l'emploi en France renforce le rôle et la légitimité du CIL.

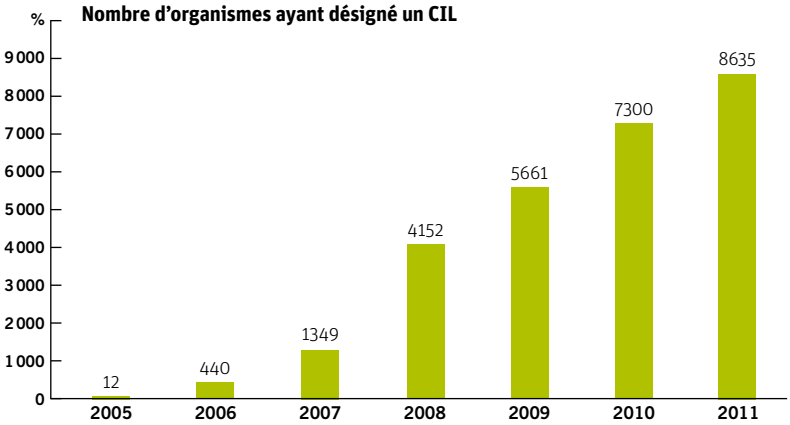
ÉVALUER

Dans le cadre du programme annuel des contrôles pour 2010, la Commission a souhaité apprécier l'efficacité des CIL. Pour cela, elle a procédé à des contrôles dans des organismes dotés d'un CIL. Elle a également effectué des contrôles comparatifs auprès d'organismes ayant la même activité, certains s'étant dotés d'un CIL, d'autres pas, afin d'évaluer leur niveau respectif de conformité à la loi « Informatique et Libertés ». Au total, 18 organismes ont été contrôlés dont 8 dans le cadre des contrôles comparatifs (4 avec CIL, 4 sans). Cette campagne de contrôles a permis de dresser un premier bilan du métier de CIL. Elle a également amené la CNIL à décider de mesures destinées à promouvoir le développement de ce métier tout en prévenant les possibles dérives.

Les contrôles effectués ont permis de répartir les CIL en trois catégories, en fonction de la manière dont ils accomplissent leurs missions :
• des CIL compétents et investis dans leurs fonctions,
• des CIL qui accomplissent partiellement leurs missions faute de temps, de moyens ou de reconnaissance, et enfin,
• des CIL mis en place comme « paravent » dans le seul but de bénéficier d'un allégement des formalités ou d'un effet d'affichage.

Il est ainsi clairement apparu que **l'efficacité des correspondants est grandement liée aux moyens et ressources qui leur sont affectés par le responsable de traitement ainsi qu'à leur investissement personnel.**
Lors de certains contrôles, il est apparu que des correspondants et des responsables de traitement n'ont pas véritablement conscience de leurs obligations. Pourtant, le choix d'un correspondant doit avoir pour effets un meilleur fonctionnement de l'organisme et la maîtrise des enjeux liés à la protection des données. Pour atteindre cet objectif, la CNIL va encore renforcer son offre d'ateliers à destination des CIL, notamment sur les procédures et les stratégies d'audit interne. Il sera également procédé à de nouveaux contrôles chaque année. ■

Nombre d'organismes ayant désigné un CIL



3. CONSEILLER ET PROPOSER

L'article 11 de la loi du 6 janvier 1978 modifiée confère à la CNIL une mission de conseil au gouvernement et au parlement. Cette mission prend la forme d'avis.

Le registre national des crédits aux particuliers

Avis sur le décret relatif à la conservation d'informations par les hébergeurs et les FAI

GROS PLAN
Observations sur la proposition de loi relative à la protection de l'identité

La CNIL informe les pouvoirs publics

LE REGISTRE NATIONAL DES CRÉDITS AUX PARTICULIERS

La loi Lagarde portant réforme du crédit à la consommation[1] a créé un Comité chargé de préfigurer la création d'un registre national des crédits aux particuliers. La mission assignée au Comité n'était pas de se prononcer sur l'opportunité d'introduire en France une centrale de crédit, susceptible de recenser des informations sur près de 25 millions de personnes, mais d'étudier les modalités pratiques de son introduction.

LES TRAVAUX ET LE RAPPORT DU COMITÉ DE PRÉFIGURATION

La CNIL a pris part à l'ensemble des réunions du Comité et de ses groupes de travail. Celui-ci s'est notamment penché sur la question de l'identifiant, les types de crédit concerné, les données collectées, etc. La CNIL a contribué aux travaux du Comité sur le respect des dispositions de la loi « Informatique et Libertés » (proportionnalité des données collectées, durée de conservation limitée, etc.).

Le rapport du Comité a été rendu public en août 2011 et soumis à consultation publique par le Ministre de l'Économie, des finances et de l'industrie jusqu'au 15 septembre 2011. Dans le cadre de cette consultation, la Commission réunie en séance plénière le 8 septembre 2011 a émis un avis. Du fait de l'importance des enjeux inhérents à l'introduction d'une centrale de crédit en France, la Commission, en tant que régulateur de la protection des données, a souhaité s'exprimer sur le principe même de son introduction et sur le recours au numéro d'inscription au Répertoire national d'identification des personnes physiques (numéro de sécurité sociale), identifiant préconisé par le Comité.

25 millions
DE PERSONNES SERAIENT CONCERNÉES PAR LE REGISTRE

L'introduction d'une centrale de crédit

La CNIL se montre réservée quant à la pertinence d'une centrale de crédit pour lutter contre le surendettement. Cette position constante de la Commission a été exprimée à de nombreuses reprises[2].

L'objectif d'une telle centrale est de prévenir le risque de surendettement. Elle vise à recenser des informations relatives aux crédits en cours et susceptibles de constituer des éléments d'alerte de situation de surendettement afin d'éviter l'octroi « du crédit de trop ». Or, les situations actuelles de surendet-

INFOS +

Qu'est qu'une centrale de crédit ?

Une centrale de crédit également appelée « fichier positif », ou registre des crédits est un fichier regroupant l'ensemble des encours de crédit, c'est-à-dire des crédits octroyés par les banques à des particuliers (crédit immobilier, crédit à la consommation, etc.). Ce fichier accessible à tous les établissements de crédit vise à permettre une meilleure évaluation de la solvabilité de la personne concernée dans le but de lutter contre le surendettement.
Inversement les fichiers dits « négatifs » recensent des incidents de remboursement sur les crédits octroyés. En France, il s'agit du FICP[3] qui regroupe actuellement des informations sur 2,5 millions de personnes.

[1] Loi n°2012-737 du 1er juillet 2010 / [2] Notamment dans le cadre de son rapport annuel 2001 et à l'occasion d'auditions par les parlementaires / [3] Fichier national des incidents de crédit aux particuliers.

tement semblent plus résulter d'une accumulation de causes dont certaines sont imprévisibles (augmentation des dépenses énergétiques, etc.) et d'une dégradation de la situation économique de l'intéressé suite à un « accident de la vie » (chômage, maladie, divorce, etc.) que d'une souscription abusive de crédits. Dans certains cas, notamment en cas d'accession à la propriété, le premier crédit, c'est-à-dire celui entraînant l'inscription de la personne concernée dans la centrale serait déjà le crédit de trop.

En outre, la centrale de crédit belge introduite en 2003 n'a pas eu, à cette date, d'effet significatif sur le surendettement. Après une diminution du nombre de contrats défaillants en 2006 et 2007, on constate une nouvelle hausse à compter de 2008[4] ce qui permet clairement d'établir un lien entre le phénomène du surendettement et la situation économique. Dès lors, il n'existe pas d'études statistiques permettant d'établir l'efficacité de la centrale en termes de prévention du surendettement.

Enfin, il conviendrait au préalable d'évaluer les effets sur le surendettement de la loi Lagarde dont l'ensemble des dispositions ne sont entrées en vigueur qu'en 2011.

En tout état de cause, la CNIL estime être allée au bout de sa réflexion sur ce sujet et considère depuis 2007[5] que *« seul le Législateur (a) compétence pour se prononcer sur l'utilité sociale de la constitution de « fichiers positifs » dans le secteur du crédit »*.

Le recours au Numéro de sécurité sociale (NIR)

Le Comité de préfiguration a considéré que la création d'un identifiant dérivé du numéro de sécurité sociale, le NIR, était la « seule option permettant une identification fiable au sein du futur Registre ». La CNIL a réitéré ses réserves de principe quant à l'utilisation du NIR qui doit, selon elle, **être strictement réservée à la sphère sociale**. Elle a souligné les dérives possibles notamment en raison du risque d'interconnexion et de détournement de finalité de cet identifiant. Elle considère, en outre, que l'utilisation d'un identifiant dérivé du NIR ne devrait être utilisé qu'en dernier recours c'est-à-dire si aucune autre solution ne pouvait être envisagée et sous réserve que le NIR fasse l'objet d'un double hachage. ■

INFOS +

Qu'est-ce que le « hachage » ?

Il s'agit d'une fonction mathématique qui génère une empreinte à partir d'une donnée. Cette empreinte se présente sous la forme d'une chaîne de caractères non signifiants qui ne permet pas de retrouver la donnée initiale. De plus, il est très peu probable que deux données distinctes génèrent la même empreinte.

> Seul le Législateur a compétence pour se prononcer sur l'utilité sociale de la constitution de fichiers positifs

[4] Chiffres Banque nationale de Belgique / [5] Délibération n°2007-044 du 8 mars 2007.

AVIS SUR LE DÉCRET RELATIF À LA CONSERVATION D'INFORMATIONS PAR LES HÉBERGEURS ET LES FAI*

En 2007, la Chancellerie avait saisi la CNIL pour avis d'un projet de décret relatif à la conservation des données permettant l'identification d'une personne ayant contribué à la création d'un contenu mis en ligne, pris pour l'application de l'article 6 de la loi pour la Confiance dans l'Économie Numérique. La CNIL avait rendu sa délibération le 20 décembre 2007 sur le fondement de l'article 11-4° a).

Le décret a été finalement adopté le 25 février 2011. Ce nouveau dispositif vient en complément des dispositions de l'article 34-1 du Code des postes et des communications électroniques qui oblige les opérateurs à conserver des données techniques relatives aux communications électroniques concernant notamment les appels téléphoniques et les mails.

Dans son avis sur le projet de décret, la Commission avait relevé que les catégories de personnes soumises à cette obligation de conservation de données de connexion étaient insuffisamment précisées. La Commission avait également souligné que les données devant être conservées apparaissaient insuffisamment définies, notamment en ce qui concerne les données d'identification des personnes physiques concernées. En effet, les données désignées par « l'identifiant de la connexion » ou l'« identifiant attribué (…) à l'abonné » peuvent varier en fonction du type de ligne (ADSL, câble ou fibre optique).

La CNIL avait également formulé des réserves sur :

• Les conditions de conservation des données, du fait qu'elles étaient insuffisamment précisées.

• Les modalités de mise à disposition des données aux autorités en charge de la lutte contre le terrorisme. La CNIL avait recommandé que le décret précise que les données seront transmises par des employés individuellement désignés et appartenant aux services en charge des demandes de communication de données des prestataires concernés.

• La collecte des références de paiement. En effet, le numéro de carte bancaire ne doit en aucun cas être utilisé comme identifiant d'une personne physique. La CNIL avait rappelé que la durée de conservation d'un numéro de carte bancaire ne saurait excéder le délai nécessaire à la réalisation de la transaction.

Ces demandes n'ont pas été prises en considération.

Plusieurs observations de la CNIL ont toutefois été reprises dans le texte adopté. C'est ainsi que l'identifiant du terminal utilisé pour la connexion ne doit être conservé que lorsque les FAI y ont effectivement accès. De même, l'identifiant utilisé par l'auteur de l'opération ne doit être conservé par les hébergeurs que lorsque les utilisateurs l'ont fourni.

L'ensemble de ces dispositions s'inscrit dans une tendance générale visant à conserver de plus en plus de traces laissées sur les réseaux, afin de faciliter la recherche, la constatation et la poursuite des infractions pénales ou des manquements au code de la propriété intellectuelle. Au niveau européen, la directive 2006/24/CE a créé l'obligation de conservation de certaines données, pour des durées comprises entre 6 mois et 2 ans. Cette directive pourrait être prochainement révisée, comme l'indique la Commission européenne dans son rapport d'évaluation publié le 18 avril 2011, afin notamment de mieux harmoniser les transpositions nationales et s'assurer de la proportionnalité des dispositifs de conservation. ■

INFOS +

De quoi s'agit-il ?

Le 25 février 2011, le gouvernement a mis fin à près de 7 ans d'attente, en publiant le décret d'application de l'article 6 de la Loi du 21 juin 2004 pour la Confiance dans l'Économie Numérique (LCEN). Ce décret vient préciser les données que les fournisseurs d'accès internet et les hébergeurs doivent conserver lors de la création de contenu en ligne. La CNIL avait rendu son avis sur le projet de décret en 2007.

** Fournisseurs d'Accès à Internet*

GROS PLAN

OBSERVATIONS SUR LA PROPOSITION DE LOI RELATIVE A LA PROTECTION DE L'IDENTITÉ

« Un projet sans précédent en France »

Depuis le début des années 2000, plusieurs projets de cartes d'identité biométriques et électroniques ont vu le jour. La CNIL a ainsi été saisie par le ministère de l'intérieur de trois avant-projets de loi : « Titre fondateur » et « INES » qui n'ont pas abouti, ainsi que « Protection de l'identité » sur lequel elle s'est prononcée dans sa délibération n°2008-306 du 17 juillet 2008, qui n'a pas été rendue publique.

À l'occasion du débat parlementaire sur la proposition de loi n° 682 relative à la protection de l'identité déposée au Sénat le 27 juillet 2010 (devenue la loi n°2012-410 du 27 mars 2012), la CNIL a estimé nécessaire, conformément à ses missions générales de conseil et d'information prévues par l'article 11 de la loi du 6 janvier 1978 modifiée, de rendre publique son analyse en la matière par une note d'observations en date du 25 octobre 2011.

PRÉSENTATION DE LA PROPOSITION DE LOI RELATIVE À LA PROTECTION DE L'IDENTITÉ

La CNIL s'est prononcée à de multiples reprises sur des projets de traitements biométriques mis en œuvre aux fins de délivrance de titres d'identité ou de voyage, tout particulièrement dans le cadre de son avis sur les passeports biométriques du 11 décembre 2007. Pour gérer les procédures d'établissement, de délivrance, de renouvellement, de retrait des passeports et de prévention et détection des falsifications et contrefaçons, le ministère de l'Intérieur et l'Agence

▸▸▸

nationale des titres sécurisés (ANTS) mettent en œuvre un traitement de données à caractère personnel dénommé « TES ». Ce processus s'inscrit dans la dynamique européenne de sécurisation et d'intégration d'éléments biométriques dans les passeports et documents de voyage (Règlement CE n°2252/2004).

FOCUS

Zoom sur le passeport biométrique

Le passeport biométrique a été autorisé par le décret n° 2008-426 du 30 avril 2008, pris après avis de la CNIL. Le système repose sur l'équipement des passeports par une puce électronique contenant des données biométriques (photographie et deux empreintes digitales) et la création d'une base de données centralisée. Ce traitement a pour unique objectif de sécuriser la délivrance de ces titres et de lutter contre la fraude à l'identité. À cette fin, le ministère de l'intérieur a adopté une organisation limitant les possibilités d'interrogation de la base biométrique. Pour cela, la base des données d'état civil a été séparée de la base des données biométriques. Cette séparation est réalisée en créant un numéro unique ne permettant pas de retrouver le nom à partir de ce seul numéro. Ainsi, il est possible à partir d'un nom de retrouver les données biométriques correspondantes, par exemple afin de vérifier, en cas de perte ou de vol du passeport, l'identité du demandeur. En revanche, il n'est pas possible d'identifier une personne à partir de ses seules empreintes digitales.

INFOS +

En quoi consiste la proposition de carte d'identité numérique ?

La carte d'identité numérique telle que prévue par la proposition de loi était un titre d'identité sur support matériel auquel deux puces électroniques sécurisées sont ajoutées. La première permettrait de certifier l'identité du titulaire de la carte et contiendrait des éléments d'identification : nom de famille, prénom(s), sexe, date et lieu de naissance, domicile, taille, couleur des yeux, empreintes digitales et photographie. La seconde, optionnelle, permettrait de s'identifier sur les réseaux de communications électroniques et de créer une signature électronique pouvant être utilisée pour les relations avec l'administration en ligne et dans le cadre du commerce électronique.

La proposition de loi reprend dans une large mesure le dispositif mis en œuvre dans le cadre des passeports biométriques. Elle prévoit en effet la délivrance de cartes d'identité biométriques (munies d'une puce électronique contenant notamment deux empreintes digitales) et la création d'une base de données contenant l'ensemble des informations requises pour la délivrance du titre, et notamment huit empreintes digitales du demandeur.

Cependant, le dispositif est sensiblement élargi. Tout d'abord, par la mise à disposition d'une seconde puce permettant l'utilisation de nouveaux services tels l'authentification et la signature électroniques. Mais surtout, la proposition de loi créé une base de données commune aux demandeurs de cartes d'identité et de passeport et permet l'identification des personnes à partir de leurs empreintes digitales.

C'est pourquoi le dispositif projeté est un projet sans précédent en France. Le fichier central serait en effet en capacité de conserver les informations d'état civil et les données biométriques de tous les citoyens français, majeurs et mineurs, ayant fait la demande d'un titre d'identité. Seuls quelques pays européens disposent actuellement d'une base de données centrale, mais aucun n'y conserve huit empreintes digitales, comme le prévoyait le projet initial.

Pays	Carte d'identité électronique	Carte d'identité Biométrique	Puce		Base de données			Remarque
			Photo	Empreinte (nombre de doigts)	Centralisée	Photo	Empreinte (nombre de doigts)	
Allemagne	OUI	OUI	OUI	[Sur demande du citoyen : 2]	NON	NON	NON	
Autriche	NON	NON						
Belgique	OUI	OUI	OUI	NON	OUI	OUI	NON	
Bulgarie	NON	NON						
Chypre	NON	NON						
Danemark	Pas de Carte d'identité							
Espagne	OUI	OUI	OUI	OUI [1]	OUI	OUI	OUI [2]	Même base que le passeport. La carte d'identité est un pré-requis pour celui-ci
Estonie	OUI	NON						La puce sert uniquement à s'authentifier et signer
Finlande	OUI	NON						La puce sert uniquement à s'authentifier et signer
Grèce	NON	NON						
Hongrie	NON	NON						
Irlande	Pas de Carte d'identité							
Italie	OUI	OUI	OUI	OUI [2]	OUI	OUI	OUI [2]	
Lettonie	Pas de Carte d'identité							
Lituanie	OUI	OUI	OUI	OUI [2]	OUI	?	OUI [?]	
Luxembourg	NON	NON						
Malte	NON	NON						
Pays-Bas	OUI	OUI	OUI	OUI [min 2, max 3]	NON	OUI	Suspendue	La base de données est décentralisée
Pologne	NON	NON						Une carte d'identité électronique sans biométrie est prévue pour 2012
Portugal	OUI	OUI	OUI	OUI [2]	OUI	OUI		
République tchèque	NON	NON						
Roumanie	NON	NON						en projet
Royaume-Uni	Carte d'identité lancée en 2006, arrêtée depuis mai 2010							
Slovaquie	NON	NON						
Slovénie	NON	NON						
Suède	OUI	OUI	OUI	OUI [?]	NON	NON	NON	Peu utilisée

[1] La Carte d'identité électronique à travers l'Europe, novembre 2011 / [2] La Carte d'identité électronique à travers l'Europe, novembre 2011

LA POSITION DE LA CNIL

Dans ces conditions, la CNIL a estimé nécessaire de faire connaître son analyse sur cette proposition en publiant une note d'observations adoptée en séance plénière de la Commission le 25 octobre 2011.

En premier lieu, elle a rappelé que les **données biométriques ne sont pas des données à caractère personnel « comme les autres ».** Elles permettent en effet l'identification de la personne par une réalité biologique qui lui est propre, produite par son corps. La CNIL a toujours apporté une attention particulière à ces données, notamment celles dites « à trace » comme les empreintes digitales ou les caractéristiques du visage, qui ont la faculté d'être capturées et utilisées à l'insu de la personne concernée. Cette spécificité des données biométriques a pour conséquence d'accroître le niveau d'exigence quant à leur utilisation.

En ce qui concerne la délivrance de titres biométriques, la Commission a rappelé sa position constante selon laquelle l'introduction dans les titres d'identité et de voyage d'un composant électronique contenant des données biométriques est proportionnée par rapport à l'objectif de renforcement de la sécurité de l'établissement et de la vérification de ces titres. Elle a cependant souhaité que cette délivrance soit assortie de **garanties complémentaires,** concernant en particulier l'âge minimal de collecte des identifiants biométriques ou les sécurités techniques entourant les composants électroniques.

S'agissant de la création de la base de données biométriques, la CNIL a tout d'abord relevé qu'il existe des modalités de lutte contre la fraude qui apparaissent tout à la fois aussi efficaces et plus respectueuses de la protection de la vie privée des personnes que la constitution d'une telle base. Il en est ainsi en particulier de la procédure de vérification des données d'état civil, qui permet de sécuriser les « documents sources » à produire pour la délivrance de titres d'identité et dont la mise en œuvre a été recommandée par la Commission à de nombreuses reprises depuis 1986. Dans ces conditions, elle a estimé que **la proportionnalité de la conservation des données biométriques, au regard de l'objectif légitime de lutte contre la fraude documentaire, n'était pas démontrée.**

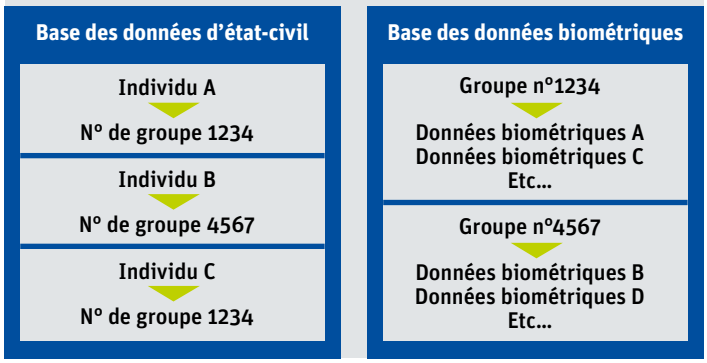
En outre, la Commission a considéré qu'il convenait de s'assurer que le traitement ne soit pas utilisé à d'autres fins que la sécurisation de la délivrance des titres d'identité et de voyage et de lutte contre la fraude à l'identité. Ainsi, elle a recommandé l'interdiction de procéder à une interconnexion du fichier avec tout autre traitement de données à caractère personnel et **de s'assurer par des moyens juridiques et techniques que le système ne soit pas détourné de sa finalité,** et notamment qu'il ne soit pas utilisé à des fins de police judiciaire. La CNIL a par exemple

INFOS +

Lien fort / lien faible : de quoi s'agit-il ?

Le « lien fort » est une méthode d'identification d'une personne au moyen d'éléments biométriques. Ainsi, un jeu d'empreintes permet d'identifier dans la base de données centrale l'identité de la personne concernée, et inversement.
Il est donc possible de construire une table de correspondance entre état civil et données biométriques. Cette méthode est utilisée pour le passeport biométrique.
Le « lien faible », au contraire, est une technique d'identification novatrice qui rend impossible l'identification d'une personne à partir d'un jeu d'empreintes. La personne n'est pas associée à un numéro renvoyant à son identité, mais à un groupe contenant les empreintes digitales de plusieurs personnes. L'interrogation de la base permet seulement de fournir un numéro de groupe. La tentative de fraude peut ainsi être déjouée, sans que l'identité du titulaire des empreintes soit révélée.
Sans se prononcer expressément sur cette technique, la CNIL a estimé que le « lien faible » permettrait de s'assurer que la base centrale n'est pas utilisée à des fins étrangères à son objectif initial, notamment à des fins d'identification policière ou judiciaire des personnes.

Description d'une architecture d'une base de données centralisée à « lien faible »



cité la limitation du nombre d'empreintes digitales enregistrées dans la base centrale ou encore l'absence de lien univoque entre les données biométriques enregistrées dans le traitement central et les données d'état civil (technique dite du « lien faible », voir tableau p. 48).

Par ailleurs, la Commission a également évoqué la possibilité de mettre en œuvre des dispositifs de reconnaissance faciale, prévue par la proposition de loi. Dans le contexte de multiplication du nombre des systèmes de vidéoprotection, de leur interconnexion et de leur interopérabilité, **la CNIL a exprimé sa plus grande réserve quant à la possibilité de recourir à de telles fonctionnalités.**

Enfin, la Commission a souhaité que les nouvelles fonctionnalités électroniques de la carte d'identité (signature et authentification en ligne) soient mieux encadrées, tout en relevant que la proposition de loi prévoyait déjà des garanties importantes (notamment le caractère facultatif de l'activation et de l'utilisation de ces fonctionnalités).

Afin de s'assurer que ces fonctions ne permettent pas la création d'un identifiant unique, voire la constitution d'un savoir public sur les agissements des citoyens, **la CNIL a proposé des mesures supplémentaires d'encadrement :** la mise en place de mécanismes de « divulgation partielle » limitant la transmission de données aux strictes informations nécessaires à l'exécution du service, de mesures d'information claires et préalables à toute transmission de données, ou encore de mesures techniques de nature à garantir la sécurité des communications.

LES SUITES DONNÉES AUX PROPOSITIONS DE LA COMMISSION

La CNIL a été auditionnée à de nombreuses reprises par les parlementaires sur cette proposition de loi. À la suite de ces auditions et surtout de la publication de sa note d'observations, le Gouvernement a modifié certaines de ses dispositions. En particulier, l'interdiction de recourir à des dispositifs de reconnaissance faciale a été inscrite dans le texte, l'enregistrement des empreintes digitales dans la base centrale a été réduit à deux doigts et les finalités de ce traitement ont été précisées.

Cependant, toutes les garanties demandées par la CNIL n'ont pas été introduites dans le projet. En particulier, le principe même de la conservation en base centrale d'éléments biométriques relatifs à l'ensemble de la population française n'a pas été abandonné. En outre, la possibilité d'utiliser les fonctionnalités d'identification biométrique n'a pas été limitée à la délivrance des titres d'identité et de voyage : en prévoyant son utilisation à des fins judiciaires, limitées cependant aux situations liées à la lutte contre la fraude à l'identité, le texte ouvrait la voie, potentiellement, à un élargissement progressif des cas dans lesquels la base pouvait être utilisée, comme l'a bien montré l'exemple récent du FNAEG.

C'est notamment pour prévenir ce risque que la loi relative à la protection de l'identité adoptée par l'Assemblée nationale le 6 mars 2012 a fait l'objet d'une saisine du Conseil constitutionnel par des sénateurs et des députés.

La loi n° 2012-410 relative à la protection de l'identité a été publiée le 27 mars 2012 dans sa version modifiée à la suite de la décision du Conseil constitutionnel. Ainsi, le composant électronique de la carte d'identité numérique comportera les nom, prénoms, sexe, date et lieu de naissance, nom d'usage, domicile, taille, couleur des yeux, deux empreintes digitales et une photographie.

La CNIL sera attentive au devenir de la loi et sera notamment saisie d'un projet de décret en Conseil d'État en fixant les modalités d'application.

La CNIL a ainsi joué son rôle de conseil des pouvoirs publics, conformément à l'article 11 de la loi Informatique et Libertés, en proposant des aménagements protecteurs des libertés individuelles, de la vie privée et des données biométriques traitées. ■

FOCUS

Dernière minute : la décision du Conseil constitutionnel du 22 mars 2012

Le Conseil constitutionnel s'est prononcé sur la loi relative à la protection de l'identité. Il considère que la collecte et l'enregistrement des empreintes digitales dans une puce électronique jointe à la carte d'identité offrent une meilleure identification des personnes, au même titre que le passeport électronique. En revanche, il rejette la proposition d'une base de données centrale contenant les données biométriques de quasiment toute la population. Les finalités de police administrative ou judiciaire projetées au moyen de ce traitement portent atteinte au droit au respect de la vie privée et sont disproportionnées au regard des données collectées à l'objectif initial de délivrance de titres d'identité et de voyage.

Le Conseil considère en outre que la deuxième puce électronique ayant pour finalités l'authentification et la signature électronique sur les réseaux de communications électroniques ne satisfait pas les garanties légales pour assurer l'intégrité et la confidentialité des données enregistrées.

LA CNIL INFORME LES POUVOIRS PUBLICS

Les thématiques intéressant la CNIL ont été, une nouvelle fois cette année, au cœur des préoccupations du Parlement. Avec plus d'une trentaine de rencontres et d'auditions auxquelles elle a participé dans les deux assemblées, notre Commission a encore renforcé ses liens avec les élus. Les questions relatives à la protection de la vie privée ont ainsi très largement nourri les débats parlementaires, aussi bien sur les fichiers de police, que sur l'instauration d'une carte d'identité électronique, la mise en œuvre d'une centrale de crédit aux particuliers, la lutte contre la fraude sociale…

En 2011, la CNIL a été auditionnée à 23 reprises par les membres du Parlement français, contre 18 l'année précédente. Elle a également participé à 10 rendez-vous avec des députés et sénateurs désireux d'échanger sur la protection des données personnelles.

Les principales initiatives législatives intéressant la CNIL

• Promulgation, le 29 mars 2011, des lois organique et ordinaire relatives au Défenseur des droits ;
• Promulgation, le 14 mars 2011, de la loi d'orientation et de programmation pour la performance de la sécurité intérieure, dite LOPPSI 2 ;
• Promulgation, le 23 mars 2011, de la loi portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques (transposition du « Paquet Telecom ») ;
• Publication du rapport d'information n°4113 sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police (Assemblée nationale) ;
• Publication du rapport d'information n°3560 sur les droits de l'individu dans la révolution numérique (Assemblée nationale) ;
• Publication du rapport d'information n°3603 sur la lutte contre la fraude sociale (Assemblée nationale) ;
• Début des travaux parlementaires sur la proposition de loi relative à la protection de l'identité ;
• Début des travaux parlementaires sur le projet de loi renforçant les droits, la protection et l'information des consommateurs ;
• Dépôt, le 14 décembre 2011, de la proposition de loi tendant à prévenir le surendettement.

Pour la première fois, notre Commission a auditionné en séance plénière les députés du groupe Nouveau Centre Jean DIONIS du SEJOUR et Jean-Christophe LAGARDE, dans le cadre de leurs travaux préparatoires au dépôt de leur proposition de loi tendant à prévenir le surendettement. L'envoi de quatre nouveaux numéros de la lettre d'information de notre Commission à l'ensemble des parlementaires, ainsi qu'aux députés européens français, sur la création de la Direction des Études, de l'Innovation et de la Prospective, sur la géolocalisation, sur la révision du cadre juridique européen en matière de protection des données personnelles, et sur les perspectives pour l'année 2012, a permis l'information des parlementaires sur les problématiques actuelles. À cela s'ajoute également l'organisation de déjeuners thématiques et de réunions de travail, les nombreuses notes, les analyses techniques et juridiques de notre Commission en réponse aux interrogations des élus… qui ont ainsi très largement participé à leur sensibilisation sur tous nos sujets, notamment sur la révision de la directive européenne de 1995. ■

4.
RÉGLEMENTER

Conformément à l'article 24 de la loi du 6 janvier 1978 modifiée, la CNIL établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes représentatifs, des normes destinées à simplifier l'obligation de déclaration.

GROS PLAN

LA DIFFUSION SUR INTERNET DES ARCHIVES PUBLIQUES

“Une recommandation pour encadrer les traitements des services d'archives publiques”

Les archives publiques que sont les actes de l'état civil, sont susceptibles d'être réutilisées, notamment par des sociétés de généalogie. Cette réutilisation consiste parfois en une diffusion sur internet.
L'acte de naissance d'une personne comporte en marge tous les actes de sa vie civile : adoption, légitimation, reconnaissance, changement de nom, de sexe, mariage, divorce, PACS, mentions du répertoire civil (placement sous tutelle, curatelle, changement de régime matrimonial), disparition, décès. Ce sont autant de données révélatrices de la vie privée et des secrets des familles qui, à l'expiration d'un délai de 75 ans à compter de la clôture du registre deviennent librement communicables.

La Commission a encadré la réutilisation de documents d'archives contenant des données à caractères personnels par une recommandation n° 2010-460 du 9 décembre 2010.

▸ **La recommandation procède d'un double constat :**

• le recueil de **l'accord exprès** des personnes apparaît difficile compte tenu de l'ancienneté des documents en cause et donc de la difficulté de retrouver les personnes concernées lorsqu'elles sont en très grand nombre. Il en est de même des ayants droit des personnes concernées,

• en conséquence et à défaut de rendre ces données **anonymes ou de procéder à leur masquage,** il appartient à la Commission d'autoriser ou non les réutilisations envisagées et de préciser les garanties qu'elle estime indispensables pour autoriser ces dernières.

▸ **La recommandation exclut la réutilisation :**

• des données dites **sensibles** au sens de l'article 8 de la loi Informatique et Libertés, c'est-à-dire les « données à caractère personnel qui font apparaître,

directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » ;
• des données relatives aux infractions, condamnations et mesures de sûreté au sens de l'article 9 de la même loi ;
• des mentions apposées en marge des actes de l'état civil (adoption, légitimation, perte de nationalité, divorce…) qui sont de nature à porter atteinte à la vie privée et familiale. Même si de telles données sont communicables au titre du code du patrimoine, elles doivent être rendues anonymes ou occultées avant toute réutilisation, l'efficacité de ce masquage doit pouvoir être vérifié par la CNIL.

▸ **La recommandation rappelle les droits des personnes :**

• Les responsables de traitement doivent procéder à une information claire, large et générale sur leur site internet. Cette information doit préciser la finalité du traitement et les droits des personnes. L'internaute qui découvre la publication de ses données personnelles doit pouvoir s'y opposer en ligne de façon simple sur le site consulté.
• le consentement des personnes n'ayant pu être recueilli, elles et leurs ayants droit bénéficient au titre **de la protection de la vie privée d'un droit d'opposition sans conditions.**

▸ **Enfin, la recommandation énumère les précautions à prendre en matière de sécurité :**

• **l'indexation nominative** de ces documents ne peut être réalisée avant que l'expiration d'un délai de **120 ans** à compter de la naissance de la personne.
• Il convient de préserver la sécurité et la confidentialité des données communiquées, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance. Ces précautions doivent pouvoir être vérifiées par la CNIL. ■

FOCUS

Dernière minute : l'autorisation unique n° 29 (AU-029 « ARCHIVES PUBLIQUES ») : le cadre « Informatique et Libertés » pour les traitements des services d'archives publiques

Certes, les services publics d'archives ne font pas de « réutilisation commerciale ». Cependant, à travers leur mission de « mise en valeur du patrimoine », de nombreux services diffusent sur leurs sites internet des documents archivés contenant des données personnelles.
Par délibération n° 2012-113, la Commission encadre les traitements de ces services publics d'archives, nationales et locales, par l'autorisation unique n°29 (AU-029 « ARCHIVES PUBLIQUES »). L'AU-029 simplifie également les déclarations préalables auprès de la CNIL. Dans l'hypothèse d'un traitement ne correspondant pas en tous points au cadre décrit par l'AU-029, le responsable de traitement devra demander une autorisation spécifique à la CNIL.

GROS PLAN

LES ALERTES PROFESSIONNELLES

2109
ORGANISMES ONT DÉCLARÉ LEUR DISPOSITIF D'ALERTE PROFESSIONNELLE

“Une clarification nécessaire pour une plus grande sécurité juridique”

En 2005, le champ d'application de l'autorisation unique était le suivant : domaines comptable, financier, bancaire, des pratiques anti-concurrentielles et de la lutte contre la corruption.
Cette autorisation unique a permis une simplification des formalités des sociétés soumises aux obligations de la loi Sarbanes-Oxley (SOX) qui impose aux entreprises cotées de renforcer le contrôle interne par l'adoption de dispositifs d'alertes.

Par un arrêt du 8 décembre 2009, la chambre sociale de la Cour de cassation a mis cependant en lumière les difficultés d'interprétation de certaines dispositions de l'autorisation unique n°AU-004, en particulier celles relatives au champ d'application.

Dans ce contexte, il est apparu nécessaire à la Commission de clarifier son autorisation unique, les organismes aspirant légitimement à une plus grande sécurité juridique. Préalablement, elle a procédé à de nouvelles auditions des principaux acteurs concernés par les dispositifs d'alerte pour déterminer dans quelle mesure il y avait lieu de modifier les termes de l'autorisation unique.

357
DÉCLARATIONS DE CONFORMITÉ EN 2011

INFOS +

Qu'est-ce qu'une alerte professionnelle ?

Une « alerte professionnelle » (ou « whistleblowing ») est un système d'alerte mis à la disposition des salariés qui leur permet de signaler des problèmes pouvant sérieusement affecter l'activité de leur entreprise ou engager gravement sa responsabilité. Il peut s'agir par exemple d'un numéro de téléphone de type «ligne éthique» ou d'une adresse électronique particulière. Les alertes recueillies sont ensuite vérifiées, dans un cadre confidentiel, et permettent à l'employeur de décider, en connaissance de cause, des mesures correctives à prendre.
Certains de ces dispositifs peuvent prendre la forme de traitements automatisés de données à caractère personnel susceptibles, du fait de leur portée, de conduire au licenciement de personnes et donc de les exclure du bénéfice de leur contrat de travail. Dès lors, de tels dispositifs constituent des traitements relevant de l'article 25-I 4° de la loi « Informatique et Libertés » et doivent, à ce titre, être autorisés par la CNIL.
Dans le cadre de son pouvoir d'autorisation, la CNIL veille à ce que les dispositifs mis en œuvre ne favorisent pas un système généralisé de délation grâce au recueil et au traitement de signalements anonymes. Par ailleurs, elle a toujours insisté sur le fait que ces dispositifs étaient complémentaires des systèmes traditionnels de remontée des alertes (voie hiérarchique, représentants du personnel, inspection du travail) et avaient seulement vocation à traiter les cas ou ces mécanismes traditionnels étaient défaillants.

Quelques chiffres*

	2011	Total depuis 2005
Nombre de déclarations de conformité à l'AU-004 en 2011	357	2 109
Autorisations spécifiques (accord)	19	134
Autorisations spécifiques (refus)	1	5

* *au 24/02/12*

LA NOUVELLE AUTORISATION UNIQUE N°4

Les pratiques anticoncurrentielles sont dorénavant comprises dans le champ d'application de l'AU-04. Cette modification est intervenue après plusieurs décisions de l'Autorité de la concurrence enjoignant aux organismes sanctionnés de prévenir toute atteinte à la concurrence, par la mise en place d'un mécanisme d'alerte à destination de l'ensemble des salariés.

Il s'agissait également d'inclure dans l'AU-04 la loi japonaise « *Financial Instrument and exchange Act* » du 6 juin 2006 dite « *Japanese SOX* » car elle s'inspire fortement de la loi SOX américaine.

Les organismes avaient jusqu'à juin 2011 pour se mettre en conformité avec la nouvelle autorisation unique ou déposer un dossier de demande d'autorisation spécifique en justifiant, motivation à l'appui, les raisons pour lesquelles leurs dispositifs ne sont pas conformes au cadre posé par l'AU-04.

Les dispositifs non conformes à l'AU-04

La CNIL a constaté un accroissement du nombre de demandes d'autorisation concernant des systèmes d'alerte professionnelle non conformes à l'AU-04. Pour la seule année 2011, elle a été saisie d'une trentaine de dossiers.

Les services de la CNIL sont quotidiennement sollicités par les entreprises et les avocats quant aux conditions d'autorisation de ces traitements.

Il existe en France des procédures d'alerte dont les objectifs sont très éloignés du cadre proposé par l'AU-004 et de la loi SOX américaine. Les principales différences concernent le champ d'application (qui dépasse le strict champ financier) et le fondement juridique (dispositifs mis en œuvre en dehors de toutes obligations réglementaires ou législatives).

Lorsque le champ d'application est plus large que celui visé à l'article 1er de l'autorisation unique, l'entreprise doit lister avec précision les domaines entrant dans le champ d'application. Le choix de chaque domaine doit être dûment motivé en raison de la gravité des alertes qui peuvent en résulter et des conséquences pour une entreprise, en termes de sanctions pénales, d'image ou de continuité d'activité.

La Commission examine au cas par cas la proportionnalité du champ d'application de chaque dispositif d'alerte.

Elle a ainsi délivré en 2011, 19 autorisations spécifiques et 1 refus.

Ce refus a été motivé par plusieurs manquements à la loi « Informatique et Libertés » et aux règles édictées par la CNIL en matière d'alertes professionnelles (champ trop large, information des personnes incomplète, anonymat encouragé, etc.).

En effet, la CNIL a constaté que les salariés pouvaient alerter sur toutes les préoccupations concernant le non-respect des lois et règlements ainsi que sur les comportements contraires aux principes du code de conduite. En outre, l'utilisation anonyme du dispositif d'alerte de cette société était présentée comme une modalité normale de remontée d'alerte.

▸▸▸

LES DISPOSITIFS D'ALERTE AU SERVICE DE LA LUTTE CONTRE LES DISCRIMINATIONS

De nombreuses actions sont lancées par les entreprises et les pouvoirs publics pour promouvoir la diversité, notamment dans le monde du travail, et lutter contre les discriminations.

Certains employeurs ont mis en place des dispositifs d'alerte informatisés pour prévenir et identifier les discriminations au travail. Pour ce faire, ils ont souhaité mettre à disposition de leurs salariés une voie de réclamation dédiée dont la gestion est assurée par des personnes formées aux questions relatives à la discrimination. Les employeurs espèrent ainsi lever toute inhibition qu'aurait un salarié à évoquer des faits aussi sensibles et personnels que la discrimination.

En effet, selon l'ex HALDE (actuel Défenseur des droits), les salariés ont tendance à s'autocensurer sur ces domaines, d'autant plus que les voies classiques d'alerte ne s'avèrent pas toujours les plus efficaces. Le manque de soutien et d'écoute de la hiérarchie sont les justifications le plus souvent apportées à cette situation. En outre, pour certaines discriminations touchant à la vie privée ou à l'intimité, les salariés ont du mal à en parler à leur hiérarchie ou à des représentants du personnel (orientation sexuelle, problème de santé, opinion philosophique, etc.).

Ces dispositifs ne sont pas couverts par l'AU-04 et une autorisation spécifique est requise. **La Commission a autorisé, pour la première fois le 3 mars 2011, deux sociétés à mettre en place un dispositif d'alerte professionnelle dédié aux plaintes et réclamations en matière de lutte contre les discriminations.** Depuis, ce sont 5 autres entreprises qui ont reçu une autorisation.

La Commission a autorisé ces dispositifs d'alerte dédiés à la lutte contre les discriminations après avoir vérifié les garanties mises en œuvre et notamment :

- l'obligation pour le donneur d'alerte de s'identifier (pas d'alertes anonymes) ;
- l'information des salariés sur les finalités du dispositif, les personnes habilitées à traiter les alertes, ainsi que leurs droits d'accès et de rectification ;
- le caractère facultatif et complémentaire du dispositif (pas d'obligation pour les salariés d'utiliser le dispositif d'alerte) ;
- le traitement confidentiel de l'identité du donneur d'alerte ;
- la conservation limitée des données ;
- les mesures de sécurité (confidentialité des informations et traçabilité des accès).

La CNIL a rappelé que ces nouveaux outils d'alerte devaient rester complémentaires et facultatifs. En effet, il est important de privilégier la ligne managériale et les voies légales d'alerte, notamment par l'intermédiaire des délégués du personnel.

Enfin, la CNIL a été particulièrement attentive à l'information faite auprès des représentants du personnel des organismes. Dans certaines entreprises, un accord collectif groupe portant notamment sur la lutte contre les discriminations a d'ailleurs été conclu avec les organisations syndicales ce qui démontre la forte implication des partenaires sociaux. La mise en œuvre de ces dispositifs ne résulte donc pas d'une décision unilatérale de l'employeur.

QUEL AVENIR POUR CES DISPOSITIFS ?

Compte tenu de l'émergence de nouvelles réglementations telles que la *UK Bribery act* et les initiatives de plus en plus importantes des entreprises en matière d'éthique et de responsabilité sociétale, ces outils seront amenés à se développer dans les années qui viennent.

Il est donc nécessaire de communiquer plus largement sur les conditions dans lesquelles les dispositifs d'alerte professionnelle peuvent être mis en œuvre afin qu'ils respectent les obligations issues de la loi « Informatique et Libertés » et que les droits des personnes soient garantis. ■

FOCUS

Qu'est-ce que le label Diversité ?

Le « label diversité » a été créé par un décret du 17 décembre 2008 et s'inscrit dans le cadre de la politique du Gouvernement en faveur de la prévention des discriminations. Les organismes qui candidatent pour l'obtention du label doivent se conformer à un cahier des charges défini par l'AFNOR certification. Ce cahier des charges préconise la mise en place d'outils permettant d'identifier les plaintes et réclamations internes ou externes et d'assurer la traçabilité des signalements des salariés victimes de discriminations.
La position de la CNIL était attendue car de nombreux organismes privés comme publics ont déjà adhéré au label. Selon les chiffres disponibles, en octobre 2011, leur nombre s'élèverait à 265.

INFOS +

Qu'est-ce que la loi dite *UK Bribery act* ?

Entrée en vigueur le 1er juillet 2011, elle impose à toutes les entreprises exerçant des activités au Royaume-Uni de mettre en place des procédures internes appropriées destinées à prévenir la corruption des personnes qui leur sont associées sous peine d'encourir de lourdes sanctions pénales.

5. CONSULTER ET INNOVER

WiFi, iPhone et géolocalisation

C'est nouveau !

GROS PLAN
Consultation sur le *Cloud computing*

WIFI, iPhone ET GÉOLOCALISATION

La géolocalisation est souvent associée à la technologie GPS. Pourtant, la plupart des smartphones font fréquemment appel à une toute autre technique de géolocalisation : la détection de points d'accès WiFi.
Quel risque représente cette technologie pour la vie privée ? Pour essayer de répondre à cette question les experts de la CNIL ont, dans le cadre de leur laboratoire, mis sous surveillance un iPhone 3Gs pour analyser ses communications et observer les données de géolocalisation qui sont transmises au fabricant de l'appareil.

UNE DEMANDE DE GÉOLOCALISATION

Lorsqu'un utilisateur d'iPhone demande à être géolocalisé, en utilisant par exemple l'application « Boussole » ou « Maps », le téléphone interroge le serveur de géolocalisation d'Apple. Pour cela, il envoie à Apple une courte liste des quelques points d'accès WiFi qu'il a détectés autour de lui. Le serveur d'Apple répond avec une liste répertoriant la localisation de plusieurs centaines de points d'accès WiFi situés autour du téléphone.

C'est alors le téléphone lui-même qui calcule sa propre position à l'aide des informations fournies en ligne.

L'iPhone « BAVARDE » PENDANT VOTRE SOMMEIL...

La surveillance du téléphone a réservé des surprises : durant la nuit, l'iPhone contacte également les serveurs de géolocalisation d'Apple ponctuellement, sans aucune intervention de l'utilisateur. Il envoie en effet à Apple des informations de géolocalisation sur la position des points

d'accès WiFi qu'il a « vus » dans les heures ou les jours précédents.

Il semble que les serveurs d'Apple enrichissent et mettent à jour ainsi leur base de données de géolocalisation WiFi, en mettant à contribution l'iPhone alors que leurs utilisateurs ne s'en servent pas. Cette approche peut soulever des inquiétudes pour la vie privée des personnes mais l'analyse des échanges a montré que le téléphone n'est pas identifié, ce qui est rassurant.

VERS D'AUTRES BAVARDAGES ?

Les « smartphones » sont des objets personnels qui communiquent en permanence avec les réseaux. Si le fabricant de votre iPhone ne vous piste pas, qu'en est-il des multiples applications installées et de vos données personnelles ? C'est un vaste chantier pour les autorités de protection des données dans les années à venir. ■

INFOS +

Géolocalisation WiFi, comment ça marche ?

La plupart des boîtiers Internet sont équipés d'un point d'accès WiFi qui émet en permanence des signaux. Ces signaux contiennent un numéro unique appelé adresse MAC (ou BSSID), qui est propre à chaque point d'accès WiFi. En se basant sur une cartographie des points d'accès WiFi identifiés par leur adresse MAC, certains fournisseurs de services comme Apple ou Google proposent un outil de géolocalisation WiFi : en analysant les adresses MAC des points d'accès WiFi détectés par le téléphone, on peut en déduire la position du téléphone lui-même.

C'EST NOUVEAU !

En 2011, la CNIL a été confrontée à plusieurs innovations technologiques en matière de biométrie.

La Commission a autorisé pour la première fois le recours à **un dispositif biométrique reposant sur la reconnaissance combinée de l'empreinte digitale et du réseau veineux des doigts de la main, pour contrôler l'accès aux locaux sur le lieu de travail**. En l'espèce, l'avantage de la multimodalité biométrique est notamment de rendre plus difficile la collecte des biométries de la personne à son insu.
Le dispositif autorisé permet également de limiter de manière significative le risque de détournement de finalité grâce à de nombreuses mesures de sécurité, parmi lesquelles un stockage des données dans le lecteur biométrique et non sur un serveur, le recours à un chiffrement dit « fort » avec une clé spécifique à chaque lecteur, une protection physique des composants, ou encore un système de signalement de toute tentative d'accès au lecteur.

De nouvelles méthodes d'authentification des personnes sur internet ont aussi vu le jour, telles que **la reconnaissance de la frappe au clavier**. En effet, comme la vitesse de frappe sur un clavier est propre à chaque individu, il est possible de reconnaître une personne sur la base de la saisie d'une séquence qu'elle a préalablement enregistrée, typiquement son identifiant et son mot de passe. Cette technologie, qui ne doit jamais se substituer aux méthodes d'authentification existantes, intervient plutôt en complément de celles-ci afin de renforcer l'authentification de la personne sans introduire de gêne particulière pour l'utilisateur. La CNIL a autorisé ce système, dès lors qu'il ciblait une population limitée.

En outre, la CNIL a constaté que certaines technologies arrivent à maturité et soulèvent de nombreuses questions. Par exemple, **la reconnaissance faciale** et les techniques d'étiquetage *tagging* investissent les réseaux sociaux et les services de stockage de photos en ligne. Le principe consiste à détecter et ajouter automatiquement, dans la photo elle-même, les noms des personnes qui y figurent. La CNIL mène actuellement une réflexion sur ce sujet, qui concerne l'ensemble des photos postées sur certains sites internet très populaires.

La reconnaissance vocale se déploie quant à elle progressivement sur les téléphones mobiles. Là encore, la technologie fait appel à internet, en transmettant la demande sur des serveurs chargés de la comprendre et d'y répondre. Ces services peuvent aussi utiliser des données se trouvant dans un téléphone, par exemple pour appeler un contact dans le carnet d'adresses.

Enfin, au cours des derniers mois, des événements ont rappelé aux personnes qu'elles génèrent de plus en plus de traces numériques. Ainsi, le logiciel *CarrierIQ* transmettait dans certains pays de nombreuses données sur l'utilisation des téléphones à l'insu de leur propriétaire, tandis que, dans le domaine des réseaux sociaux, un étudiant autrichien a démontré que toutes les données qu'il avait déposées sur Facebook avaient en réalité été conservées, malgré leur effacement supposé. ■

GROS PLAN

CONSULTATION SUR LE *CLOUD COMPUTING*

> La sécurité des données, enjeu majeur pour les entreprises ”

L'expression *Cloud computing* (traduite officiellement par la Commission générale de terminologie et de néologie par « informatique en nuage »[1]) aurait été prononcée pour la première fois en 2006 par Eric Schmidt, directeur exécutif de Google Inc. Elle désigne le déport vers « le nuage Internet » de données et d'applications qui auparavant étaient situées sur les serveurs et ordinateurs des sociétés, des organisations ou des particuliers.

Pour les entreprises, le modèle économique associé s'apparente à la location de ressources informatiques avec une facturation qui dépend souvent de la consommation réelle. La gamme d'offres correspondantes a connu un fort développement ces trois dernières années, notamment au travers du stockage et de l'édition en ligne de documents ou même des réseaux sociaux par exemple, ce qui fait dire à certains que « *demain, l'endroit où l'on stockera ses données mais celui aussi où l'on fera tourner ses applications ne sera plus le PC… mais une nébuleuse de méga-centres informatiques dispersés sur la planète.* »[2]

LE CLOUD : UNE NOTION PROTÉIFORME

Sur la base des travaux du NIST (*National Institute for Standards and Technologies*), on peut retenir cinq critères pour définir le *Cloud computing* :

▸ **La simplicité d'un service à la demande :** un utilisateur peut, de manière unilatérale, immédiate et généralement sans intervention humaine, avoir à sa disposition les ressources informatiques dont il a besoin (temps de calcul de serveurs, capacité de stockage, etc.). La complexité de la gestion des ressources informatiques disparaît, puisque les problèmes de conception, d'administration et de maintenance se trouvent déportés chez le prestataire.

▸ **Une extrême flexibilité :** les ressources mises à disposition ont une capacité d'adaptation forte et rapide à une demande d'évolution, généralement de manière transparente pour l'utilisateur. Cette capacité d'adaptation et d'extension des ressources paraîtra souvent sans limites à l'utilisateur.

[1] *Cf. JO du 6 juin 2010* / [2] *Extrait de l'article « Vers la fin de l'ère du PC – Microsoft dans le piège Internet » de Dominique Nora, correspondant du Nouvel Observateur à San Francisco, 1er mai 2008.*

▸ **Un accès « léger » :** l'accès aux ressources ne nécessite pas d'équipement ou de logiciel propriétaire ou dédié. Il se fait au travers d'applications facilement disponibles (parfois libres), généralement depuis un simple navigateur Internet. Ceci permet un accès depuis quasiment n'importe quel appareil disposant d'un accès réseau (ordinateur fixe ou portable, assistant personnel, téléphone portable) presque indépendamment de ses capacités, de sa configuration et de son système d'exploitation.

▸ **La mutualisation des ressources :** les ressources informatiques du prestataire sont configurées pour être utilisées par une multitude de machines et sont souvent réparties dans différents centres d'hébergements (éventuellement dans différents endroits de la planète). Elles sont allouées de manière dynamique en fonction des demandes des clients, de sorte qu'il peut être difficile, voire impossible, de savoir physiquement où sont stockées les données à un moment donné (et où sont réalisés les traitements).

▸ **Le paiement « à l'usage » :** généralement, le paiement de la prestation de *Cloud computing* se fait proportionnellement à l'usage, même lorsque le paiement se fait de manière indirecte par l'affichage de publicité par exemple. Le client paye donc en fonction des applications, du temps de calcul ou d'utilisation, ou encore de la capacité de stockage qui lui sont fournies.

On distingue également trois modèles de service et quatre modèles de déploiement.

Les modèles de services correspondent à différents types de services offerts par le *Cloud* :

• La mise à disposition d'infrastructures (de calcul, de stockage, etc.) : *Infrastructure as a Service*, « IaaS ». Ces services sont les évolutions des services d'hébergement classiques en mode « Cloud ».

• Les applications en ligne : *Software as a Service*, « SaaS ». Ce type de service est la forme la plus répandue et la plus connue de *Cloud computing* (Google Apps, Salesforce, etc.).

• Les plateformes de développement en ligne : *Platform as a Service*, « PaaS ». Destinés aux fournisseurs d'application, ces services fournissent tous les outils nécessaires pour développer une application, qui pourra ensuite être proposée en SaaS au client final.

Les modèles de déploiement dépendent du degré de mutualisation des infrastructures :

• Le ***cloud privé*** est une infrastructure dédiée au client. Quand les infrastructures de plusieurs clients ayant les mêmes intérêts sont mutualisées, on parle également de « Cloud communautaire ».

• À l'inverse, le ***cloud public*** est une infrastructure mutualisée entre tous les clients d'un même prestataire. Dans ce cas, l'utilisateur final n'a généralement aucun moyen de savoir quels autres usagers sont présents sur le serveur, le réseau ou le disque sur lequel ses tâches sont exécutées.

• Enfin, le ***cloud hybride*** consiste à mettre en place deux entités de Cloud de nature distincte et prévoir des mécanismes de transferts des données entre ces entités.

Le marché représenté par le *Cloud* est gigantesque et présente un caractère stratégique pour l'ensemble des entreprises utilisant des services informatiques. La Commission européenne en a d'ailleurs fait un axe majeur de son Agenda numérique (*Digital Agenda*), notamment pour aider les PME européennes à profiter au maximum du *Cloud computing*. En effet, pour ce type d'entreprises, le *Cloud* est présenté comme permettant une réduction importante des coûts tout en garantissant une bonne qualité de prestation. De plus, l'élasticité inhérente au *Cloud* permet d'accompagner la croissance des entreprises et de leur permettre de mieux gérer les variations d'activité.

En revanche, de nombreuses entreprises nourrissent des craintes sur les implications juridiques et techniques du passage au *Cloud*, au premier rang desquelles figure la confidentialité des données.

▸▸▸

LE DÉVELOPPEMENT DU *CLOUD COMPUTING* : UN ENJEU POUR LES DONNÉES PERSONNELLES

Du point de vue des utilisateurs, le *Cloud computing* se caractérise par une gestion simplifiée des services et des ressources informatiques (montée en charge « en un clic », facturation à la demande, etc.). Pour le prestataire, le *Cloud computing* constitue une véritable évolution de l'externalisation, avec le recours à de multiples serveurs répartis en différents points géographiques, pouvant être situés partout dans le monde. On assiste ainsi à une dématérialisation des ressources qui sont accessibles en tout lieu et à tout moment.

La localisation des données et la détermination de la loi applicable aux données deviennent ainsi des enjeux majeurs. En effet, les données sont transférées sur différents serveurs qui peuvent être situés en tout point de la planète. Il est alors difficile de les encadrer efficacement, d'autant plus que les clients ne sont souvent pas en mesure d'identifier à l'avance sur quels serveurs leurs données seront stockées.

Dans ces conditions, il peut s'avérer compliqué pour les personnes concernées d'exercer leurs droits. Auprès de quelle entité la personne concernée doit-elle faire valoir ses droits ? Comment s'assurer qu'elle bénéficie d'un droit d'accès lorsque ses données sont stockées sur un serveur situé à l'autre bout du monde ? Comment vérifier que les données sont effectivement effacées lorsqu'elles ont fait l'objet de sauvegardes sur de multiples serveurs ?

Par ailleurs, afin d'optimiser la répartition des ressources entre les différents centres de stockages, les données à caractère personnel font l'objet d'échanges permanents entre le client et le prestataire. La gestion informatique du client est alors parfois entièrement confiée au prestataire opérant ainsi un transfert de risques vers ce dernier. Dans certains cas, il arrive que le client utilise les services de *Cloud computing* d'un prestataire qui fait lui-même appel à un autre prestataire, pour son infrastructure par exemple. La détermination des rôles des différents acteurs et l'identification de leurs qualifications respectives peut alors s'avérer particulièrement complexe, et ce d'autant plus que le public concerné par les offres de *Cloud computing* est très varié : de la petite entreprise à la multinationale, en passant par les particuliers.

Enfin, compte tenu de la multiplicité des espaces de stockage et de l'accessibilité permanente aux données, le niveau de sécurité offert par le *Cloud computing* est une question majeure.

Dans ce contexte, la CNIL souhaite prendre position sur ce sujet pour clarifier l'encadrement juridique et technique du *Cloud computing*. La CNIL souhaite notamment identifier les risques du passage au cloud et formuler des recommandations à destination des clients et des prestataires. **Compte tenu de l'importance du sujet et avant de produire ses recommandations, la CNIL a lancé d'octobre à décembre 2011 une consultation publique afin de recueillir l'avis des acteurs du *Cloud* sur la question de la protection et de la sécurité des données personnelles dans le *Cloud*.**

DES PROPOSITIONS ET UNE CONSULTATION POUR CLARIFIER LA PROTECTION DES DONNÉES DANS LE *CLOUD*

La consultation lancée par la CNIL a permis de soumettre à la réflexion des propositions concrètes relatives aux différents aspects de la protection des données personnelles.

La qualification des parties

Aux termes de l'article 3 de la loi « Informatique et Libertés », le responsable de traitement est défini comme la personne physique ou morale qui détermine les finalités et les moyens du traitement de données à caractère personnel. Le sous-traitant, quant à lui, traite des données à caractère personnel pour le compte du responsable de traitement et selon ses instructions (article 35 de la loi « Informatique et Libertés »).

La CNIL a proposé l'analyse suivante :

- le client est nécessairement responsable de traitement puisqu'il détermine

les finalités et les moyens de traitement des données ;
• le prestataire est présumé sous-traitant, à moins que l'application d'un faisceau d'indices[1].

Par ailleurs, dans le cadre de la réflexion menée sur la révision de la directive 95/46/CE, la CNIL a soumis la création d'un statut légal pour le sous-traitant, afin de faire peser sur ce dernier un certain nombre d'obligations spécifiques.

Le droit applicable

Le *Cloud computing* étant basé sur l'utilisation de multiples serveurs situés en divers points de la planète, les difficultés liées à la détermination du droit applicable sont évidentes. En effet, la flexibilité et la fluidité des transferts de données rendent potentiellement applicables autant de lois que de pays dans lesquels se trouvent les serveurs traitant les données. Il est pourtant particulièrement important d'identifier la loi applicable, afin notamment de déterminer quelles obligations pèsent sur le responsable de traitement.

Aux termes de l'article 5 de la loi « Informatique et Libertés », la loi s'applique si le responsable de traitement :
• a son établissement sur le territoire français ou ;
• a recours à des moyens de traitement situés sur le territoire français (sans être établi sur le territoire d'un autre État membre).

Bien que favorable à une interprétation large de la notion de moyen de traitement, la CNIL a interrogé les acteurs du *Cloud* sur les critères qui devraient être pris en compte pour déterminer la loi applicable.

L'encadrement des transferts

Aux termes de l'article 68 de la loi « Informatique et Libertés », les données à caractère personnel ne peuvent faire l'objet d'un transfert que si l'État dans lequel se situe le destinataire de données assure un niveau de protection adéquat. L'article 69 de cette même loi prévoit expressément les outils permettant d'encadrer ce type de transferts : clauses contractuelles types, règles internes d'entreprises (ou *BCR, Binding Corporate Rules*), Safe Harbor ou exceptions.

Toutefois, le recours à ces outils **implique de connaître le ou les pays dans lesquels les données vont être traitées, élément essentiel pour procéder aux déclarations/autorisations auprès de la CNIL et pour informer les personnes concernées des transferts vers ces pays.**

Or, le *Cloud computing* est le plus souvent fondé sur une absence de localisation stable des données. Le client est donc rarement en mesure de savoir où se trouvent les données et où elles sont transférées et stockées. Dans ce contexte de multiplication des lieux potentiels de stockage des données, les instruments juridiques permettant d'encadrer les transferts de données susmentionnés montrent leurs limites. Afin de résoudre cette difficulté, la CNIL a demandé aux prestataires de services s'ils étaient prêts à intégrer les clauses contractuelles types dans leurs contrats de prestations de services, et invitait les acteurs du Cloud à réfléchir à la faisabilité de BCR sous-traitants.

Ces « BCR sous-traitants » permettraient à un client de confier ses données personnelles à un sous-traitant en étant assuré que les données transférées au sein du groupe de ce dernier bénéficient d'un niveau de protection adéquat.

La sécurité des données

Dans le cas d'un organisme ayant recours à une offre de *Cloud computing*, la gestion de la sécurité de ses données est largement déléguée au prestataire, auprès duquel il est souvent difficile d'obtenir des garanties sur le niveau de sécurité réel. En application de l'article 35 de la loi de 1978 modifiée, le sous-traitant doit « *présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité* », incombant au responsable de traitement, ce dernier ayant quant à lui « *une obligation de veiller au respect de ces mesures [de sécurité et de confidentialité]* ».

La CNIL considère que les exigences de sécurité doivent être matérialisées dans un contrat afin d'établir clairement les responsabilités et rôles des parties. Ce contrat permet notamment de traiter efficacement les incidents pouvant aboutir à une perte ou à une divulgation de données. Toutefois, de nombreuses offres de *Cloud* sont fondées sur des contrats d'adhésion type qui ne peuvent pas être négociés par le client. Afin de recenser les

[1] *Tel que proposé dans le rapport relatif « aux questions posées en matière de protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques », http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/20100909-externalisation.pdf*

▸▸▸

pratiques des acteurs, la CNIL a demandé l'avis de ceux-ci sur les relations contractuelles entre client et prestataire.

En accord avec les recommandations de l'ENISA (Agence européenne de la sécurité des systèmes d'information), la CNIL conseille aux responsables de traitement d'effectuer une analyse de risques lorsqu'ils souhaitent utiliser le *Cloud computing*, afin d'évaluer l'impact de cette évolution de leur système d'information. Cette procédure encore trop peu répandue est une méthode efficace pour évaluer précisément l'équilibre coûts-bénéfices d'un projet. La CNIL a demandé aux contributeurs de faire part de leurs commentaires sur une telle recommandation.

En termes de mesures de sécurité concrètes, la CNIL insiste sur l'importance de certains aspects de la sécurité :

- **la protection externe du réseau :** pare-feu, serveur proxy avec analyse de contenu, détection d'intrusion, etc. ;
- **la protection du terminal** (PC portable, assistant personnel, téléphone portable) : antivirus, système d'exploitation et des logiciels mis à jour régulièrement, firewall ;
- **le chiffrement des liaisons**[1] **la traçabilité :** conserver un historique des connexions et des opérations effectuées sur les données (en effet, dans de nombreuses offres, y compris de grandes sociétés, les évènements de type « administration » qui permettent par exemple la création/suppression de compte ou les accès aux données ne sont pas enregistrés) ; de manière à garantir la confidentialité des échanges ;
- **la gestion des habilitations :** par exemple, le compte d'une personne ayant quitté l'organisme doit être immédiatement désactivé car le fait qu'elle n'a plus accès aux locaux ne l'empêche pas d'accéder aux systèmes d'information ;
- **l'authentification :** de même, l'authentification doit être renforcée. Le recours à une authentification forte s'avérera nécessaire dès lors que les données accédées sont sensibles et/ou volumineuses.

La CNIL souligne l'importance du chiffrement, seul moyen d'empêcher que les administrateurs informatiques du prestataire aient accès aux données qui lui sont confiées. Les acteurs étaient donc invités à se prononcer sur l'opportunité des mesures proposées dans le cas du *Cloud computing*, et notamment sur la question du chiffrement.

La question de la réversibilité et de la destruction des données en fin de contrat est également essentielle et doit être prise en compte par le client avant la souscription à un service de *Cloud computing*. En outre, la CNIL a identifié le besoin pour de nouvelles normes de sécurité incluant la question de la protection des données personnelles dans le *Cloud*, afin de renforcer la transparence vis-à-vis des clients. La CNIL invitait donc les acteurs à s'exprimer sur ces points.

Alors que cette consultation publique était la première organisée par la CNIL, les nombreuses réponses reçues (49) montrent qu'il existe une grande attente du secteur sur la position de la CNIL. En 2012, la CNIL publiera les conclusions de cette consultation, ainsi que des recommandations sur les mesures à prendre pour la protection des données personnelles lors du passage au *Cloud computing*. En parallèle, la CNIL continuera à coordonner son action avec ses homologues européens ainsi qu'avec la Commission européenne, compte tenu du caractère international des problématiques liées au *Cloud computing*. Un avis du G29 (groupe des CNIL européennes) est d'ailleurs en préparation. ■

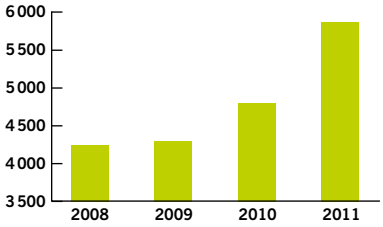
[1] *Par exemple en ayant recours à https (HyperText Transfer Protocol Secure) pour sécuriser la navigation.*

6. PROTÉGER ET CONTRÔLER

UN NOMBRE RECORD DE PLAINTES

Dans le prolongement de l'augmentation constatée en 2010, l'année 2011 a encore connu une nette augmentation des plaintes adressées à la CNIL. Avec 5738 plaintes reçues, un nouveau record vient d'être établi.

Évolution du nombre de plaintes reçues par la CNIL



Ces chiffres sont d'autant plus remarquables qu'ils ne tiennent pas compte des milliers de demandes écrites de particuliers directement traitées par le Service d'orientation et de renseignement du public (SORP) de la CNIL, autrefois comptabilisées comme plaintes. Ils n'intègrent pas, non plus, les multiples questions téléphoniques de particuliers qui ont été prises en charge par le SORP et par le service des plaintes.

5738
PLAINTES REÇUES

Ils révèlent de façon incontestable **l'intérêt de plus en plus marqué des personnes pour la protection de leurs données personnelles et la sensibilité de cette question**.

Comme en 2010, si tous les secteurs sont concernés par cette hausse d'activité, les problématiques liées au **« droit à l'oubli sur internet »** + 42 % entre 2010 et 2011 (pour demander la suppression de contenus – textes, photographies, vidéos – qui apparaissent sur des sites ou des blogs) et à la **vidéosurveillance** + 30% entre 2010 et 2011 sont en nette progression. La CNIL continue également de recevoir un nombre important de plaintes concernant les secteurs de la banque et du crédit, du travail (notamment sur les questions de surveillance des salariés) et du commerce (gestion des fichiers de clients ou d'envoi de publicité).

Le service de « plainte en ligne », accessible de façon simple sur **www.cnil.fr**, permet également d'expliquer ce nombre important de plaintes reçues. En effet, **26 % des personnes ont utilisé internet en 2011 pour adresser leur plainte à la CNIL** ; elles n'étaient que 8 % à le faire en 2010.

Les délais d'instruction varient de quelques jours à plusieurs mois en fonction de la complexité de la plainte, de la qualité des réponses apportées par le responsable du fichier ou encore des actions entreprises pour instruire le dossier (contrôle sur place, mise en demeure, procédure de sanction…). Malgré l'augmentation constante des volumes de plaintes reçues, la réduction de ces délais de résolution continue à être l'une des priorités du service des plaintes afin d'apporter un service de qualité à ses usagers. ■

INFOS +

La plainte en ligne, comment ça marche ?

1. Je vais sur www.cnil.fr et je clique sur « plainte en ligne ».
2. Je sélectionne le cas qui me concerne (suppression de contenus sur internet, opposition à recevoir de la publicité, accès ou mise à jour de mes données).
3. Je reçois une information courte et précise sur le cas sélectionné.
4. Je vérifie que j'ai bien exercé mes droits d'accès, d'opposition ou de rectification des données qui me concernent ; des modèles de courriers sont proposés par la CNIL.
5. J'accède au formulaire de plainte en ligne où je peux préciser mon problème et joindre tout document utile (copie des échanges avec le responsable de fichier, copie des publicités reçues, etc.).
6. L'envoi de ma plainte est sécurisé et je reçois un accusé de réception d'abord par e-mail puis par courrier postal.
7. Mon dossier est géré par le service des plaintes de la CNIL, que je peux contacter si je le souhaite (par courrier ou téléphone).
8. À l'issue de l'instruction de ma plainte (variable en fonction de la complexité du dossier), la CNIL me précise les démarches accomplies auprès du responsable du fichier concerné et les résultats obtenus.

LE DROIT D'ACCÈS INDIRECT

En application de l'article 41 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 (STIC, JUDEX, ancien fichier des renseignements généraux, etc.) doivent en effectuer la demande par écrit auprès de la CNIL.

En 2011, la CNIL a été destinataire de 2 099 demandes de droit d'accès indirect contre 1 877 en 2010. Ce nombre, bien que demeurant inférieur à celui des années antérieures, marquées par les effets du débat sur la création du fichier EDVIGE et la réorganisation des services de renseignement du ministère de l'Intérieur, atteste d'une augmentation sensible **(plus 12 % par rapport à 2010)**. Elle résulte principalement de la progression des demandes portant sur les fichiers d'antécédents judiciaires (STIC et JUDEX), formulées par des personnes qui se sont vues opposer une décision défavorable pour accéder à certains types d'emploi ou qui appréhendent d'y être éventuellement confrontées. Aujourd'hui, on évalue à 1,3 million le nombre d'emplois concernés par des procédures administratives.

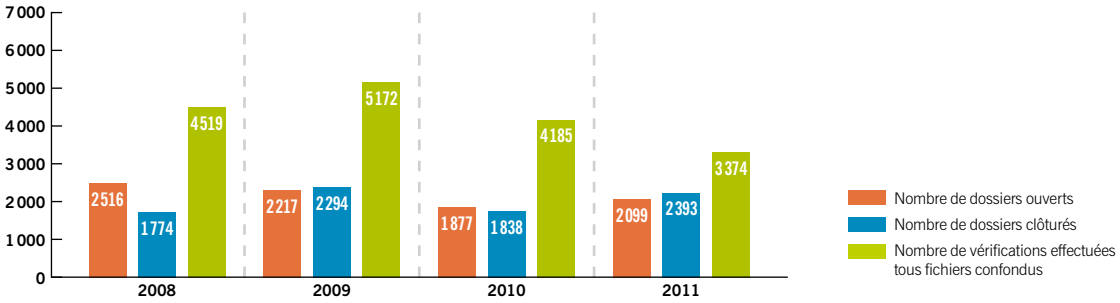
2099
DEMANDES DE DROIT D'ACCÈS INDIRECT

La reconnaissance par le Conseil d'État, par un arrêt du 29 juin 2011 *(CE n° 339147 – 10ème et 9ème sous-sections réunies)*, du droit d'accès des héritiers aux données bancaires enregistrées dans le fichier FICOBA (fichier des comptes bancaires et assimilés), en leur qualité « d'ayant droit du solde des comptes détenus par la personne décédée », a également eu pour effet d'accroître les demandes de droit d'accès en ce domaine. Leur traitement demeure néanmoins subordonné à l'adoption d'un protocole d'accord avec l'administration fiscale qui devrait intervenir prochainement.

Chaque demande de droit d'accès indirect implique des vérifications dans plusieurs fichiers afin de répondre aux attentes de la personne concernée. Ainsi **les 2 099 demandes reçues en 2011 imposent 4 833 vérifications** dans différents fichiers, au premier rang desquels les fichiers de police judiciaire de la police et de la gendarmerie nationales (STIC et JUDEX), les fichiers des services de l'Information Générale du ministère de l'Intérieur (EASP et PASP[1]) et le Système d'Information Schengen (SIS). ▸▸▸

[1] Fichiers relatifs aux « Enquêtes administratives liées à la sécurité publique » et à la « Prévention des atteintes à la sécurité publique ».

Évolution des demandes de droit d'accès indirect 2008-2011

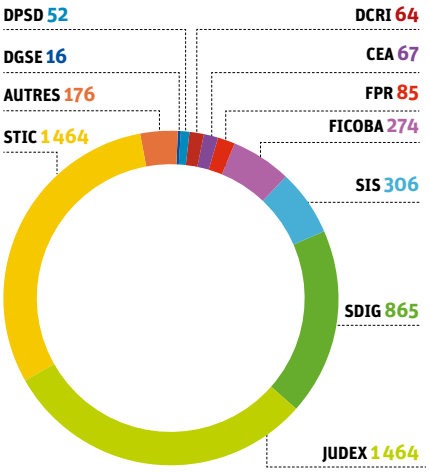


INFOS +

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 2011 : les principaux fichiers concernés par les vérifications



STIC : Système de Traitement des Infractions Constatées. / JUDEX : Système Judiciaire de Documentation et d'Exploitation. / SDIG : Services de l'Information Générale. / SIS : Système d'Information Schengen. / FICOBA : Fichier des comptes bancaires et assimilés. / FPR : Fichier des Personnes Recherchées. / CEA : Direction centrale de la sécurité du Commissariat à l'énergie atomique. / DCRI : Direction Centrale du Renseignement Intérieur. / DPSD : Direction de la Protection et de la Sécurité de la Défense. / DGSE : Direction Générale de la Sécurité Extérieure. / Autres : Fichier des Courses et Jeux (FICOJ), Fichier des Interdits de Stade (FNIS), Système de gestion informatisée des détenus dans les établissements pénitentiaires (GIDE), Europol…

▸▸▸

3 374 vérifications ont été menées au cours de l'année 2011 qui ont permis d'arriver au terme de la procédure pour 2 393 demandes, engagées pour la plupart au cours des années précédentes. Plus de 60 % de ces vérifications ont porté sur les fichiers de police judiciaire avec les résultats suivants.

Fichiers de police judiciaire	STIC	JUDEX
Nombre de vérifications effectuées	1 112	946
Nombre de personnes inconnues	224	648
Nombre de personnes enregistrées uniquement en tant que victime	222	71
Nombre de fiches « mis en cause » vérifiées*	666	227
Fiches exactes	28 %	38 %
Fiches rectifiées (qualification des faits entraînant ou non une réduction du délai de conservation, ajout de mentions pour tenir compte des suites judiciaires réservées aux infractions enregistrées…)	44 %	30 %
Fiches supprimées	28 %	32 %

** Chaque fiche individuelle peut comporter une ou plusieurs procédures d'infraction / [2] Fichiers relatifs aux « Enquêtes administratives liées à la sécurité publique » et à la « Prévention des atteintes à la sécurité publique ».*

FICHIERS D'ANTÉCÉDENTS JUDICIAIRES ET PROBLÉMATIQUE D'EMPLOI : LES AVANCÉES DE LA LOPPSI

Sur la base d'un amendement présenté par Madame Delphine BATHO, Députée des Deux-Sèvres *(membre de la mission d'information parlementaire sur les fichiers de police)*, l'article 230-8 du code de procédure pénale, issu de la loi n°2011-267 du 14 mars 2011, prévoit l'adjonction systématique d'une mention dans les fichiers d'antécédents judiciaires pour tous les faits ayant bénéficié d'une décision de classement sans suite et ce, quel qu'en soit le motif *(rappel à la loi, dédommagement de la victime, préjudice peu important, injonction thérapeutique…)*.

Réservé jusqu'alors aux seules décisions de classement sans suite pour « *absence d'infraction* » ou « *insuffisance de charges* », l'ajout de mention a pour effet d'exclure les affaires concernées du champ des enquêtes administratives menées pour l'accès à certains emplois publics ou privés (agents de sécurité privée, personnes exerçant leur activité en zone aéroportuaire, agents de police municipale, agents de sûreté ferroviaire, etc.).

Si les possibilités d'effacement demeurent strictement limitées *(faits ayant bénéficié d'un jugement de relaxe ou d'acquittement, d'une ordonnance de non-lieu ou d'une décision de classement sans suite pour « absence d'infraction » ou « insuffisances de charges »)* et subordonnées à l'accord du procureur de la République, cette évolution particulièrement attendue va permettre d'**atténuer l'effet pénalisant de la consultation de ces fichiers en termes d'emploi**.

L'application effective et immédiate de cette disposition à l'ensemble des enregistrements existants *(environ 6,5 millions de personnes mises en cause enregistrées dans le fichier STIC et 2,5 millions dans le fichier JUDEX en 2011)* se heurte néanmoins aux difficultés structurelles de mise à jour de ces fichiers qui dépend, dans une large proportion, de la communication aux services de police, par les procureurs de la République, des suites judiciaires intervenues pour chacune des infractions relevées.

Si des progrès sensibles méritent d'être soulignés, une mise à jour presque en temps réel de ces fichiers ne pourra intervenir, à l'avenir, que par le biais de l'interconnexion prévue entre l'application CASSIOPEE du ministère de la Justice et le « Traitement des Procédures Judiciaires » (TPJ), appelé à succéder prochainement aux fichiers STIC et JUDEX.

FOCUS

Monsieur P. 35 ans, a sollicité la délivrance d'une carte professionnelle pour exercer dans la sécurité privée. Il a parallèlement saisi la CNIL d'une demande de droit d'accès indirect aux fichiers de police judiciaire. Au terme des vérifications, deux affaires de nature contraventionnelle ont été supprimées du STIC et les deux restantes ont fait l'objet d'une mise à jour par mention des décisions de classement sans suite pour « carence du plaignant » et « préjudice peu important » dont il avait bénéficié. Monsieur P. qui, malgré ces inscriptions, a pu obtenir sa carte professionnelle ne devrait, dès lors, pas avoir de difficultés à obtenir son renouvellement à l'avenir car il est désormais inconnu administrativement de ce fichier.

Ça la fiche mal !

Absence de mise à jour par les Parquets

▸ Madame B., 34 ans, a été placée en garde à vue pour détention et usage d'un faux permis de conduire étranger. À la suite de la réception du certificat d'authenticité de son permis, établi par le ministère des Transports de son pays d'origine, le procureur de la République a informé Madame B. qu'il avait décidé de procéder à un classement sans suite pour insuffisances de charges. Il a également ordonné que son permis, placé sous scellés, lui soit restitué. Madame B. a souhaité saisir la CNIL pour vérifier son éventuel enregistrement dans le fichier STIC à la suite de cette affaire. Il s'avère qu'elle faisait effectivement l'objet d'un enregistrement pour cette affaire qualifiée de *« faux et usage de faux, obtention frauduleuse de documents administratifs »*, à laquelle s'applique un délai de conservation de 20 ans. Les vérifications de la CNIL ont assuré l'effacement de ces informations.

▸ Monsieur K, 39 ans a été destinataire en 2006 d'une lettre du procureur de la République l'informant qu'il faisait droit à sa demande d'effacement du fichier STIC pour des faits de *« recel »* dans la mesure où il avait bénéficié d'un classement sans suite pour insuffisances de charges. C'est donc avec surprise que Monsieur K. a appris, à l'occasion de l'examen de sa demande de naturalisation, que ces faits demeuraient inscrits dans ce fichier et pouvaient, dès lors, nuire à son obtention. Les vérifications de la CNIL ont permis d'assurer la suppression effective de cet enregistrement conformément à la demande du procureur de la République.

Fichage d'un mineur

▸ Monsieur et Madame G. ont souhaité engager une procédure de droit d'accès indirect aux fichiers de police judiciaire pour leur fils mineur de 17 ans afin de s'assurer de l'état des informations le concernant enregistrées dans le STIC. Leur fils avait été en garde à vue pour des faits de *« dégradation de biens privés »* puis avait bénéficié d'un jugement de relaxe. Ce dernier n'a été effectivement porté à la connaissance des services gestionnaires du fichier STIC, par le parquet concerné, qu'à l'occasion des vérifications menées par la CNIL. Il a eu pour effet la suppression immédiate de l'enregistrement.

▸ Madame M. est intervenue auprès de la CNIL pour son fils mineur de 17 ans qui a été mis en cause puis relaxé pour des faits d'*« atteintes sexuelles »* qui se sont déroulées dans son établissement scolaire. Son fils désirant intégrer la gendarmerie nationale, elle voulait s'assurer de l'absence d'inscription de cette affaire dans les fichiers de police judiciaire. En l'occurrence, les faits qui étaient toujours enregistrés au moment de sa saisine dans le fichier JUDEX, ont été effacés au terme des vérifications de la CNIL.

Mauvais enregistrement initial des faits

▸ Monsieur G., 57 ans, commandant de bord depuis plus de vingt ans au sein d'une compagnie aérienne, a été confronté à des difficultés de renouvellement de son badge aéroportuaire. Si ce badge lui a finalement été délivré avec retard, sa validité a été limitée à 1 an au lieu de 3 ans. N'ayant pu obtenir de plus amples explications, Monsieur G. a souhaité exercer son droit d'accès indirect afin de déceler l'origine de ses difficultés. Les vérifications menées par la CNIL ont conduit à la suppression de son enregistrement dans le fichier JUDEX pour une affaire de *« travail clandestin, abus de biens sociaux et escroquerie »* dans laquelle il n'était pas mis en cause. Monsieur G était juste cité dans la procédure mais ni en tant que mis en cause ni en tant que victime. Lors de l'intégration du compte rendu d'enquêtes dans JUDEX, il y a été intégré à tort comme l'auteur de ces faits ce qui a été à l'origine de ses difficultés.

▸ Monsieur C., 27 ans, exerçant la profession de transporteur de fonds, a souhaité exercer son droit d'accès indirect aux fichiers de police judiciaire, après avoir découvert, au terme de l'enquête administrative dont il a fait l'objet, son inscription dans le STIC pour des faits *« d'agression sexuelle »*. Monsieur C. a été particulièrement surpris par cette mention. En effet, s'il avait effectivement souvenir qu'un élève du centre de vacances dans lequel il séjournait, alors qu'il était mineur, a été victime de tels faits, pour sa part il a été seulement entendu au même titre que l'ensemble des enfants présents dans la chambre. Seuls deux d'entre eux ont été poursuivis et condamnés. À la suite des démarches de la CNIL, cette affaire a été supprimée dans la mesure où, conformément à ses dires, il n'était pas mis en cause.

▸ Monsieur L., 35 ans, agent de police municipale, a souhaité exercer son droit d'accès au fichier STIC ayant découvert l'existence d'un enregistrement le concernant se rapportant à un incident, dans l'exercice de ses fonctions, avec le propriétaire d'un autre chien qui ▸▸▸

... ça la fiche mal !

▸▸▸ avait conduit ce dernier à déposer plainte contre lui. Au terme de vérifications menées par la CNIL, les faits ont été supprimés du fichier STIC dans la mesure où les faits, de nature contraventionnelle, n'avaient pas à y figurer.

Expiration du délai de conservation

▸ Monsieur C., 24 ans, mécanicien aéronautique, a souhaité exercer son droit d'accès indirect aux fichiers de police judiciaire, à la suite de la décision de refus de délivrance de son badge aéroportuaire, indispensable à l'exercice de sa profession. Les vérifications effectuées par la CNIL, ont conduit à la suppression de son signalement dans le STIC pour une affaire de « *vol simple* » dont le délai de conservation, fixé à 5 ans, était expiré.

Les usurpations d'identité

▸ Mademoiselle B., 24 ans, en formation d'hôtesse de l'air, a saisi la CNIL d'une demande de droit d'accès indirect après que sa sœur, mineure, lui ait avoué avoir présenté sa pièce d'identité lors de son interpellation par les services de police pour « *vol à l'étalage* ». Si Mademoiselle B. avait déjà été alertée sur l'utilisation de son identité par un tiers après avoir reçu plusieurs procès-verbaux de sociétés de transport, ce dernier fait, de nature à compromettre son avenir professionnel, l'a conduit à déposer immédiatement plainte au commissariat. La comparaison d'empreintes effectuées, sur la base du relevé effectué lors de son dépôt de plainte, a permis à la CNIL de s'assurer de la suppression de l'inscription la concernant.

UN NOUVEAU RAPPORT PARLEMENTAIRE SUR LES FICHIERS DE POLICE

80
FICHIERS DE POLICE RECENSÉS

Auditionnée à plusieurs reprises par les auteurs de ce rapport, la Commission se félicite que les conclusions des députés soient très largement cohérentes avec son analyse sur de nombreuses questions.

Les députés Delphine BATHO et Jacques Alain BENISTI soulignent notamment l'amélioration des relations entre le ministère de l'Intérieur et notre Commission. Ils mettent également en avant le développement d'une culture « Informatique et Libertés » dans la gestion des fichiers de police, et l'engagement d'un processus de régularisation des traitements n'ayant fait l'objet d'aucune formalité auprès de notre Commission.

Ce mouvement reste néanmoins très incomplet et doit être poursuivi au cours de l'année à venir. Dans leur dernier rapport du 21 décembre 2011, les députés ont procédé, comme à l'occasion de leurs précédents travaux, à un recensement de l'ensemble des traitements mis en œuvre par les services du ministère de l'Intérieur ou actuellement en cours de développement. Les conclusions de cet exercice font apparaître l'existence de 80 fichiers (contre 58 en mars 2009 dans le premier rapport), dont un certain nombre demeurent encore illégaux au regard des dispositions de loi « Informatique et Libertés ». La CNIL s'est ainsi rapprochée du ministre de l'Intérieur pour obtenir les informations nécessaires, et connaître les suites éventuelles qu'il compte donner aux conclusions de ces travaux. ■

LES CONTRÔLES

L'année 2011 a été une année importante pour la CNIL dans le cadre de son activité de contrôle. En effet, d'une part, la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 (LOPPSI 2) a étendu les pouvoirs de la CNIL en lui confiant le contrôle des dispositifs dits de « vidéoprotection ». D'autre part, la loi du 29 mars 2011 relative au Défenseur des droits a sensiblement modifié les conditions d'exercice des pouvoirs de contrôle de la CNIL.

En application de la jurisprudence de la Cour européenne des droits de l'homme (16 avril 2002 Société Colas Est c/France) et du Conseil d'État (arrêt PRO DECOR et INTER CONFORT du 6 novembre 2009), la CNIL informe, avant de commencer ses opérations de contrôle, les responsables de locaux professionnels privés de leur droit d'opposition et de la possibilité qu'ils ont de l'exercer.

La loi du 29 mars 2011 a complété la loi « Informatique et Libertés » afin de préciser les conditions dans lesquelles l'autorité judiciaire peut être saisie pour autoriser le contrôle en cas d'opposition. Ainsi, la présidente de la CNIL peut saisir le juge des libertés et de la détention (JLD), qui doit se prononcer dans un délai de 48 heures.

On doit relever qu'en 2011, 3 organismes ont exercé leur droit d'opposition. Chaque fois qu'elle a été saisie, l'autorité judiciaire a autorisé par ordonnance le déroulement des opérations de contrôle.

Surtout, la loi de mars 2011 a introduit la possibilité, pour la CNIL, de saisir le juge des libertés et de la détention compétent préalablement aux opérations de contrôle, afin que celui-ci autorise la visite. Dès lors, le responsable des lieux concerné ne peut s'opposer au contrôle de la CNIL. Cette faculté de saisir préalablement le juge peut s'exercer lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie.

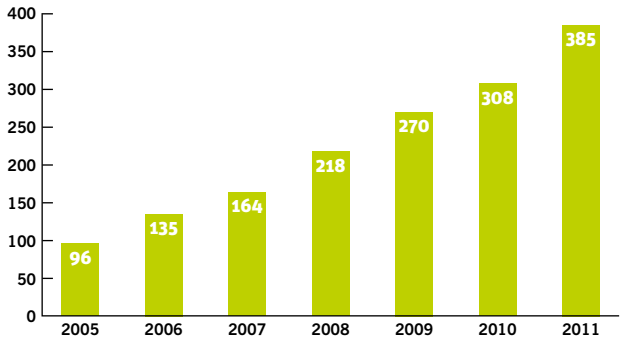
En 2011, la CNIL a utilisé 4 fois cette possibilité. À chaque fois, le juge saisi, se fondant sur les éléments apportés par la CNIL en motivation de sa requête, a autorisé le déroulement du contrôle.

L'année 2011 a encore été marquée par une nette augmentation du nombre de contrôles effectués. Ainsi, la CNIL a réalisé 385 contrôles sur l'ensemble de l'année, soit **une augmentation de 25 % par rapport à l'année précédente**. Cette augmentation illustre une nouvelle fois la volonté de la Commission d'assurer le respect de la loi « Informatique et Libertés » par l'intermédiaire de contrôles sur place.

385
CONTRÔLES

> Une augmentation de 25 % du nombre de contrôles par rapport à 2010

Évolution du nombre de contrôles depuis 2005



Concernant les organismes contrôlés au titre de la loi « Informatique et Libertés », on peut relever que 85 % appartiennent au secteur privé et 15 % relèvent du secteur public.

Concernant l'origine des contrôles, 40 % des contrôles ont été réalisés dans le cadre du programme annuel adopté

▸▸▸

par la formation plénière. Comme elle l'avait annoncé, la CNIL avait inscrit à son programme des contrôles les thèmes suivants :

• **« La sécurité des données de santé »** : au cours de l'année 2011, plus d'une vingtaine de contrôles ont concerné le traitement de données de santé. Ces contrôles ont été opérés auprès d'établissements de soins (cliniques, hôpitaux, etc.), d'hébergeurs de données de santé, d'agrégateurs de données médicales, etc.

• **« Client/prospect : peut-on échapper au traçage ? »** : une vingtaine de contrôles ont été effectués au cours de l'année 2011 ; ils ont principalement concerné des sites de commerce en ligne (problématique du nouveau régime juridique des « cookies »), des prestataires intervenant en matière de marketing (routeurs et agences de publicité) ainsi que des entreprises intervenant dans la gestion de données clients ou prospects (méga-base de données). Le bilan de ces constats devrait faire l'objet d'une communication globale courant 2012.

• **« Les agences de recouvrement/ les détectives privés »** : une dizaine de contrôles ont été effectués auprès d'agences de recherche privée et de recouvrement. Même si des contrôles sur cette thématique se dérouleront au cours du premier trimestre 2012, on peut d'ores et déjà considérer que les contrôles et les sanctions adoptées en 2006 ont fortement structuré ce milieu professionnel dont les acteurs se sont, par exemple, largement dotés de correspondants «Informatique et Libertés».

• **« Les flux de données transfrontières »** : une quinzaine de contrôles ont été réalisés auprès de multinationales basées en France qui ont obtenu des autorisations de transfert hors de l'Union européenne. Ces contrôles n'ont pas jusqu'ici démontré de manquements majeurs à l'autorisation qui leur avait été délivrée, ni mis en évidence des transferts qui ne seraient pas encadrés.

> 24 % des contrôles ont été opérés dans le cadre de l'instruction de plaintes

On peut également noter que 24 % des contrôles ont été opérés dans le cadre de l'instruction de plaintes, 11 % dans le cadre de procédures de sanction et 25 % en réaction à des sujets d'actualité, notamment des failles de sécurité portées à la connaissance de la CNIL.

Enfin, l'année 2011 aura conduit la CNIL à effectuer de nombreux contrôles dans le cadre des partenariats qu'elle a passés avec d'autres autorités administratives. On pense, ici, à la mise en œuvre du protocole signé le 6 janvier 2011 avec la Direction générale de la concurrence, de la consommation et de la répression des fraudes. Dans le cadre de cette coopération, des échanges d'informations ont permis l'intervention de la CNIL auprès des sites web sur lesquels les enquêteurs de la DGCCRF ont relevé des manquements, soit par l'envoi de courriers, soit par des procédures de contrôle sur place.

La CNIL a également effectué un certain nombre de contrôles sur la base de signalements venant de l'Inspection du travail ou de saisines du Défenseur des droits.

La liste des organismes contrôlés est disponible en annexes p 97. ■

GROS PLAN

LES « PRIMAIRES CITOYENNES » ORGANISÉES PAR LE PS

26
CONTRÔLES DE LA CNIL

L'année 2011 a notamment été marquée par l'organisation des élections dites « primaires citoyennes » organisées par le Parti socialiste (PS).
Les 9 et 16 octobre 2011, environ 2,8 millions de votants se sont déplacés pour désigner le candidat officiel du parti à l'élection présidentielle.
Cette consultation s'est appuyée principalement sur les listes électorales, qui recensent plus de 45 millions d'électeurs. Si l'accès à ces listes ne relève pas de la compétence de la CNIL et est prévu par le code électoral, les fichiers mis en œuvre aux fins de la préparation, de l'organisation, puis du déroulement de cette élection relèvent des dispositions de la loi « Informatique et Libertés ».

La Commission s'est fortement mobilisée pour encadrer, du point de vue de la protection des données personnelles, cette consultation. Par les préconisations qu'elle a formulées en amont de celle-ci puis par les contrôles qu'elle a menés durant et après les élections « primaires », elle s'est assurée du haut niveau de protection des données personnelles traitées. ▸▸▸

> “La majorité des préconisations de la CNIL ont été suivies par le PS”

FOCUS

Peut-on utiliser la liste électorale à des fins de communication politique ?

Oui. L'article L28 du code électoral permet à tout électeur, candidat et parti ou groupement politique de prendre communication et copie de la liste électorale.
Les candidats et partis politiques peuvent ainsi utiliser la liste électorale à des fins de communication politique lors d'élections nationales ou locales, y compris en dehors des périodes de propagande officielle. Ils peuvent également l'utiliser pour chercher de nouvelles sources de financement ou organiser une consultation des électeurs dans le cadre, par exemple, d'une élection primaire.
Les maires, gestionnaires des listes électorales communales pour le compte de l'État, ne peuvent pas s'opposer à la transmission de ces informations à un organisme ou une personne physique remplissant les conditions de délivrance prévues par le code électoral. Cette transmission n'est pas subordonnée au recueil du consentement de chaque électeur ou à son information, celui-ci ne pouvant pas davantage s'opposer à cette transmission.

LA PRÉPARATION DES PRIMAIRES : LE RÔLE DE CONSEIL DE LA CNIL

Dès l'annonce dans la presse de l'organisation de primaires par le PS, la CNIL a organisé des réunions de travail avec des représentants du parti, aux mois de février et d'avril 2011. Elles ont été l'occasion de rappeler les principes de la loi « Informatique et Libertés » applicables à cette consultation, puis de préciser les nécessaires garanties devant entourer les différentes phases de cette opération (limitation de la durée de conservation des données, modalités d'exercice du droit d'opposition, mesures de sécurité adaptées, etc.).

Saisie officiellement le 26 avril 2011 du dossier de formalités préalables, la Commission a examiné le 5 mai les caractéristiques des trois fichiers mis en œuvre par le PS aux fins de l'organisation des élections primaires : la liste des participants potentiels à cette consultation, le fichier de composition des lieux de vote, et le fichier de personnes souhaitant être recontactées dans le cadre des échéances électorales prévues en 2012. Au regard de la nouveauté et de l'importance de la consultation organisée, cet examen a été particulièrement minutieux.

La Commission a constaté que la majorité de ses préconisations avaient été suivies par le PS. Celui-ci avait ainsi prévu de :

• permettre aux personnes de s'opposer à figurer sur les listes de participants potentiels avant même l'agrégation des listes électorales et faciliter l'exercice de cette opposition par la mise en ligne d'un formulaire *ad hoc* ;

• ne pas enregistrer dans la liste électorale informatisée le fait de participer ou non à la consultation, de même que l'adhésion à la « charte des valeurs de la gauche » ;

• détruire les listes utilisées par les bureaux de vote pour vérifier l'identité des participants à cette consultation et permettre leur émargement à l'issue de l'investiture du candidat officiel du PS à l'élection présidentielle ;

• recueillir le consentement exprès des personnes souhaitant être contactées par le PS dans le cadre des échéances électorales de 2012, par le biais d'un formulaire de collecte spécifique ;

• mettre en place les mesures de sécurité techniques adaptées pour préserver la confidentialité des données lors de leur transmission aux bureaux de vote et durant l'intégralité de leur période d'utilisation.

> Des améliorations demandées afin de renforcer le niveau de protection des données traitées lors de cette consultation

La CNIL a toutefois demandé des améliorations sur les aspects suivants, afin de renforcer le niveau de protection des données traitées lors de cette consultation :

• en ce qui concerne les droits des personnes concernées, la Commission a recommandé que les demandes d'opposition présentées sur place, dans les bureaux de vote les jours de scrutin, soient également prises en compte par le PS, par la radiation de l'identité de la personne sur les listes papier ;

• elle a également demandé au PS d'assurer une plus large information du public sur les aspects « protection des données » de cette consultation et de faire apparaître des mentions d'information « Informatique et Libertés » sur les supports de communication ;

• sur la sécurité des données, de nouvelles mesures étaient demandées, en particulier sur le site internet utilisé pour les pré-inscriptions, le contrôle du prestataire technique et les mesures de traçabilité ;

• enfin, dans la mesure où des listes électorales papier devaient être adressées aux présidents de bureaux de vote à l'étranger, la Commission a demandé au PS de lui adresser une demande d'autorisation de transfert de données en dehors de l'Union Européenne sur ce point.

Aux termes d'un courrier en date du 28 juin 2011, le Parti socialiste a de nouveau donné suite aux demandes formulées par la CNIL le 5 mai (information, opposition, sécurité des données). Elle a ainsi considéré que le dispositif final, tel que modifié à la suite de ses recommandations, assurait un niveau suffisant de protection des données.

À la suite des réponses du Parti socialiste, la CNIL a autorisé, le 21 juillet 2011, les transferts de données hors de l'Union européenne. Elle a considéré que des garanties suffisantes, en termes techniques et de responsabilité, encadraient le transfert des listes d'émargement.

Cependant, elle a pris la décision, comme elle l'avait fait s'agissant de l'élection primaire organisée en juin 2011 par Europe Écologie - Les Verts (EE-LV), de réaliser des contrôles sur place pendant les opérations de vote.

LE DÉROULEMENT DES PRIMAIRES : LES CONTRÔLES DE LA CNIL

La CNIL a ainsi réalisé, entre octobre et décembre 2011, une série de contrôles sur place dans le cadre des élections « primaires citoyennes ».

Globalement, ces contrôles ont conduit à constater que le Parti Socialiste a mis en œuvre les recommandations de la CNIL.

▸ Tout d'abord, la Commission a constaté que **la nature des données traitées** était conforme aux engagements du Parti socialiste.

▸ Sur la sécurité et la confidentialité des données, les contrôles ont permis de s'assurer de l'effectivité des conditions de sécurité entourant la communication des listes d'électeurs entre les fédérations départementales et les bureaux de vote durant les deux tours de l'élection. Si certaines délégations de contrôle ont noté quelques insuffisances ponctuelles, il est apparu que les données ont été globalement traitées dans des conditions satisfaisantes de sécurité et de confidentialité. Au terme des opérations de vote, la CNIL s'est assurée de la destruction des listes d'électeurs émargées.

▸ S'agissant de l'information des personnes dont les données sont traitées, notamment quant à l'existence de leurs droits d'accès, de rectification et d'opposition, il est apparu que, dans chaque bureau de vote, une affiche présentant une mention d'information « Informatique et Libertés » en caractères lisibles était placardée dans les locaux des bureaux de vote. Pour autant, celle-ci n'était pas systématiquement située sur le parcours de vote.

▸ Concernant le « fichier des sympathisants » (personnes acceptant d'être recontactées à l'occasion des élections de 2012), les délégations de la CNIL ont constaté que ce traitement était constitué par l'inscription volontaire des votants, sur une liste dédiée, à l'aide d'un stylo électronique enregistrant les mentions inscrites (nom, prénom, numéro de téléphone portable, adresse électronique). Les contrôles ont permis de s'assurer que les votants étaient informés du caractère facultatif de cette inscription. Un contrôle, auprès du prestataire ayant fourni les stylos, a démontré que les données enregistrées dans ces stylos étaient à terme effacées et, en tout état de cause, illisibles sans disposer du matériel approprié mis à disposition par cette société.

Toutefois, la CNIL a relevé que, sur certains points, ses recommandations avaient été insuffisamment suivies d'effets.

▸ Il est ressorti des contrôles que les personnes ne souhaitant pas figurer dans les fichiers d'électeurs devaient, pour exercer leur droit d'opposition, remplir un formulaire exclusivement téléchargeable sur le site internet du Parti socialiste. Or, la CNIL rappelle très régulièrement que l'exercice des droits d'accès, de rectification et d'opposition ne doit pas être limité par des conditions qui ne sont pas prévues par la loi.

▸ Plus généralement, si le respect des exigences « Informatique et Libertés » a manifestement été une préoccupation centrale pour les instances nationales du Parti socialiste, les instances locales, et tout particulièrement les présidents de bureaux de vote, n'ont pas toujours été suffisamment informés des modalités concrètes de mise en œuvre des engagements pris auprès de la CNIL.

FOCUS

Les contrôles des « primaires citoyennes » en quelques chiffres

26 contrôles (dont 14 effectués dans des communes situées dans 9 départements) ayant permis d'être présent à **chaque étape** du processus des élections primaires :

- **1 contrôle, quelques jours avant le premier tour de l'élection, au siège du Parti socialiste ;**
- **16 contrôles, durant le premier tour, dans les bureaux de vote ;**
- **6 contrôles, à l'occasion des deux tours, auprès de fédérations départementales ;**
- **2 contrôles, après le second tour, dans les locaux du prestataire chargé de centraliser puis de détruire les listes d'électeurs émargées ;**
- **1 contrôle, au terme des opérations, auprès du prestataire ayant mis à disposition les stylos électroniques utilisés pour constituer le « fichier des sympathisants ».**

LES PRIMAIRES : UN MODE DE CONSULTATION APPELÉ À SE DÉVELOPPER

Dans la mesure où ce mode de consultation semble amené à se développer dans les prochaines années, la Commission a entamé fin 2011 un travail de refonte de sa recommandation, relative aux fichiers utilisés par les partis politiques, en s'appuyant notamment sur les élections organisées par le Parti socialiste. La nouvelle recommandation, portant recommandation relative à la mise en œuvre, par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives, de fichiers dans le cadre de leurs activités politiques, a été adoptée le 26 janvier 2012. ■

7. SANCTIONNER

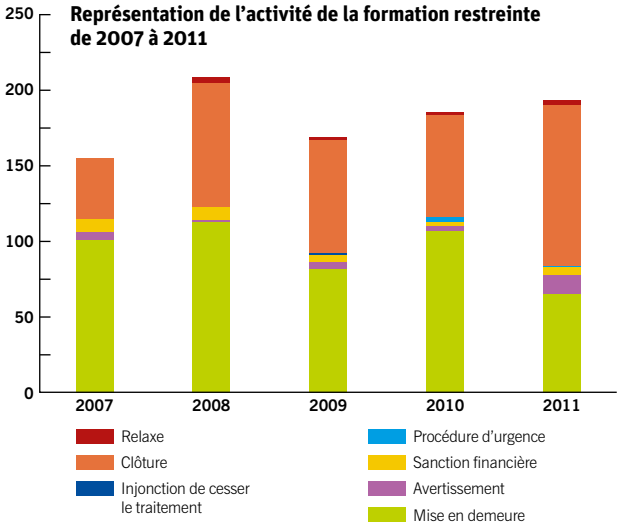
Résumé de l'activité
de la formation restreinte

GROS PLAN

La nouvelle organisation de la formation restreinte

RÉSUMÉ DE L'ACTIVITÉ DE LA FORMATION RESTREINTE

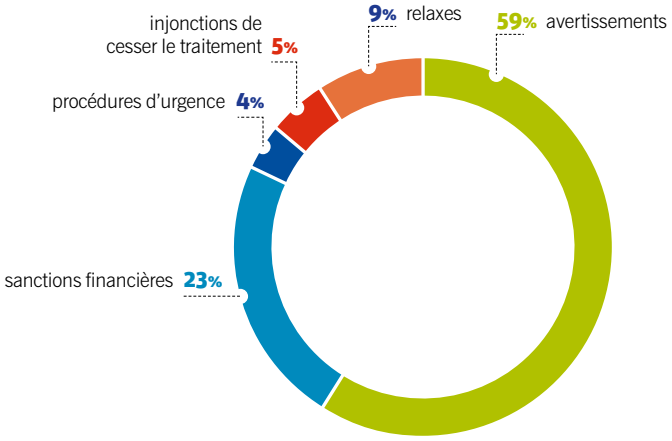
65 mises en demeures ont été adoptées au cours de l'année 2011, dont 27 par la formation restreinte avant la réforme introduite par la loi du 29 mars 2011 relative au Défenseur des droits et 38 par le Président de la CNIL depuis la réforme.
19 sanctions ont été prononcées par la Formation restreinte, dont 13 avertissements au cours de l'année 2011, 5 sanctions financières et une injonction de cesser le traitement.



65
MISES EN DEMEURES ONT ÉTÉ ADOPTÉES

19
SANCTIONS ONT ÉTÉ PRONONCÉES

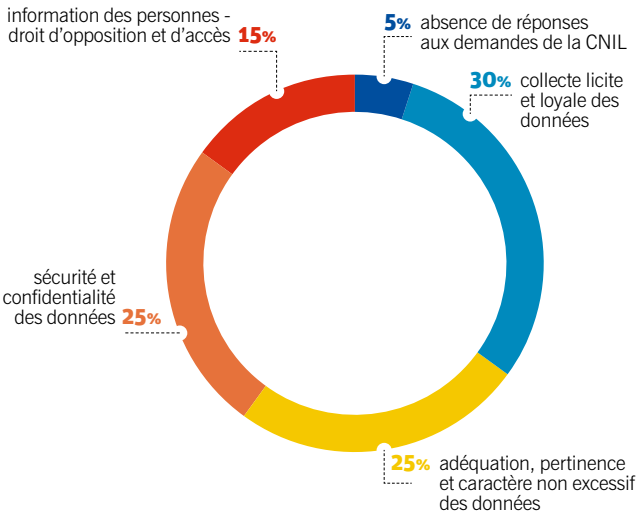
13
AVERTISSEMENTS



Le bilan de l'année 2011 est marqué par nombre important de clôtures des mises en demeures *(nombre de clôtures en 2011 : 105 - nombre de clôtures en 2010 : 67 - nombre de clôtures en 2009 : 75)*. La mise en demeure est avant tout utilisée comme un instrument permettant aux organismes de se mettre en conformité avec la loi « Informatique et Libertés ». Le taux de clôture démontre l'efficacité des mises en demeure qui permettent de faire prendre conscience aux organismes concernés des manquements à la loi « Informatiques et Libertés » et de les aider à régulariser leur situation.

Cette démarche explique dès lors que le nombre d'avertissements prononcés par la formation restreinte soit plus important que celui des sanctions pécuniaires. En effet, le prononcé d'un avertissement n'est pas conditionné à l'adoption préalable d'une mise en demeure, alors que la sanction pécuniaire ne sera envisagée qu'après l'échec de la mise en conformité.

Les manquements Informatiques et Libertés les plus sanctionnés



INFOS +

Un avertissement est-il une sanction ?

L'article 45 de la loi du 6 janvier 1978, tel que modifié par la réforme « Défenseur des droits », précise désormais expressément que l'avertissement est une sanction. Cette dernière n'est pas conditionnée par l'adoption préalable d'une mise en demeure, comme c'est le cas pour la sanction pécuniaire. Elle peut en effet être requise et prononcée directement après la révélation d'un manquement. La formation restreinte, saisie par le Président de la CNIL, peut donc utiliser cette voie pour sanctionner des faits avérés, quand bien même ils seraient révolus au jour de l'audience. Par exemple, une faille de sécurité portée à la connaissance de la Commission et constatée par elle pourra faire l'objet d'une procédure d'avertissement, quand bien même elle serait réparée au jour de l'audience. L'avertissement peut également sanctionner des manquements avérés qui persistent au jour du prononcé de la décision.

Liste des sanctions prononcées en 2011

Date	Nom ou type d'organisme	Décision adoptée	Manquement principal	Thème
06/01/2011	Google	Sanction pécuniaire de 100 000 euros	Collecte excessive	Télécom
03/02/2011	Soutien scolaire*	Avertissement	Commentaires excessifs	Cours à domicile
03/03/2011	Soutien scolaire*	Avertissement	Commentaires excessifs	Cours à domicile
03/02/2011	Société commercialisant des coffrets cadeaux*	Sanction pécuniaire de 50 000 euros	Non prise en compte du droit d'opposition	Commerce
17/03/2011	Société de crédits et de recouvrement de créances*	Avertissement	Commentaires excessifs	Banque
24/03/2011	Banque*	Avertissement	Collecte d'information	Banque
16/06/2011	PM Participation	Sanction pécuniaire de 10 000 euros	Collecte déloyale	Immobilier
30/06/2011	Organisme public*	Relaxe	sécurité et confidentialité	Secteur public
30/06/2011	Société anonyme d'habitations à loyer modéré*	Avertissement	Collecte déloyale et illicite	Secteur public - immobilier
05/07/2011	Pages jaunes **	Avertissement public	Collecte et traitement déloyaux	Télécom
05/07/2011	Fédération sportive*	Avertissement	Sécurité insuffisante	Sport
05/07/2011	Réseau d'agences immobilières **	Avertissement public	Commentaires excessifs	Immobilier
12/07/2011	Association LEXEEK **	Sanction pécuniaire de 10 000 euros et injonction de cesser le traitement	Non prise en compte du droit d'opposition	Association
21/07/2011	Mouvement politique*	avertissement et procédure d'urgence	sécurité et confidentialité	Secteur public
15/09/2011	Entreprise de vente par correspondance	Relaxe	Non prise en compte du droit d'opposition	Commerce
15/09/2011	Agence immobilière*	Avertissement	Absence de réponse aux demandes de la CNIL	Immobilier
13/10/2011	Hébergeur de données de santé*	Avertissement	Sécurité et collecte illicite	Santé
13/10/2011	Fournisseur d'accès télévision, téléphone et internet*	Avertissement	sécurité et confidentialité	Télécom
10/11/2011	Société d'aménagement urbain et rural*	Avertissement	Commentaires excessifs	Secteur public
01/12/2011	GROUPE DSE FRANCE	Sanction pécuniaire de 20 000 euros	Collecte déloyale	Immobilier

** Sanctions non rendues publiques par la formation restreinte. - ** Recours auprès du Conseil d'État.*

GROS PLAN

LA NOUVELLE ORGANISATION DE LA FORMATION RESTREINTE

> Dès 2008, le Conseil d'État a qualifié la CNIL de tribunal"

La réforme introduite par la loi du 29 mars 2011 relative au Défenseur des droits a apporté des modifications substantielles aux pouvoirs de mise en demeure et de sanction de la Commission. Un certain nombre de dispositions, en modifiant notamment les articles 11, 45 et 46 de la loi « Informatique et Libertés » du 6 janvier 1978, ont eu un impact immédiat sur la structure et le fonctionnement de la CNIL, et plus particulièrement sur ses procédures de contrôle, de mise en demeure et de sanction.

Les modifications apportées par le Législateur à ces trois dispositions découlent de l'interprétation faite, par la Cour européenne des droits de l'homme (CEDH), de l'article 6 de la Convention européenne des droits de l'homme et de sauvegarde des libertés fondamentales (CEDHSLF), qui garantit aux personnes un « *droit au procès équitable* ».

En effet, la CEDH, comme la Cour de cassation et le Conseil d'État, applique désormais de manière systématique, même s'il existe des différences substantielles, les dispositions de l'article 6 de la Convention européenne des droits de l'homme relatives au procès équitable aux procédures de sanction des autorités administratives indépendantes (AAI).

Ces procédures dites « *contentieuses* » sont en effet assimilées à des « *accusations en matière pénale* » au sens de la Convention, notion dont l'interprétation européenne est autonome des significations nationales et englobe l'ensemble de la matière répressive. Des AAI peuvent ainsi avoir la qualité de « *tribunal* » au sens de la CEDHSLF sans être pour autant des « *juridictions* » au sens du droit interne. Ainsi, dès 2008, le Conseil d'État a qualifié la CNIL de « *tribunal* ». À ce titre, celle-ci est tenue d'appliquer un certain nombre de garanties considérées comme substantielles par la CEDH, telles que le caractère contradictoire de la procédure, le principe général des droits de la défense et le principe général d'impartialité.

▸▸▸

UNE SÉPARATION STRICTE DES FONCTIONS DE POURSUITE, D'INSTRUCTION ET DE JUGEMENT

Le principe d'impartialité suppose que les différentes phases de la procédure juridictionnelle, à savoir la poursuite de l'organisme mis en cause, l'instruction et le jugement, ne soient pas confiées aux mêmes personnes, afin d'assurer une séparation stricte des fonctions.

Par un arrêt du 11 juin 2009, la CEDH a d'ailleurs condamné la France pour ne pas avoir assuré une séparation suffisante entre les fonctions de poursuite et de jugement au sein de la Commission bancaire[1]. Elle a notamment constaté que les mêmes organes étaient intervenus à plusieurs reprises au cours de la procédure de sanction, aussi bien lors de la phase de poursuite que de jugement.

En l'absence de base textuelle explicite, la CNIL avait toutefois anticipé l'application des exigences européennes à ses propres procédures. Elle avait d'ores et déjà pris diverses mesures visant à assurer une meilleure séparation des phases de poursuite (missions de contrôle et mise en demeure des organismes), d'instruction (nomination du rapporteur et notification des griefs) et de jugement (sanction) en son sein.

La loi relative au Défenseur des droits a permis de donner un fondement légal à ces mesures, et de confirmer la distinction organique entre les différentes phases de la procédure dite « contentieuse » de la CNIL. Désormais, il existe une séparation stricte entre les différentes fonctions au sein de la CNIL. L'organisme sanctionné ne peut donc plus nourrir l'impression que ce sont les mêmes personnes qui l'ont poursuivi et jugé.

Aujourd'hui comme hier, la loi prévoit que le président et les cinq autres membres composant la formation restreinte de la CNIL demeurent élus par la Commission en son sein, selon des règles de quorum et de vote spécifiques. En revanche, les membres du bureau de la Commission (c'est-à-dire son Président et ses deux Vice-présidents) ne sont plus éligibles à la formation restreinte, ce qui constitue une rupture avec la situation antérieure. Le Président de la Commission étant désormais investi de l'exclusivité des pouvoirs de poursuite (contrôles et mises en demeure), et de décision du passage à la phase d'instruction (désignation d'un rapporteur et notification du rapport en sanction), il ne peut par conséquent plus cumuler ces attributions avec des fonctions de jugement.

En application de ces nouvelles dispositions, la Commission a procédé à une nouvelle élection des six membres de la formation restreinte le 5 mai 2011. Mme Claire DAVAL ainsi que MM Jean-Marie COTTERET, Claude DOMEIZEL, Dominique RICHARD, Jean-François CARREZ et Sébastien HUYGHE ont été élus. Mme Claire DAVAL a également été élue Présidente de cette formation[2] qui s'est réunie pour la première fois en cette composition en juin 2011.

Un décret d'application en date du 29 décembre 2011[3] a également créé la fonction de Vice-Président de la formation restreinte ; M. Jean-Marie COTTERET a été élu par la formation plénière le 17 janvier 2012[4] pour remplir cette fonction.

> En l'absence de base textuelle explicite, la CNIL avait anticipé l'application des exigences européennes à ses propres procédures

[1] CEDH, 11 juin 2009, Dubus c. France, n° 5242/04. / [2] Délibération n° 2011-123 du 5 mai 2011 portant élection des membres et du président de la formation restreinte de la Commission nationale de l'informatique et des libertés. / [3] Décret n° 2011-2023 du 29 décembre 2011 relatif aux pouvoirs de contrôle et de sanction de la Commission nationale de l'informatique et des libertés. / [4] Délibération n° 2012-015 du 17 janvier 2012 portant élection du Vice-président de la formation restreinte de la Commission nationale de l'informatique et des libertés.

LES POUVOIRS MODIFIÉS DU PRÉSIDENT DE LA COMMISSION ET DE LA FORMATION RESTREINTE

Les pouvoirs de sanction de la CNIL sont prévus aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, largement remaniés par la loi relative au Défenseur des droits.

La procédure de mise en demeure appartient désormais au seul Président, et non plus à la formation restreinte, depuis l'entrée en vigueur de la loi du 29 mars 2011.

Le Conseil d'État, dans une ordonnance du 5 septembre 2008, a appliqué à la CNIL sa jurisprudence constante selon laquelle une mise en demeure, si elle est une décision faisant grief, ne saurait en revanche être qualifiée de sanction – et n'est, de ce fait, pas soumise au principe du contradictoire[5].

En effet, l'adoption d'une mise en demeure ne vise pas à sanctionner l'organisme, mais au contraire à ouvrir une phase de « réparation » des manquements commis en lui offrant la possibilité de se conformer à la loi. De fait, cette procédure permet, dans la grande majorité des cas, de faire prendre conscience aux organismes qu'ils ne respectent pas les exigences de la loi « Informatique et Libertés », comme l'atteste le taux élevé de clôture des mises en demeure pour mise en conformité (de 60 à 80 % des cas, selon les années)[6].

Au titre des nouveautés apportées au dispositif par la loi relative au Défenseur des droits, les mises en demeure adoptées par le Président pourront désormais être rendues publiques. Cette publicité relève de la compétence du bureau de la Commission (composé du Vice-président délégué et du Vice-président), qui devra d'abord être saisi d'une demande en ce sens par le Président. Il aura bien évidemment la faculté de la refuser. Par ailleurs, le fait que l'organisme se soit conformé à la mise en demeure et que la procédure ait été de ce fait clôturée devra faire l'objet de la même publicité que celle accordée, le cas échéant, à la mise en demeure elle-même.

> L'adoption d'une mise en demeure ne vise pas à sanctionner l'organisme, mais au contraire à ouvrir une phase de « réparation » des manquements

La publicité des décisions de la CNIL peut s'effectuer sur son site Internet ou sur le site Internet de Légifrance, qui rediffuse l'intégralité des délibérations de la CNIL dans le cadre d'un partenariat historique. Le bureau peut également ordonner l'insertion de ses décisions dans des publications, journaux et supports qu'il désigne, aux frais des personnes sanctionnées.

S'agissant de la procédure de sanction, la loi relative au Défenseur des droits n'y a apporté que des modifications mineures. En particulier, la décision de publier une sanction prononcée pour non-respect d'une mise en demeure n'est désormais plus soumise à la condition de mauvaise foi du responsable de traitement.

En revanche, le décret du 29 décembre 2011 **relatif aux pouvoirs de contrôle et de sanction de la CNIL** apporte des modifications plus notables à la procédure de sanction. Il prévoit en effet que les observations écrites de l'organisme visé par un rapport de sanction devront désormais parvenir à la formation restreinte *au moins 3 jours francs avant la séance* et que ses observations orales en séance devront *venir à l'appui de* [ses] *conclusions écrites*. Ce décret instaure donc une véritable clôture de l'instruction et vise à ce que les observations des organismes concernés ne puissent désormais plus être adressées tardivement à la formation restreinte.

Ce décret permet également à la formation restreinte de publier ses décisions de sanction dès qu'elles auront été notifiées aux organismes concernés, sans attendre que ces décisions deviennent définitives. La CNIL devra alors mentionner que la décision de sanction est susceptible de faire l'objet d'un recours. ■

[5] Conseil d'État, Société DIRECT ANNONCES, n°319071, ordonnance du 5 septembre 2008. / [6] Ainsi, pour l'année 2010 : 67 clôtures pour mise en conformité sur 111 mises en demeure prononcées.

8. LES SUJETS DE RÉFLEXION POUR 2012

Révision de la directive : réussir l'Europe de la protection des données

Au-delà de la loi : la protection des données et de la vie privée, valeur de l'entreprise

RÉVISION DE LA DIRECTIVE : RÉUSSIR L'EUROPE DE LA PROTECTION DES DONNÉES

UNE ANNÉE DE RÉFLEXION ET DE CONSULTATION POUR LA COMMISSION EUROPÉENNE

Une priorité stratégique pour la Commission européenne

La révision de la Directive européenne 95/46/CE, qui fixe le cadre juridique européen en matière de protection des données à caractère personnel, est un objectif prioritaire de la Commission européenne et de la Vice-présidente Viviane REDING, Commissaire en charge de la justice, des droits fondamentaux et de la citoyenneté.

La communication publiée par la Commission européenne en novembre 2010 a constitué le socle des réflexions conduites en 2011. La Commission y avait présenté cinq objectifs :

- renforcer les droits des personnes,
- renforcer la dimension « marché intérieur » et assurer une plus grande harmonisation des règles de protection des données,
- étendre l'application des règles générales de protection des données au domaine de la coopération policière et judiciaire,
- affirmer la dimension mondiale de la protection des données,
- renforcer le rôle des autorités nationales de protection des données et du groupe des CNIL européennes, le G29, en vue d'un plus grand respect des règles de protection des données.

L'année 2011 aura été celle de la maturation du projet par la Commission européenne qui aura consulté différents acteurs et experts sur la mise en œuvre concrète de ses grandes orientations. La Commission a adopté le 25 janvier 2012 un projet de règlement et un projet de directive réformant le cadre de la protection des données.

Le Parlement et le Conseil s'emparent du débat

Le Parlement européen et le Conseil sont intervenus en réagissant à la communication de la Commission européenne de novembre 2010.

Ainsi, le Conseil JAI (Justice et Affaires Intérieures) de l'Union européenne et le Parlement européen (Commission LIBE) ont accueilli positivement les orientations de la Commission. Cependant, le

Parlement s'est inquiété des mesures prévues en matière de droit applicable et a appelé à une clarification des critères garantir un niveau de protection homogène et élevé pour toute l'Europe afin d'éviter tout phénomène de *forum shopping**.

* *Le forum shopping désigne le fait qu'une entreprise choisisse de s'implanter dans un pays plutôt que dans un autre en considération d'avantages liés à la législation de celui-ci.*

FOCUS

La Charte des droits fondamentaux de l'Union européenne

Ce texte a été adopté lors du Conseil européen de Nice, le 7 décembre 2000. Mais, c'est le traité de Lisbonne qui, depuis son entrée en vigueur le 1er décembre 2009, lui a donné la même valeur juridique que celle des traités. Elle est donc désormais contraignante pour les États membres et tout citoyen peut s'en prévaloir en cas de non-respect de ces droits par un texte européen. La Charte comporte 54 articles définissant les droits fondamentaux des personnes au sein de l'UE. Ceux-ci sont répartis entre six valeurs individuelles et universelles constituant le socle de la construction européenne : dignité, liberté, égalité, solidarité, citoyenneté et justice.
La Charte est le premier document de ce type à reconnaître explicitement la protection des données comme un droit fondamental. Ainsi, l'article 8 proclame que « toute personne à droit à la protection des données à caractère personnel la concernant ».

LA CNIL MOBILISÉE POUR LE MAINTIEN D'UN HAUT NIVEAU DE PROTECTION EN EUROPE

S'investir fortement dans les travaux du G29

En tant qu'instance représentant l'ensemble des autorités de protection des données de l'Union européenne, le G29 a été étroitement associé à la révision de la Directive.

À la demande de la Commission européenne, il a produit cinq avis auxquels la CNIL a largement contribué, relatifs aux sujets fondamentaux suivants : le régime juridique applicable aux données sensibles, la simplification du système de notification des traitements, la coopération entre les autorités de protection des données, le droit applicable et la notion de consentement. Par ailleurs, la Commission européenne a organisé plusieurs réunions avec le G29 dédiées aux orientations de la réforme.

En tant que Président du G29 jusqu'en 2009, Alex Türk avait initié la préparation d'un avis stratégique sur le futur de la vie privée, lequel a été pris en compte par la Commission européenne pour sa communication de novembre 2010. La CNIL est attachée à la promotion d'une approche équilibrée de la réforme : les attentes des entreprises doivent être entendues, l'évolution du cadre actuel doit se faire avant tout au bénéfice des citoyens.

Développer les relations avec la Commission européenne et le Parlement européen

La CNIL est allée à la rencontre des services de la Commission européenne en charge de la rédaction du nouvel instrument. Prenant appui sur son expérience de plus de 30 ans, **la CNIL défend un système de protection des données tout à la fois participatif et décentralisé qui lui paraît plus adapté au monde numérique et à la diversité des situations rencontrées** sur le terrain, imbriquant plusieurs pans du droit, qu'il s'agisse de droit du travail, droit pénal, fiscal, des affaires… que seules les autorités **nationales sont à même de connaître**. La gouvernance européenne de la protection des données, pour être efficace et démocratique, doit **reposer sur une coopération approfondie entre autorités souveraines compétentes**.

Seule institution européenne élue directement par les citoyens, le Parlement européen est attaché aux sujets qui touchent les droits fondamentaux. Il s'est montré particulièrement exigeant sur les projets « Swift[1] » et « PNR[2] ». La CNIL a estimé utile de rencontrer plusieurs eurodéputés en mai 2011 dans le cadre du projet de rapport parlementaire sur la communication de la Commission européenne. Ces rendez-vous ont permis d'établir un premier contact avec plusieurs acteurs clés de l'institution européenne et de poser les jalons d'une coopération avec eux.

Enfin, la Présidente de la CNIL s'est entretenue avec Mme Reding à Paris le 26 novembre 2011. Cette rencontre a été l'occasion pour la CNIL de réitérer ses positions vis-à-vis des orientations retenues sur le projet de règlement à quelques semaines de la finalisation du projet par la Commission.

[1] PNR (Passenger Name Record) : il s'agit des informations collectées auprès des passagers aériens au stade de la réservation commerciale / [2] SWIFT (Society for Worldwide Interbank Financial Telecommunication) : il s'agit d'une société coopérative de droit belge fondée en 1973, qui offre aux banques un ensemble de services, dont un système de messagerie sécurisée.

LES PRINCIPAUX POINTS DE DISCUSSION AVEC LA COMMISSION EUROPÉENNE

La CNIL, tout comme l'ensemble des autorités nationales de protection des données, salue les avancées du projet européen en ce qui concerne le renforcement des droits des personnes, notamment en matière de droit à l'oubli, portabilité des données et consentement. Pour autant, certaines dispositions lui paraissent insuffisamment claires ou poser problème.

Compétence des autorités : l'approche risquée de la Commission européenne pour les droits des citoyens

Afin de remédier à la fragmentation des législations nationales, l'axe fort dégagé par la Commission européenne est d'harmoniser strictement les règles applicables et de simplifier la vie des entreprises dont les traitements ont un impact sur le territoire de plusieurs États membres. Elle a prévu **un critère permettant d'attribuer compétence à une seule autorité, à savoir** le critère de **l'établissement principal** du responsable de traitement, ce qui suscite l'inquiétude de la CNIL.

Cette solution aurait des conséquences politiques importantes puisqu'elle participerait à un éloignement sensible des citoyens des autorités compétentes. En effet, si l'autorité compétente est celle où se situe l'établissement principal d'une entreprise, quel que soit le public ciblé par son activité, **les autorités nationales de protection des données ne joueraient qu'un rôle de « boîte aux lettres » pour les citoyens qui seraient pourtant fondés à les saisir de leurs difficultés.** Concrètement, cela signifierait qu'en cas de problème pour un internaute sur un réseau social dont l'établissement principal est implanté dans un autre État membre, cette plainte sera traitée par l'autorité de ce dernier et non par l'autorité du lieu de sa résidence. Le citoyen souhaitant contester les résultats de l'instruction de sa plainte devrait alors le faire auprès d'un tribunal étranger, ce qui s'avérerait difficilement praticable.

> Le critère de l'établissement principal risque d'éloigner le citoyen des autorités nationales

La CNIL a fait valoir les inconvénients d'une telle approche. Il serait paradoxal que la protection en matière de données personnelles soit finalement plus faible qu'en droit de la consommation qui privilégie une compétence basée sur le lieu de résidence du consommateur. Aussi, pour une même transaction commerciale, le citoyen français devrait saisir la DGCCRF pour l'aspect consommation et devrait s'en remettre à une autorité située dans un autre État pour l'aspect protection des données.

Ce critère encouragerait de plus les pratiques de *forum shopping*[1] pour les traitements ayant pourtant un impact immédiat sur notre territoire, notamment ceux réalisés par les grands acteurs de l'Internet.

Transferts internationaux : les autorités de protection doivent conserver un rôle de contrôle

Du fait de la mondialisation des échanges et des services sans cesse croissante, illustrée par exemple par le développement du *cloud computing*, les transferts internationaux de données constituent un enjeu économique et politique de premier ordre pour la France et l'ensemble des États membres de l'Union européenne.

Afin de pallier les risques de perte de maîtrise des informations échangées, la CNIL considère que les garanties apportées par le projet de règlement ne peuvent découler que d'instruments juridiques contraignants : clauses contractuelles types ou règles internes d'entreprise, validées préalablement par les autorités de protection selon des référentiels prédéfinis.

Ces instruments, testés et améliorés depuis plusieurs années par l'Union européenne, et qui suscitent un fort intérêt des entreprises, permettront d'assurer une meilleure protection lors du transfert à l'étranger des données per-

[1] *Le forum shopping désigne le fait qu'une entreprise choisisse de s'implanter dans un pays plutôt que dans un autre en considération d'avantages liés à la législation de celui-ci.*

sonnelles des citoyens. Il convient dès lors de ne pas fragiliser ce dispositif au moyen d'instruments non contraignants et non préalablement approuvés par les autorités de protection.

La protection des données est l'affaire de tous : quelle responsabilité pour les acteurs ?

La notion de responsabilisation des acteurs consiste en une obligation générale de rendre des comptes (*accountability*) **en exigeant de leur part la mise en place de mesures proactives de protection des données** (désignation d'un correspondant informatique et libertés, études d'impacts, réalisation régulière d'audits…). Une fois mises en œuvre, ces mesures doivent permettre à l'entreprise de démontrer pleinement qu'elle respecte la réglementation. Ainsi, cette responsabilisation permettrait de faire entrer la question de la protection de la vie privée au cœur des entreprises afin de rendre cette protection concrète et efficace.

Il est essentiel que les autorités conservent un pouvoir d'encadrement et de contrôle de ces nouveaux instruments, notamment en ce qui concerne les référentiels en matière de formation ou d'audits afin de permettre d'évaluer la conformité et l'effectivité des mesures prises. **Ces mesures de responsabilisation des acteurs ne doivent pas être des mesures d'autorégulation se substituant aux valeurs fondamentales mais doivent être considérées comme un complément des principes existants**.

> L'*accountability* ne doit pas se substituer à la régulation mais compléter les principes existants

L'EUROPE DOIT RELEVER LE DÉFI D'UN ENVIRONNEMENT INTERNATIONAL EN ÉVOLUTION

Les réflexions menées sur l'avenir de la protection des données au sein des diverses régions du monde constituent une opportunité pour aller vers davantage de cohérence entre les instruments nationaux et internationaux et la définition d'une approche globale. La CNIL et l'ensemble des autorités de protection des données réunies lors de la conférence internationale de 2009 ont adopté des principes communs en la matière, appelés les « standards de Madrid ». Il s'agit désormais de mettre en place un instrument juridique contraignant au niveau mondial reprenant ces principes.

Par ailleurs, tous les cadres juridiques existants dans le monde sont en cours de modifications ce qui révèle la prise de conscience de l'importance du sujet :

▸ **Le Conseil de l'Europe :** la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (ci-après « Convention 108 ») date de 1981. Le Conseil de l'Europe a lancé une large consultation publique dans le but de la moderniser. **La CNIL soutient particulièrement la vocation mondiale de la Convention 108 et encourage les États non-membres du Conseil de l'Europe à la ratifier**. Le Comité consultatif entend finaliser une proposition afin de la soumettre au Comité des ministres fin 2012.

▸ **L'Organisation de Coopération et de Développement Économique (OCDE) :** en 1980, l'OCDE a adopté les Lignes directrices sur la protection de la vie privée et les flux transfrontières de données personnelles. À l'occasion du 30ème anniversaire de ces lignes directrices, l'OCDE a engagé une réflexion sur leur révision à laquelle la CNIL a participé. Les conclusions sur l'opportunité de réformer ce document seront publiées en 2012.

▸ **L'APEC (Forum de coopération économique de la région Asie-Pacifique) :** un sous-groupe constitué sur la protection de la vie privée s'est réuni en septembre

2011 à San Francisco (États-Unis). Pour la première fois, la CNIL a pu y participer en tant qu'observateur, représentant la Conférence internationale des commissaires à la protection des données personnelles et de la vie privée. Cette réunion a porté sur la mise en place du système de règles transfrontalières de protection de la vie privée dénommées *Cross Border Privacy Rules* (CBPR). Le système n'est pas encore opérationnel mais la question d'une possible interopérabilité entre ce système et les Règles internes d'entreprise dites « BCR » européens, qui sont d'ores et déjà en œuvre, sera un enjeu crucial dans les prochaines années. ■

AU-DELÀ DE LA LOI : LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE, VALEUR DE L'ENTREPRISE

LES RELATIONS CNIL-ENTREPRISES DOIVENT INTÉGRER UNE NOUVELLE DIMENSION

La protection des données : plus qu'une contrainte légale, un avantage concurrentiel et social

Le développement de l'économie numérique a modifié de manière irréversible la manière dont travaillent les entreprises. La dématérialisation des relations commerciales, des échanges, des procédures, des modes de travail, l'emprise croissante des nouvelles technologies sur l'activité professionnelle, ont eu pour conséquence de placer les traitements des données au cœur de leurs activités.

Ainsi, en apprenant à tirer parti des progrès accomplis dans les moyens d'exploitation des données personnelles de leurs clients, les entreprises les ont progressivement transformées en des actifs à forte valeur financière.

Cet impératif de protection de ces données devient chaque jour plus aigu. Ainsi, les entreprises doivent garantir le respect de règles strictes de sécurité et de confidentialité, la loyauté de la collecte ou du partage d'informations personnelles, afin de faire face aux risques juridiques mais aussi en terme d'image auxquels elles sont exposées.

Cet impératif de protection va au-delà de la volonté de satisfaire à une obligation légale. Il s'agit en réalité de préserver la valeur commerciale des données dont les entreprises ont la responsabilité : en effet, le non-respect de ces règles mine la confiance que les clients plaçaient jusqu'à présent dans l'entreprise, et produit des effets négatifs avérés. Ainsi, la prise en compte de la protection des données personnelles de leurs clients par les entreprises constitue **un avantage concurrentiel** qui tend à fidéliser une clientèle par ailleurs de plus en plus volatile.

Une tendance similaire se fait jour à l'intérieur de l'entreprise, au sein de laquelle le respect de la vie privée et la protection des données tendent aujourd'hui à être identifiés comme une forme **d'avantage social**. De fait, salariés et collaborateurs sont en quête de sens dans une économie en crise, inquiets dans un monde du travail de plus en plus complexe, souvent anxiogène. Or, comment espérer susciter leur motivation en les plaçant sous surveillance permanente, quand des caméras de vidéosurveillance sont déployées de manière irraisonnée, quand des dispositifs de géolocalisation ou d'alerte anonyme sont mis en place sans concertation, quand des données d'évaluation subjectives sont remontées à la maison-mère du groupe, à l'étranger, sans information précise sur la finalité de ce transfert ?

Changer l'image de la protection des données

On le voit : le souci de respecter la vie privée doit aujourd'hui irriguer l'intégralité des activités de l'entreprise. Il ne s'agit ni d'un luxe, ni de répondre à une simple contrainte légale. Il s'agit, plus profondément, de susciter la confiance des personnes dans l'entreprise en respectant leurs libertés, leur identité et leur dignité.

Une véritable prise de conscience s'opère en ce sens dans la société française, comme dans la plupart des sociétés occidentales.

La protection des données intègre ainsi, progressivement, les impératifs éthiques identifiés comme s'imposant à l'entreprise. À ce titre, ils sont d'ailleurs le plus souvent repris à leur compte par les promoteurs des mouvements d'« éthique des affaires » et de « responsabilité sociale des entreprises ». Citons par exemple l'Observatoire de la responsabilité sociétale des entreprises (ORSE) avec lequel la CNIL a collaboré à la rédaction du guide sur le télétravail et le Club informatique des grandes entreprises françaises (CIGREF) qui, dans un rapport de juin 2009, ont préconisé un développement des technologies de l'information et des communications au sein des entreprises, « *dans le respect des principes de la loi « Informatique et Libertés » et des préconisations de la CNIL* ».

Si ce mouvement de la responsabilité sociétale des entreprises (RSE) met principalement l'accent sur l'impact environnemental de l'action de l'entreprise et sur le concept de développement durable, on observe une prise en compte croissante des conséquences sociales de l'activité des entreprises dans ce mouvement, dans lequel la protection des données a naturellement vocation à s'intégrer.

Mais la protection des données trouve également à s'inscrire dans un cadre durable, et non seulement social. En effet, le développement des nouvelles technologies doit, selon une définition désormais établie, répondre aux besoins des générations présentes sans compromettre la capacité des générations futures à répondre aux leurs.

Relevons, enfin, que la protection des données figure parfois dans les textes internationaux – non contraignants – relatifs à la RSE. Ainsi par exemple, les principes directeurs de l'OCDE et l'ISO 26000, et de nombreuses communications de la Commission européenne en la matière, consacrent plusieurs paragraphes à la protection des données et à la protection de la vie privée des employés et des consommateurs ; de même, des chartes et codes éthiques de plus en plus nombreux, notamment parmi les entreprises du CAC 40, comportent des dispositions relatives au respect de la vie privée ou à la confidentialité des données.

Ce contexte nouveau incite les entreprises à protéger les données personnelles pour des raisons allant au-delà des contraintes légales. Ce faisant, il impose aux entreprises de modifier le regard qu'elles portent sur la matière, autant que celui qu'elles portent sur la CNIL.

Changer l'image de la CNIL

Il importe que les entreprises se défassent de l'image réductrice de la CNIL qui est souvent la leur.

Certes, pèse sur elle, comme d'ailleurs sur les organismes publics, d'abord et avant tout une obligation de conformité aux règles applicables, y compris l'accomplissement de formalités préalables auprès d'elle. De même, la Commission fait un usage croissant de ses pouvoirs de contrôle, de mise en demeure et de sanction pour faire respecter la loi, et cette réalité impose aux entreprises de gérer le risque institutionnel ainsi créé.

Mais l'action de la CNIL ne saurait être réduite ni à l'accomplissement de formalités administratives à l'utilité souvent mal comprise (CNIL = déclaration), ni à une dimension coercitive crainte, mais mal identifiée (CNIL = sanction). Le « tout répressif », en particulier, trouve vite ses limites et ne peut fonder, seul, un mode de régulation. Les notions de concertation, de « démocratie administrative », d'« administration délibérative » invitent aujourd'hui les autorités publiques, dont la CNIL, à associer toujours davantage l'entreprise et la société civile à ses réflexions et processus décisionnels.

De fait, les entreprises sont aujourd'hui au cœur de la protection des données. Le projet de règlement ayant vocation à former le nouveau cadre européen en la matière simplifie considérablement la procédure de déclaration (voire la fait disparaître) mais augmente, en quelque sorte comme une contrepartie, la responsabilité du responsable de traitement, en instaurant de nouveaux principes européens.

Ces modifications induisent **de partager le poids de la régulation** dans l'environnement complexe et évolutif auquel les entreprises, comme la CNIL, font face aujourd'hui.

▸▸▸

> La protection des données s'inscrit dans une démarche durable et sociale

La CNIL et les entreprises, coresponsables et co-régulatrices de la protection des données

Entreprises et autorités sont aujourd'hui appelées à travailler en partenariat pour dégager des solutions adaptées à la réalité des entreprises tout en garantissant un niveau élevé de protection aux individus concernés. Cette adaptation des modes de régulation permettra aux entreprises de développer et de maintenir un avantage compétitif notable, et à la CNIL d'accomplir sa mission de régulation de manière éclairée.

De ce fait, elle a développé ou contribué au lancement d'outils et d'initiatives qui placent son action non plus seulement dans une stricte logique de conformité mais, plus largement, dans la perspective d'une recherche de valeur ajoutée pour les personnes ou les entreprises :

- Les *binding corporate rules* ou BCR, qui constituent un code de conduite définissant la politique d'une entreprise en matière de transferts de données, au sein d'une même entreprise ou d'un même groupe ;
- La conclusion de conventions de partenariat entre la CNIL et des syndicats professionnels ou des organisations représentatives tels que l'Assemblée permanente des chambres de commerce et d'industrie de France (AFCCI) ou le Conseil national des barreaux, aux fins, notamment de mutualiser les ressources et de démultiplier les canaux de diffusion de la culture « Informatique et Libertés » ;
- La validation de codes de déontologie et chartes, comme par exemple le **Code de déontologie de la communication directe électronique** élaboré par le Syndicat National de la Communication Directe (SNCD), ou le **Code de conduite sur l'utilisation de coordonnées électroniques à des fins de prospection directe** de l'Union Française du Marketing Direct (UFMD) ;
- La délivrance de labels, réservées, pour l'heure, aux seules procédures d'audit et formations, qui permet aux entreprises de se distinguer par la qualité de leur service, et aux utilisateurs d'identifier et privilégier certains produits et procédures ;
- La délivrance d'avis de conformité à la loi de procédures garantissant une meilleure protection de la vie privée et des données des personnes : ainsi, le 18 octobre 2011, la Commission s'est prononcée sur l'ensemble des procédures et des outils utilisés par l'Association pour le Développement du Service Notarial (ADSN) au titre de ses fonctions de correspondant « Informatique et Libertés » pour les notaires ;
- Le développement d'un service dédié aux correspondants et la mise en place des CIL, relais essentiel des problématiques identifiées par la CNIL au sein de l'entreprise ;
- L'organisation de consultations publiques, comme par exemple sur le *cloud computing*, auxquelles les entreprises ont été invitées à répondre. Celles-ci permettent à la CNIL d'envisager toutes les solutions, juridiques et techniques, pour que soit garanti un haut niveau de protection aux données personnelles tout en tenant compte des enjeux économiques.

L'ensemble de ces exemples montrent que la CNIL, aujourd'hui plus encore qu'hier, a clairement l'intention de jouer un rôle de conseil et d'accompagnement des entreprises qui dépasse, et de loin, un seul rôle de mise en application de la loi, sans concertation ni dialogue avec les entreprises.

Il appartient aujourd'hui aux entreprises de faire leur part du chemin en saisissant les outils qui leur sont proposés. ■

La CNIL et les entreprises doivent partager la charge de la régulation

ANNEXES

Les membres de la CNIL

Les moyens de la CNIL

Organigramme des directions et services

Liste des organismes contrôlés en 2011
Dispositifs de vidéoprotection (loi de 1995)

LES MEMBRES DE LA CNIL

LE BUREAU

Présidente

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

Vice-président délégué

Emmanuel de GIVRY, conseiller honoraire à la Cour de cassation
Secteur : Ressources humaines
Emmanuel de Givry est membre de la CNIL depuis février 2004, et vice-président délégué depuis février 2009.

Vice-président

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

LES MEMBRES (COMMISSAIRES)

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

Dominique CASTERA, membre du Conseil économique, social et environnemental
Secteur : Coopération policière internationale – Vie associative
Dominique Castera est membre de la CNIL depuis octobre 2010.

Jean-Marie COTTERET, professeur émérite des universités
Secteurs : Police nationale et sûreté de l'État
Jean-Marie Cotteret est membre de la CNIL depuis janvier 2004.
Il est vice-président de la formation contentieuse.

Claire DAVAL, avocate
Secteur : Justice
Claire Daval est membre de la CNIL depuis janvier 2009.
Elle a été élue Présidente de la formation contentieuse en 2011.

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

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

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

Philippe GOSSELIN, député de la Manche
Secteur : Questions fiscales et sociales
Philippe Gosselin est membre de la CNIL depuis juin 2008.

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

Jean MASSOT, président de section honoraire au Conseil d'État
Secteur : Santé et assurance maladie – archives et données publiques
Jean Massot est membre de la CNIL depuis avril 2005.

Marie-Hélène MITJAVILE, conseiller d'État
Secteur : Recherche et statistiques
Marie-Hélène Mitjavile est membre de la CNIL depuis janvier 2009.

Eric PERES, membre du Conseil économique, social et environnemental
Secteur : Education et enseignement supérieur
Eric PERES est membre de la CNIL depuis décembre 2010.

Bernard PEYRAT, conseiller honoraire à la Cour de cassation
Secteur : Commerce et marketing
Bernard Peyrat est membre de la CNIL depuis février 2004.

Dominique RICHARD, consultant
Secteur : Affaires culturelles et sportives, vidéoprotection
Dominique Richard est membre de la CNIL depuis janvier 2009.
Il est membre élu de la formation contentieuse.

Commissaires du gouvernement

Élisabeth ROLIN

Catherine POZZO DI BORGO, adjointe

LES MOYENS DE LA CNIL

LE PERSONNEL

L'année 2011 confirme la tendance à l'augmentation régulière et continue des personnels de la CNIL, amorcée en 2004 en raison des nouvelles missions et compétences introduites par la réforme de la loi « Informatique et Libertés ».

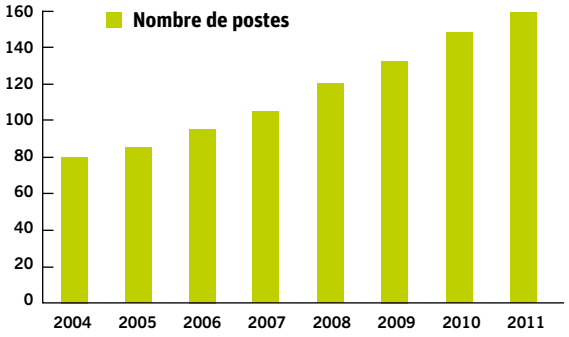
Avec ses 11 postes supplémentaires, soit une augmentation annuelle de 7,5% de ses effectifs, la CNIL affiche, en 2011, 159 postes budgétaires contre 148 en 2010. Elle double ainsi sa masse salariale en 7 ans.

Cette augmentation continue des créations de postes permet à la CNIL de rattraper progressivement le retard qui avait été constaté dès 2004, notamment par comparaison avec ses homologues européens qui disposaient déjà en moyenne de 200 agents. Cela permet à la CNIL de pouvoir assurer ses missions traditionnelles de contrôles, de sanctions, d'animation du réseau des correspondants, d'autorisation des fichiers les plus sensibles et de labellisation, principalement.

Cette augmentation significative des moyens reste encore insuffisante, comme l'ont souligné les récents débats parlementaires lors du vote de la loi de finances pour 2012.

En effet, en 2011, le périmètre des missions confiées à la CNIL s'est accru de manière substantielle.

D'une part, les dispositions de la loi LOPPSI 2 du 14 mars 2011 attribuent à la CNIL une nouvelle mission en matière de contrôle de systèmes de vidéo protection installés sur la voie publique en application de la loi du 21 janvier 1995. Or, les dispositifs en question se comptent par centaines de milliers.



D'autre part, l'article 17 de la loi du 22 mars 2011, relative à la transposition en droit français de la Directive européenne « paquet télécom », conduit à rendre obligatoire par les responsables de traitement des déclarations de failles de sécurité auprès de la CNIL, c'est-à-dire de cas de violation de l'intégrité et de la confidentialité des données à caractère personnel. À cette heure, il est encore très difficile de pouvoir quantifier le nombre de failles de sécurité qui sont susceptibles d'être déclarées auprès de nos services.

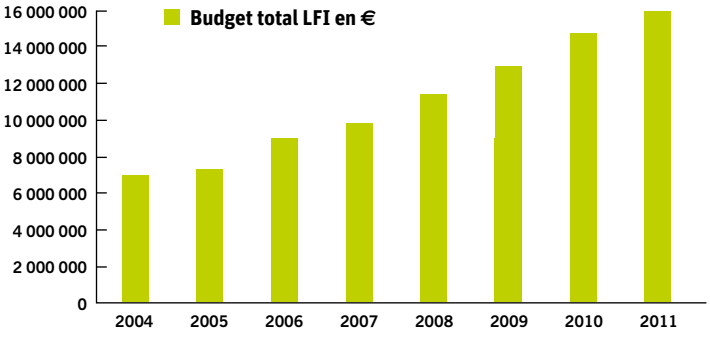
Par la volonté du législateur, les effectifs de la CNIL sont donc susceptibles d'augmenter encore de manière significative dans les prochaines années.

LES CRÉDITS

En 2011, la CNIL a été dotée d'un budget total en augmentation de 8% par rapport à 2010 : 15,8 millions d'euros répartis à hauteur de 10,3 millions pour le personnel et 5,5 millions d'euros pour le fonctionnement.

Le budget alloué au personnel croît ainsi de près d'un million d'euros entre 2010 et 2011. Cette augmentation de 10% du budget est inhérente à l'accroissement du nombre de postes ouverts à la CNIL.

Le budget de fonctionnement augmente également mais dans une moindre mesure puisque que la hausse entre les exercices 2010 et 2011 n'est que de 140 k€ après l'application de la réserve de précaution et du gel « fonds d'État exemplaire ». Cette hausse limitée confirme de ce fait la tendance dessinée depuis 2004 selon laquelle les augmentations des crédits de fonctionnement ne suivent pas celles des crédits de personnels. La CNIL mène ainsi, depuis de nombreuses années, une politique de maîtrise de ses coûts de fonctionnement en vue de diminuer les ratios relatifs aux coûts d'occupation des locaux, d'acquisition bureautique ou encore ceux liés aux déplacements et hébergement des agents. ■



ORGANIGRAMME DES DIRECTIONS ET SERVICES

Isabelle Falque-Pierrotin
Présidente

Yann Padova
Secrétaire général

Carina Chatain-Marcel
Cabinet du secrétariat général et de la présidence
Pôle institutionnel

Elsa Trochet-Macé
Service de la communication externe et interne

Clarisse Girot et Stéphane Grégoire
Pôle juridique

Sophie Vulliet-Tavernier **Direction des études, de l'innovation et de la prospective**	Edouard Geffray et Sophie Nerbonne (adjoint) **Direction des affaires juridiques internationales et de l'expertise**	Florence Fourets **Direction des relations avec les usagers et du contrôle**	Isabelle Pheulpin **Direction des ressources humaines, financières, informatiques et logistiques**
Edmée Moreau **Service de l'information et de la documentation**	Paul Hebert **Service des affaires juridiques**	Fatima Hamdi **Service d'orientation et de renseignements du public**	Olivier Tournut **Service des ressources humaines**
	Florence Raynal **Service des affaires européennes et internationales**	Norbert Fort **Service des plaintes**	Magali d'Elia **Service financier**
	Gwendal Le Grand **Service de l'expertise informatique**	Thomas Dautieu **Service des contrôles**	Hervé Brassart **Service de l'informatique interne**
		Elise Wolton **Service de la gestion des sanctions**	Marcel Fanjeaux **Service logistique**
		Mathias Moulin **Service des correspondants**	
		Maryline Abiven **Service du droit d'accès indirect**	

LISTE DES ORGANISMES CONTRÔLÉS EN 2011

ASSOCIATION

ASSOCIATION L'ABRI MAISON PROTESTANTE D'ENFANT

ASSOCIATION FRANCE-ALZHEIMER

ASSOCIATION HABITAT ET INSERTION

ASSOCIATION LES FONTAINES ABBE PIERRE MARLE

ASSOCIATION POUR LE LOGEMENT DES FAMILLES ET DES ISOLES

ASSOCIATION POUR L'INFORMATION MEDICALE EN SITUATION D'URGENCE

ASSOCIATION POUR UN URBANISME INTEGRE (FOYER DE JEUNES TRAVAILLEURS « LES VILLAGEOISES »)

ASSOCIATION SAINT PAUL

ASSOCIATION TUTELAIRE D'ILLE ET VILAINE

FEDERATION FRANCAISE DE SQUASH

PARTI SOCIALISTE

ASSURANCE

CHARTIS EUROPE

FIA-NET

BANQUE / RECOUVREMENT

BANQUE MARTIN MOREL

BANQUE POPULAIRE DU NORD

BINCKBANK N.V.

BOURSE DIRECT

CAISSE D'EPARGNE ET DE PREVOYANCE NORD FRANCE EUROPE

CAISSE REGIONALE DE CREDIT AGRICOLE MUTUEL NORD DE FRANCE

CERTEGY

CREDIREC ASSET MANAGEMENT

CREDIREC FINANCE

COLLECTIVITÉS LOCALES

CENTRE COMMUNAL D'ACTION SOCIALE DE FONTAINEBLEAU

COMMUNAUTE DE COMMUNES DES PAYS DE SORGUES

COMMUNAUTE D'AGGLOMERATION DE LA ROCHELLE

COMMUNAUTE D'AGGLOMERATION DE LA VALLEE DE MONTMORENCY

COMMUNE DE BLAGNAC

COMMUNE DE DEUIL-LA-BARRE

COMMUNE DE LUNEL

COMMUNE DE MOLIERES-SUR-CEZE

COMMUNE DE MONTMORENCY

COMMUNE DE MURET

COMMUNE DE POITIERS

COMMUNE DE SAINT-GRATIEN

SYNDICAT INTERCOMMUNAL SIVOS DES QUATRE PAYS

COMMERCE

ACXIOM FRANCE

ACCOR

AMERICAN EXPRESS CARTE FRANCE

ARI

AUDIT ET SOLUTIONS

B.E.S. SAS

BOUYGUES TELECOM

BRINK'S FRANCE

CAJIS FRANCE

CD CONSULTING INNOVATIONS CHAUDEMANCHE

CENTRAPEL COMMUNICATION DIRECTE EXTERNALISEE DE L'ENTREPRISE

CONFORAMA FRANCE

▸▸▸

▸▸▸

CUSTOM PUBLISHING FRANCE
CSA CONSULTING
CONFLANS LOISIRS
COTE COURS
DAMART
DIRECT MAILING
DREAMLEAD INTERACTIVE
ECM EXPERTISE ET CONSEIL EN MANAGEMENT
EFFICIENCY NETWORK
EMAILVISION
EMATCH
ENTREPOT LUXE DIRECT
EUROPE ECOLOGIE LES VERTS
EUROCOPTER
FACEO SECURITE PREVENTION
FACET
FCB
GAP FRANCE
GOLFERGREEN
GREEN ENERGY TRADE
GROUPEMENT ALIMENTAIRE CEVENOL
GROUPON FRANCE
HABITALIS 94
H CONSULTANTS
HERMES SELLIER
HORS ANTENNE
J MILLIET BERCY BISTROT CASH BBC
JOHNSON & JOHNSON SANTE BEAUTE FRANCE
KREACTIVE S.A.S
LA FRANCAISE DES EAUX
LA FRANCAISE DES JEUX
LA REDOUTE
LEADERS LEAGUE
LE FOURNIL DE PARIS
MARKETING CONSEIL FINANCES
MEDIASTAY
METRO
NETUNEED
NISSIROS
NUMERICABLE
PARI MUTUEL URBAIN
PASSEDAT LE PETIT NICE
PROFIDEO SERVICES
PROCTER & GAMBLE FRANCE
PROFIDEO SERVICES
PROMONDO
ODYSSEY MESSAGING
ORANGE
RECREA
RESOCOM – MTM
ROYAL SCANDINAVIA HOTEL
RUE DU COMMERCE
SACD
SAMSUNG ELECTRONICS FRANCE
SAS PLESSIS GRAND HOTEL
START PEOPLE
SEA MARCONI FRANCE
SETAYESH NADER (CAREER MONDE INTERNATIONAL)
SOCIETE EUROPEENNE DE TRAITEMENT DE L'INFORMATION
SOCIETE D'EXPLOITATION DE RESEAUX ET DE SERVICES SECURISES
SODEXO
SOFITEL LUXURY HOTELS FRANCE
SONY COMPUTER ENTERTAINMENT
SUD-OUEST TELESURVEILLANCE (SOTEL)
3 SUISSES
TABLE 14
TOYS'R'US
TRANCHANT INTERACTIVE GAMING
TRIDENT MEDIA GUARD
UNIQLO FRANCE
UNION REGIONALE DES SYNDICATS CGT DES ETABLISSEMENTS D'ENSEIGNEMENT SUPERIEUR DE L'ACADEMIE DE LILLE
VERSAILLES VOYAGES
VIALTIS

VOYAGES 31

VOYAGES TOURAVENTURES

VM 28000

VERT MARINE

WEST INTERACTIVE

YATEDO FRANCE

COMMUNICATION

LE REPUBLICAIN LORRAIN

LEXEEK

LEXISNEXIS

ÉDUCATION

ACADEMIE DE CRETEIL (SIEC)

AIS 2

COLLEGE FREDERIC MISTRAL

COLLEGE LENAIN DE TILLEMONT

FEDERATION FRANCAISE DE SQUASH

LYCEE HOCHE

RECTORAT DE BORDEAUX

SIEC

UNIVERSITE DE HAUTE ALSACE

UNIVERSITE PAUL-VALERY MONTPELLIER

IMMOBILIER

CABINET LOUIS XVI

FOYER DE JEUNES TRAVAILLEURS EUGENE HENAFF

FOYER DE JEUNES TRAVAILLEURS LE NOUVEAU MONDE

PARIS HABITAT-OPH

POLICE - JUSTICE

CAMARD & ASSOCIES

CHAMBRE NATIONALE DES COMMISSAIRES-PRISEURS JUDICIAIRES

COMPAGNIE DES COMMISSAIRES-PRISEURS JUDICIAIRES DE PARIS

DIRECTION DE L'ADMINISTRATION PENITENTIAIRE DU MINISTERE DE LA JUSTICE ET DES LIBERTES (ETABLISSEMENT PENITENTIAIRE POUR MINEURS DE MARSEILLE)

DIRECTION DE LA PROTECTION JUDICIAIRE DE LA JEUNESSE DU MINISTERE DE LA JUSTICE ET DES LIBERTES (DIRECTION CENTRALE, DIRECTION INTERREGIONALE DU SUD-EST, DIRECTION TERRITORIALE DES BOUCHES DU RHONE)

ETUDE MILLON & ASSOCIES

MINISTERE DE L'INTERIEUR (DIRECTION DEPARTEMENTALE DE LA SECURITE PUBLIQUE DU VAL-D'OISE)

PREFECTURE DE LA HAUTE GARONNE

PREFECTURE DE POLICE (DIRECTION TERRITORIALE DE LA SECURITE PUBLIQUE DU VAL DE MARNE)

SCP DELOUIS ET CARVAIS

SCP ROBY- SALMON

SCP GUEROULT-DEBADIER-LAMORIL

SYNDICAT NATIONAL DES MAISONS DE VENTES VOLONTAIRES (SYMEV)

SANTÉ / SOCIAL

ALTAO

AMEDIM

AP-HM

AP-HP

CENTRE HOSPITALIER UNIVERSITAIRE DE BESANCON

CENTRE HOSPITALIER DE CALAIS

CENTRE HOSPITALIER DE GUINGAMP

CENTRE HOSPITALIER SAINT-JOSEPH SAINT-LUC

CHRU DE TOURS

CLINIQUE GERIATRIQUE CHATEAU DE GOMBERT

ELSE CARE

EMOSYST FRANCHE COMTE

ESMS CONSEIL

EXELCIA

FONDATION ABBE PIERRE

FONDATION PAUL MILLIET

H2AD

IMADIS

KANTAR HEALTH

LINK CARE SERVICES

MAISON DE RETRAITE LA COLOMBE

▸▸▸

▸▸▸

MAISON DE RETRAITE L'OREE DU MONT

MAISON DE RETRAITE SAINT-JOSEPH

PMSIPILOT

REGIME COACH

PREFECTURE DE LA HAUTE GARONNE

SAHONA CONSEIL

SAFELOGIC

SIMPLIFY

SÉCURITE PRIVÉE

AERO TRAINING CENTER (CAMAS FORMATION)

AGENCE DE RECHERCHES PRIVEES TAILLEPIE

AGENCE DE RECHERCHES PRIVEES WATTRAINT

AGENCE TOURANGELLE ENQUETES ET RECHERCHES (ATER)

ALYZIA SURETE FRANCE

INSTITUT DE FORMATION DES AGENTS DE RECHERCHES (IFAR)

SOCIETE D'INVESTIGATION PRIVEE (SIP)

TRAVAIL

EURO DISNEY ASSOCIES SCA

RANDSTAD

START PEOPLE

TRANSPORT

AEROPORTS DE PARIS

AIR FRANCE

AVIS

CARS DE VERSAILLES

CMA CGM

GRISEL

JC DECAUX

KUNEGEL

NISSAN WEST EUROPE

PROFIDAZ

VEOLIA TRANSPORT

VEOLIA TRANSPORT MIDI-PYRENEES

VINCI PARK SERVICES

LISTE DES ORGANISMES CONTRÔLÉS EN 2011 DISPOSITIFS DE VIDÉOPROTECTION (LOI DE 1995)

ASSOCIATION

ASSOCIATION SYNAGOGUE CHASSELOUP LAUBAT

ŒUVRE FALRET

ASSURANCE

CABINET D'ASSURANCE VIGUIE

BANQUE

BANQUE DE BRETAGNE

BANQUE KOLB

BANQUE PALATINE

BANQUE POPULAIRE

BNP PARIBAS

COLLECTIVITÉS LOCALES

COMMUNE DE MOLIERE-SUR-CEZE

COMMUNE DE NIMES

COMMUNE DE PARIS (CIMETIERE MONTPARNASSE)

COMMUNE DE ROMBAS

COMMUNE DE SAINT-BENOIT

COMMUNE DE VILLENEUVE-LA-GARENNE

SIVOS DES 4 PAYS (SYNDICAT INTERCOMMUNAL)

COMMERCE

AFFLELOU

LA MAISON DU CARILLON

BIJOUTERIE KIM KEE

BOULANGERIE PATISSERIE MEYER

BOUTIQUE ORANGE

BRASSERIE LES DEUX SAVOIES

BRICORAMA

BUFFALO GRILL

CAFE TITON

C&A

CENTRE LECLERC

CINEMA GAUMONT

CINQ SUR CINQ

CHAUDEMANCHE

CMO OBERNAI

CONTINENT 2001 (CARREFOUR)

COTE MAISON

DIESEL

EDF

EMPIRE DE THES

ESPACE SFR

EURODISNEY

FCB

FNAC

GALERIES LAFAYETTE

GO SPORT

GROUPEMENT ALIMENTAIRE CEVENOL

HAUT MEGA

HEMA

HERMES SELLIER

HOTEL ADRIATIC

HOTEL ALL SEASONS

HOTEL CONCORDE SAINT-LAZARE

HOTEL HELVETIA

HOTEL HOLIDAY INN EXPRESS

HOTEL IBIS

HOTEL LE NEGRESCO

HOTEL MERCURE

HOTEL MONTPARNASSE SAINT-GERMAIN

JARDILAND

KFC

LANCASTER

LE FOURNIL DE PARIS

LEON DE BRUXELLES

LES OPTICIENS JEAN LEMPEREUR

L'ILE DE BEAUTE

MAC DONALD'S

MARIONNAUD PARFUMERIE

MONOPRIX

▸▸▸

▸▸▸

MY FIRST
ND LOGISTICS
NOVOTEL
OCEATECH EQUIPEMENT
PASSEDAT LE PETIT NICE
PHARMACIE DE LA REPUBLIQUE
PHARMACIE DES PRINCES
PHARM'HAIR (TCHIP COIFFURE)
PLACOPLATRE
POMME DE PAIN
QUICK
SARL LOPES
SAS PLESSIS GRAND HOTEL
SCALIA ADAMANTE
SCI BERCY VILLAGE
SOFITEL LUXURY HOTELS FRANCE
STARBUCKS COFFEE
SUD-OUEST-TELESURVEILLANCE
SUPERMARCHE SIMPLY MARKET
YVES ROCHER

COMMUNICATION

FRANCE TELEVISION SA

ÉDUCATION / CULTURE / SPORT

AQUAVEXIN (CENTRE AQUATIQUE)
BIBLIOTHEQUE NATIONALE DE FRANCE
CENTRE 16
CENTRE REGIONAL DE DOCUMENTATION PEDAGOGIQUE DE POITOU-CHARENTE
CINEMATHEQUE FRANCAISE
CITE SCOLAIRE COLLEGE ET LYCEE PIERRE ET MARIE CURIE
COLISEUM
ECOLE DE RECONVERSION VINCENT AURIOL
ECOLE NORMALE SUPERIEURE
ENSEMBLE SCOLAIRE JEANNE D'ARC
IUFM D'AIX-MARSEILLE
MUSEE D'ARCHEOLOGIE NATIONALE
MUSEE DE L'ARMEE
MUSEE DES DOUANES
MUSEE DE PICARDIE
MUSEE NATIONAL DE L'ORANGERIE
MUSSE RODIN
OPERA NATIONAL DE PARIS
PAROISSE NOTRE DAME DE LA NATIVITE DE BERCY
PINACOTHEQUE

IMMOBILIER

AQUITANIS
OPAC D'AMIENS

SANTÉ / SOCIAL

MAISON DE RETRAITE SAINT-JOSEPH
MAISON DE RETRAITE LA COLOMBE
MAISON DE RETRAITE L'OREE DU MONT
POLE EMPLOI POITOU-CHARENTE

TRANSPORT

CMA – CGM
SNCF
TSP AMBULANCES
VEOLIA TRANSPORT

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

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

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

www.cnil.fr

Diffusion
Direction de l'information légale et administrative

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

ISBN : 978-2-11-009075-1
DF : 5HC30880
Prix : 15 €

CNIL
Commission Nationale de l'Informatique et des Libertés