rapport d'activité 2013

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

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

CNIL
Commission Nationale de l'Informatique et des Libertés

La documentation Française

COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

RAPPORT D'ACTIVITÉ **2013**

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

LES CHIFFRES CLÉS DE 2013

DÉCISIONS ET DÉLIBÉRATIONS

2 542
DÉCISIONS ET DÉLIBÉRATIONS
dont **247** autorisations,
3 autorisations uniques,
129 avis,
3 recommandations

CONTRÔLES

414
CONTRÔLES
dont **130** contrôles
de vidéoprotection

MISES EN DEMEURE ET SANCTIONS

57
MISES EN DEMEURE
dont **4** rendues publiques,
8 concernant
des dispositifs de
vidéoprotection

14
SANCTIONS
dont **7** sanctions
financières

5
AVERTISSEMENTS
dont **2** publics,
1 relaxe,
1 non lieu

FORMALITÉS PRÉALABLES

92 351
DOSSIERS DE
FORMALITÉS TRAITÉS

11 085
DÉCLARATIONS
RELATIVES À DES
SYSTÈMES DE
VIDÉOSURVEILLANCE

5 514
DÉCLARATIONS RELATIVES
À DES DISPOSITIFS DE
GÉOLOCALISATION

416
AUTORISATIONS
DE SYSTÈMES
BIOMÉTRIQUES

AIDE ET CONSEIL

35 524
COURRIERS REÇUS

124 595
APPELS TÉLÉPHONIQUES

PLAINTES ET DEMANDES DE DROIT D'ACCÈS INDIRECT

5 640
PLAINTES

4 305
DEMANDES DE DROIT
D'ACCÈS INDIRECT
(FICHIERS DE POLICE,
DE GENDARMERIE,
DE RENSEIGNEMENT,
FICOBA, ETC.)

CORRESPONDANTS

13 000
ORGANISMES ONT DÉSIGNÉ
UN CORRESPONDANT

37
ATELIERS
D'INFORMATION
QUI ONT ACCUEILLI
1 251 PARTICIPANTS

LABELS

29
LABELS DÉLIVRÉS
(au 14 février 2014)

MOYENS DE LA CNIL

16,9
MILLIONS D'EUROS
DE BUDGET

178
AGENTS

INTERVENTIONS EXTÉRIEURES

180
INTERVENTIONS

NOTIFICATIONS DE VIOLATIONS DE DONNEES PERSONNELLES

15
NOTIFICATIONS EN 2013

SOMMAIRE

AVANT-PROPOS DE LA PRÉSIDENTE

LE CHOC DE L'AFFAIRE PRISM : VERS UNE SURVEILLANCE MASSIVE ET GÉNÉRALISÉE DE L'ENSEMBLE DE LA POPULATION

À l'heure de rédiger le bilan de l'année 2013, un événement majeur l'emporte sur les autres sujets. Je veux parler du choc consécutif aux révélations d'Edward Snowden sur le système de surveillance américain Prism. Avec Prism, un pas vers la surveillance massive et généralisée de l'ensemble de la population par des acteurs privés, pour le compte d'acteurs publics est allégrement franchi. Le choc ne consiste pas à découvrir que les services de renseignement coopèrent et collaborent, qui l'ignorait ? Le choc consiste à déchirer le voile et révéler au grand jour **une rupture majeure dans le paradigme de la surveillance**, que d'autres affaires avant Prism avaient pu déjà laisser entrevoir (PNR, SWIFT).

> « Il faut comprendre pourquoi, en dehors de quelques voix qui s'élèvent ici ou là, nos démocraties font preuve d'un tel fatalisme. »

Cette rupture réside dans le fait que, sous couvert de lutte contre le terrorisme, **la présomption d'innocence est inversée.** Ainsi donc, tout le monde est surveillé *a priori* et plus seulement les « populations à risque ou suspectes » et ceci, au travers de ses usages quotidiens. La norme devient donc la surveillance généralisée par défaut des personnes, en dehors de tout cadre légal, ce qui n'est pas acceptable dans un État de droit. Avec Prism, c'est le cœur du pacte social et démocratique qui est menacé, et ce, dans une grande indifférence, voire une certaine résignation.

On touche ici au deuxième choc de l'affaire. À part en Allemagne, la plupart des opinions publiques ou des prises de positions européennes ont en effet été fort mesurées, sinon silencieuses, mettant en avant les besoins de coopération des services de renseignement ou l'impuissance à s'opposer à la collecte de données via les grands acteurs mondiaux de l'Internet.

L'affaire Snowden est donc un choc en ce qu'elle met en lumière un changement d'univers et de mentalités et la question est de savoir comment répondre à cela.

Pour apporter ces réponses d'ordre politique, juridique et technique, et elles existent, **il faut comprendre pourquoi, en dehors de quelques voix qui s'élèvent ici ou là, nos démocraties font preuve d'un tel fatalisme.**

Tout d'abord, force est de constater que **la généralisation du numérique a fragilisé notre capacité d'analyse**, y compris au niveau de nos élites. Cette généralisation change fondamentalement notre perception des notions

Isabelle Falque-Pierrotin,
Présidente de la CNIL

de temps et d'espace et met à l'épreuve nos concepts fondamentaux. Elle nous impose donc de penser des solutions dans un monde complexe et mouvant que nous appréhendons mal.

Cette absence d'analyse critique se double d'**une fascination technologique qui vire à l'apathie**. On l'a vu d'ailleurs avec Prism, où l'on constate que la technique a pris le pas sur la politique. Les technologies, parce qu'elles procurent incontestablement un grand bénéfice d'usage et de service, ne devraient être entravées par aucune limite, aucune borne. Les besoins de l'innovation deviennent des impératifs catégoriques devant lesquels consommateurs, États ou régulateurs doivent s'incliner.

Mais si les technologies n'ont jamais été si puissantes, si accessibles, si peu chères pour certaines, apportant ainsi leurs bénéfices à tous, la tentation est aussi grande de les utiliser pour surveiller les salariés, les citoyens, les enfants, les voisins ou les conjoints. Encadrer les technologies et leurs usages n'est donc pas un crime de lèse-technologie mais une volonté légitime de garantir une utilisation de celles-ci respectueuse des libertés.

Une fascination un peu similaire s'opère à l'égard **des grands acteurs économiques (GAFA) qui sont quelques uns à centraliser entre leurs mains l'architecture d'Internet**, pourtant à l'origine très décentralisée. Parce qu'ils sont puissants, et qu'ils ont acquis une place centrale et appréciée dans la vie quotidienne des personnes, ces acteurs pourraient s'affranchir des règles applicables au « commun des mortels ». Leur utilité sociale semble telle qu'il ne leur serait demandé aucun compte. En réalité, ce que leur demandent les autorités de protection de données, c'est simplement d'ouvrir leur « boîte noire » et de rendre leurs pratiques plus transparentes. Il ne s'agit pas de remettre en cause leur modèle économique dont les données personnelles constituent la principale richesse, mais de les contraindre à une utilisation de ces données moins opaque. Ce que souhaitent d'ailleurs leurs clients.

Ceux-ci évoluent et apprivoisent progressivement le numérique. Ils ne sont pas opposés par principe à la collecte de leurs données ; ils **revendiquent même l'existence d'une vie publique en ligne à partir de celles-ci**. On voit ainsi apparaître une approche plus individuelle et quantitative de la vie privée, avec une *privacy* que chacun souhaite paramétrer selon ses souhaits, comme on paramètre son compte sur un réseau social. En ce sens, on peut dire que la vie privée tend à devenir une affaire strictement privée, voire consumériste, qui s'éloigne d'une dimension à l'origine plus collective. Aujourd'hui, c'est de maîtrise que les individus sont demandeurs, plus que de protection.

Face à ces différents constats, les réponses pour éviter une surveillance généralisée des personnes sont délicates à apporter et il faut se méfier des « fausses bonnes idées ».

La première piste avancée consiste à considérer que la loi Informatique et Libertés doit être entièrement revue sous prétexte d'obsolescence et que des principes nouveaux doivent être retenus, notamment une approche par le risque. S'il est vrai qu'une plus grande adaptation au numérique devient urgente, et c'est bien le sens du projet de règlement européen, **les principes « Informatique et Libertés » demeurent robustes et adaptables aux évolutions**

technologiques. La CNIL œuvre d'ailleurs au niveau européen pour trouver un juste équilibre entre croissance économique et libertés fondamentales. Il serait fort inopportun, alors que la concurrence mondiale autour des données se renforce, de fragiliser notre appareil normatif dans un sens fort incertain.

Le deuxième écueil réside dans la mise en avant, ici ou là, d'**une patrimonialisation des données**. *A priori* séduisante, cette démarche impose en réalité une grande prudence car la privatisation de ses données, et donc leur possible cession ou vente, revêt un caractère d'irréversibilité préoccupant pour l'individu. Les droits une fois vendus, comment reprendre la main sur ses données ? À l'inverse, le droit actuel de la protection des données personnelles ouvre des droits à l'individu même lorsque ses données sont produites et traitées par d'autres.

La troisième « fausse bonne idée » pour faire face à l'encadrement de la masse considérable de données consisterait à substituer à la régulation des autorités de contrôle, **une régulation par des tiers**. Ceux-ci seraient alors seuls compétents pour élaborer les référentiels et certifier les *process* des organismes.

Mais si la régulation doit intégrer une dimension d'autorégulation, si elle peut faire appel à des certificateurs externes, n'est-ce pas le rôle des régulateurs publics de fixer le niveau d'exigence de celle-ci et les standards généraux qu'elle doit respecter. Notre approche européenne de co-régulation est à ce titre une réponse efficace et pragmatique.

Dans le fond l'enjeu est de savoir collectivement ce que nous voulons et vers quel type de société nous souhaitons évoluer. La vitesse accrue du développement technologique et son aura quasi-systématiquement positive, ne doivent pas nous dispenser d'une réflexion morale et éthique. Certaines balises doivent être fixées, voire peut-être aussi certains tabous, sans que cela ne soit perçu comme une entrave à l'innovation technologique. Un parallèle peut être fait avec la bioéthique qui réunit une pluralité d'acteurs et de disciplines pour choisir ensemble si des limites doivent être posées, au bénéfice des individus (manipulations génétiques sur les plantes, clonage humain, procréation humaine, etc.). Cette réflexion prend aussi tout son sens à l'heure où certains affichent sans complexe des ambitions transhumanistes ou « d'humanité augmentée » ayant pour but ultime l'avènement vers 2060 d'une intelligence supérieure à l'intelligence humaine.

Dans une moindre mesure, la gouvernance des algorithmes qui est au cœur du *big data*, pose aussi la question d'un possible enserrement de l'homme dans un modèle mathématique. Les technologies de calcul mathématique et leur utilisation à des fins prédictives ne risquent-elles pas à terme de figer les individus dans des cases et les priver ainsi de leur capacité de choix ou de libre arbitre ?

On le voit, l'action de la CNIL intervient dans un contexte complexe d'interrogations.

Dans tous les cas, il faut combattre farouchement l'argument sans **cesse ressassé du « rien à se reprocher, rien à cacher ». Ce raisonnement simpliste** est précisément celui qui était utilisé par les régimes totalitaires pour justifier la surveillance généralisée. Il associe le droit à l'intimité à la culpabilité plutôt que de l'associer à une liberté fondamentale non négociable. Il affirme que la vie privée est ce que l'on cache alors que la vie privée est l'expression de la volonté légitime d'autonomie de chacun d'entre nous.

> “ L'enjeu est de savoir collectivement ce que nous voulons et vers quel type de société nous souhaitons évoluer. ”

2014 est donc une année clé pour, au plan national comme européen, avancer dans l'exercice de ces choix. C'est une CNIL combative et ouverte qui entend accélérer son virage du numérique et faire entendre sa voix, en France et au-delà, pour défendre une vision moderne de la protection des données et alerter sur les menaces réelles de la généralisation d'une société de surveillance.

Une CNIL réorganisée pour faire face aux nouveaux défis. »

MOT DU SECRÉTAIRE GÉNÉRAL

Alors que l'année 2013 a constitué une année charnière pour la protection des données, sous le double effet des révélations de M. Snowden et des avancées concomitantes des négociations sur le projet de règlement européen, la CNIL doit, plus que jamais, remplir ses missions avec exigence et efficacité. **La massification du traitement des données personnelles**, tout comme la **diversification de ses usages**, implique en effet que notre institution, non seulement soit en mesure de faire face à l'exceptionnelle croissance de son activité, mais aussi fasse preuve d'initiative et d'innovation, aussi bien en termes de méthodes que d'outils de régulation. C'est précisément pour répondre aux attentes de ses différents publics que la CNIL a procédé, en avril 2014, à la réorganisation de ses services.

L'activité de la CNIL en 2013 a tout d'abord été marquée, comme les années précédentes, par une forte croissance. Si le nombre de plaintes a pu être stabilisé, essentiellement grâce à une meilleure orientation des demandes dès leur réception, l'activité globale de la Commission et de ses services a encore connu une très forte augmentation : ce sont ainsi 2542 délibérations ou décisions qui ont été adoptées par la Commission (+ 20 % par rapport à 2012). Tous les indicateurs d'activité, repris dans le présent rapport annuel, témoignent du même phénomène : **la « datification », corollaire de l'ère numérique**, est au cœur de la vie économique et sociale contemporaine.

Cette évolution se traduit directement par la sensibilité croissante de nos concitoyens à la protection de leurs données, et par **l'intensification de la mission d'information et d'éducation au numérique de la CNIL**. Outre la constitution d'un collectif d'une cinquantaine d'organismes publics et privés à l'initiative de la CNIL en faveur de l'éducation au numérique, les services de la CNIL remplissent une mission d'information essentielle auprès de tous les publics : à titre indicatif, ce sont ainsi 124 000 appels téléphoniques qui ont été traités par la CNIL en un an, tandis que les comptes de la CNIL sur les réseaux sociaux sont suivis par un nombre croissant d'internautes.

Édouard Geffray,
Secrétaire général

La CNIL est également en première ligne pour faire face à l'accroissement des problématiques de surveillance : à la suite de l'affaire Snowden, **la CNIL a ainsi pris fortement position sur le sujet et a proposé des réponses juridiques effectives**, qui ont d'ailleurs convergé avec les amendements apportés par le Parlement européen au projet de règlement. Au quotidien, la sensibilité des citoyens à cette problématique s'est également retrouvée dans l'accroissement continu des demandes de « droit d'accès indirect » aux fichiers de sécurité publique, qui ont encore augmenté de 17 %, après une hausse de 75 % en 2012.

Mais l'activité de la CNIL ne peut se réduire à un simple bilan quantitatif. Derrière les chiffres, c'est bien **l'évolution des métiers de notre institution qui s'opère**. La CNIL, en tant que régulateur, est en effet amenée à accompagner les collectivités publiques ou entreprises, dans une véritable démarche de **mise en conformité**. Le développement de nouveaux outils de régulation en est un signe. Ainsi, ce sont plus de 13 000 organismes qui sont dotés d'un « correspondant Informatique et Libertés » (+ 20 % par rapport à 2012), véritable acteur de la mise en conformité dans son organisme. Il en va de même de l'adoption d'un troisième référentiel de labellisation (sur les coffres-forts numériques), ou encore de l'approbation des « règles d'entreprise contraignantes » (BCR) pour un cinquantième groupe international.

La régulation, pour être efficace et crédible, implique donc que la CNIL utilise une **gamme d'outils élargie** pour faire connaître et respecter les droits et obligations en termes « Informatique et Libertés ». La démarche menée tout au long de l'année 2013 sur les cookies en constitue l'illustration : après un an de concertation avec l'ensemble des fédérations représentatives des professionnels du secteur, la CNIL a émis, en décembre 2013, une recommandation sur les cookies, qu'elle a accompagnée d'une vidéo pédagogique pour le grand public, de fiches pratiques pour les différents acteurs et, pour la première fois, d'un logiciel développé par ses experts et permettant de visualiser la « face cachée » d'une navigation sur Internet. Cet outil, en *open source*, a été téléchargé plusieurs dizaines de milliers de fois.

Efficacité, concertation, diversification des outils : ce triptyque a été complété, début 2014, par **la réorganisation des services de la CNIL**. Dans le cadre du plan d'orientation stratégique 2012-2015, la CNIL a développé une stratégie claire : **s'adapter à un environnement numérique en constante évolution en développant une gamme élargie d'outils de régulation et en plaçant ses publics au cœur de son activité**. Mais ses services étaient essentiellement organisés autour des différents métiers qu'elle exerce. La présidente de la CNIL a donc procédé, après une large concertation interne, à la réorganisation des services autour de nos publics. Ainsi, les services sont désormais organisés en cinq directions : la direction de la conformité, qui sera en charge principalement de la mise en conformité des responsables de traitements ; la direction des relations avec les publics, qui portera la mission d'information des différents publics, notamment les particuliers et le monde de la recherche ; la direction de la protection des droits et des sanctions, en charge de s'assurer *a posteriori* du respect de l'effectivité des droits des personnes ; la direction des technologies et de l'innovation, qui concentrera l'expertise technologique de la CNIL au service de ses différents métiers et le suivi de l'innovation ; et la direction administrative et financière, qui regroupera les services supports (finances, moyens généraux, RH).

Enfin, la CNIL s'est dotée, dans le prolongement de cette réorganisation, d'un schéma directeur de ses systèmes d'information pour, à l'horizon 2015, refondre profondément ses outils au service des publics. L'objectif est, notamment, de développer la réponse « multicanal », grâce à un système de questions / réponses en ligne sur le site Internet de la CNIL, qui permettra à nos usagers, aussi bien particuliers que professionnels, de trouver facilement des réponses à leurs interrogations sur notre site.

À quelques mois de l'adoption du règlement européen, la CNIL se caractérise donc par son adaptation : adaptation à un environnement en constante mutation ; adaptation aux attentes de ses publics ; adaptation de ses méthodes et de ses outils. Elle est ainsi en mesure de garantir l'effectivité des droits qu'elle a pour mission de protéger, et de participer à la création du cadre de confiance et de valeurs indispensable au développement équilibré du numérique. Tout cela est rendu possible par l'engagement de ses agents : je tiens ici à remercier ces 185 femmes et hommes pour leur investissement au service d'une mission d'intérêt général, qui partagent la conviction que la protection des données personnelles constitue un marqueur des États de droit contemporains, et qui, par leur activité quotidienne, permettent de faire vivre le cadre de régulation fixé par le législateur et décliné par la Commission.

1.
ANALYSES JURIDIQUES

Données de santé : le NIR, identifiant national de santé ?

Les données personnelles à l'heure du numérique

L'application extraterritoriale des lois des États tiers et la protection des données personnelles : enjeux et perspectives

La proposition de règlement européen

DONNÉES DE SANTÉ : LE NIR, IDENTIFIANT NATIONAL DE SANTÉ ?

Le partage de l'information médicale est aujourd'hui reconnu par tous comme la garantie d'une meilleure prise en charge médicale des malades, comme un moyen de remédier aux déséquilibres croissants de la démographie médicale et de lutter contre les dérives des dépenses de santé. Ces technologies sont également susceptibles de permettre aux patients de mieux maîtriser les données de santé qui les concernent et de participer plus activement à leur parcours de soins.

Le développement d'une « médecine en réseau » revêt donc un caractère stratégique qui se traduit par le développement de la *e-santé*, notamment dans le cadre de la Stratégie nationale de santé, présentée le 23 septembre 2013.

Dans ce contexte, le déploiement de solutions de sécurité effectives et de haut niveau est une priorité. La sécurité des systèmes d'information passe notamment par une identification fiable, unique et pérenne des patients dans le cadre d'un partage d'informations les concernant.

Elle rend donc nécessaire le développement de systèmes d'informations médicales fondés sur des dispositifs d'identification des patients qui soient fiables et homogènes permettant ainsi, sans risque d'erreur et dans l'intérêt des patients, des échanges d'informations nécessaires pour coordonner de façon efficace les soins qui leur sont prodigués.

La CNIL a souligné que l'utilisation d'un identifiant qui présente des qualités de fiabilité, d'unicité et de pérennité répond à une nécessité fonctionnelle à travers les nombreux chantiers de la *e-santé* auxquels elle participe en sa qualité d'autorité de protection des données. Il convient d'éviter tant les doublons aboutissant à créer plusieurs dossiers pour une même personne, que les collisions conduisant à rattacher des données de santé d'une personne à une autre.

> La sécurité des systèmes d'information passe notamment par une identification fiable, unique et pérenne des patients.

Dans cette perspective, le législateur a prévu la création d'un identifiant national de santé (INS) des patients, utilisable dans l'ensemble du système de soins (C. santé publ., art. L. 1111-8-1).

La loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (art. 5) avait cantonné son usage à l'ouverture et la tenue du Dossier médical personnel (DMP). La loi n°2007-127 du 30 janvier 2007 relative aux professions de santé en a étendu l'usage à la prise en charge des patients dans l'ensemble du système de soins, notamment, pour l'ouverture et la tenue du DMP et du Dossier Pharmaceutique (DP).

La question, régulièrement posée à la Commission, concerne le choix de l'identifiant national de santé en général et celui du NIR en particulier.

INFOS +

Communément appelé « numéro de sécurité sociale », le NIR ou numéro d'inscription au Répertoire national d'identification des personnes physiques (RNIPP) constitue un identifiant fiable et stable attribué par l'INSEE à la naissance de la personne et certifié par lui à partir d'éléments d'état civil transmis par les mairies, selon une procédure fondée sur des outils de certification préexistants, reconnus et éprouvés depuis 1996.

Cet identifiant est familier des patients, disponible sur la carte Vitale des bénéficiaires de l'assurance maladie de plus de 16 ans, et déjà présent et utilisé dans tous les logiciels de gestion administrative et médicale des professionnels et établissements de santé, dans le cadre de leurs relations avec l'assurance maladie. Retenir le NIR comme identifiant national de santé emporterait donc pour ces derniers peu de conséquences techniques et de perturbations des systèmes existants au sein desquels il est traité.

Dès lors, le recours à l'identifiant fiable et disponible qu'est le NIR peut apparaître comme la solution permettant de résoudre les problèmes qui résulteraient de la création d'un identifiant spécifique pour une population de plus de 65 millions de personnes.

Pourtant, les arguments de simplicité, de commodité et de moindre coût ne sont pas de nature, à eux seuls, à clore le débat, bien qu'ils ne soient pas sans portée dans un contexte de gestion rigoureuse des dépenses publiques.

Le NIR a toujours occupé dans la loi « Informatique et Libertés », y compris depuis sa modification, une place particulière. L'origine même de cette loi vient d'une réflexion engagée à l'occasion d'un projet d'une connexion de fichiers publics à partir du numéro de sécurité sociale, risquant d'aboutir au « fichage » de l'ensemble de la population.

Les spécificités du NIR, et notamment son caractère signifiant, donc facile à reconstituer à partir des éléments d'état civil, justifient que le recours à cet identifiant soit strictement encadré par la loi du 6 janvier 1978 et cantonné aux finalités pour lesquelles son utilisation est permise. Parce qu'il rend plus aisées les possibilités de rapprochements de fichiers et qu'il facilite la recherche et le tri des informations dans les fichiers, le NIR reste associé au risque d'une interconnexion généralisée ou d'une utilisation détournée des fichiers.

C'est pourquoi, s'appuyant sur les dispositions de la loi, la CNIL a élaboré une doctrine de « cantonnement » du NIR, limitant l'usage de cet identifiant unique à la sphère de la sécurité sociale – qui lui a donné son nom usuel – et n'acceptant qu'à titre exceptionnel qu'il soit utilisé dans d'autres secteurs dans sa fonction de certification de l'identité.

Interrogée sur la question de l'utilisation du NIR comme identifiant national de santé en 2006, la Commission avait préconisé, dans son avis du 20 février 2007, le recours à un identifiant spécifique fondé sur une anonymisation du NIR, c'est-à-dire un identifiant distinct du NIR, mais bénéficiant du processus de certification de ce dernier.

La CNIL n'a toujours pas été saisie du projet de décret simple prévu par l'article L. 1111-8-1 du Code de la santé publique qui doit fixer le choix de cet identifiant, ainsi que ses modalités d'utilisation.

Toutefois, dans la perspective de l'élaboration de ce texte, la Commission a été invitée par le Gouvernement en 2013 à se prononcer à nouveau sur la question du choix du NIR comme INS au regard des besoins accrus de l'utilisation de cet identifiant dans le secteur de la santé, dans un contexte institutionnel et technique modifié depuis 2007.

La Commission a, dès lors, procédé à un nouveau débat sur la question. Au vu des arguments qui lui ont été présentés, elle s'est montrée ouverte à une évolution de la position adoptée dans son avis de 2007, à condition que l'utilisation du NIR dans la sphère de la santé aille de pair avec l'élévation de solides remparts vis-à-vis d'autres secteurs. ■

LES BESOINS ACCRUS D'UTILISATION DU NIR DANS LE SECTEUR DE LA SANTÉ

La coordination des soins suppose des appariements de données robustes

Le développement d'une « médecine en réseau » à des fins de coordination des soins impose de mettre à la disposition des professionnels de santé des outils d'échange et de partage qui garantissent la sécurité sanitaire des patients par une identification fiable. Le développement de la *e-santé* suppose donc la mise en œuvre d'appariements entre systèmes d'information, qui soient « robustes », sur un mode transactionnel et en temps réel. C'est un enjeu majeur de sécurité sanitaire.

À cet égard, la cœxistence actuelle d'identifiants numériques limités sur le plan géographique et temporel n'est pas satisfaisante. Les méthodes classiques d'appariements faisant appel à des traits d'identité multiples et non pérennes sont donc à exclure.

C'est pourquoi, afin d'améliorer l'identification des patients dans le cadre de projets régionaux et nationaux impliquant des échanges et partages d'informations, la CNIL a examiné au cas par cas les projets d'identifiants numériques qui lui ont été soumis dans l'attente de la mise en œuvre de l'identifiant national de santé.

Ainsi, dans le cadre de la mise en place du Dossier pharmaceutique (DP) en 2007 et de ses déploiements successifs, dans l'ensemble des officines en 2008 et des « pharmacies à usage intérieur » des établissements hospitaliers en 2013, la Commission a admis l'utilisation d'un identifiant provisoire.

Le NDP : numéro d'identification du patient est calculé automatiquement à partir des traits identifiants de la carte Vitale (dont les nom et prénom du titulaire et le numéro de série de la carte).

Dans le cadre du déploiement généralisé du DMP en 2010, l'ASIP Santé a souhaité déployer un identifiant national de santé provisoire, dénommé « INS-C », également dérivé par hachage de traits d'identité figurant sur la carte Vitale de l'assuré (NIR, jour de naissance, prénom), et calculé automatiquement par les logiciels métiers des professionnels par l'application d'un algorithme public sur ces traits d'identité.

La Commission a admis cette solution qui apparaissait conforme à ses préconisations de recourir à un identifiant spécifique, non signifiant, fondé sur une anonymisation du NIR. Elle a toutefois indiqué que compte tenu des insuffisances de l'INS-C[1], cette solution ne pouvait être admise que de façon provisoire, dans l'attente de la mise en place de l'INS aléatoire (INS-A) prévu à terme[2].

Actuellement, chaque système d'information de santé peut faire le choix de son propre numéro d'identification. Le développement de réseaux régionaux ou de plateformes régionales de santé qui permettent la création de dossiers médicaux partagés sur Internet a, dans certains cas, entraîné la création d'identifiants sectoriels.

Or, la cœxistence actuelle d'identifiants numériques limités sur le plan géographique et temporel rend difficilement interopérables des dispositifs dont la convergence serait pourtant utile à la coordination des soins et conforme à la volonté du législateur.

La question du choix de l'identifiant utilisable dans l'ensemble du système de soins n'est en outre pas sans lien avec les besoins des autorités sanitaires et des chercheurs de pouvoir relier les données de santé avec les données médico-administratives indexées sur le NIR, dans le cadre de travaux de recherche et d'études de santé publique.

Les appariements nécessaires aux besoins de santé publique

Depuis plusieurs années, les chercheurs et les autorités sanitaires réclament un meilleur accès aux données contenues dans les bases médico-administratives à des fins de surveillance épidémiologique et de pilotage des politiques de santé publique.

Le Système national d'information interrégimes de l'assurance maladie (SNIIRAM), institué par la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale, n'est pas seul concerné, mais ses données sont particulièrement convoitées en raison de son exhaustivité et de sa puissance statistique.

Les enjeux de santé publique et de sécurité sanitaire qui s'attachent à l'utilisation des bases de données médico-administratives indexées sur le NIR et la nécessité d'apparier les données contenues dans ces bases et les données cliniques produites par les professionnels de santé dans le cadre des soins font aujourd'hui l'objet d'un consensus.

Mais, la clé d'accès à de nombreux fichiers et, notamment, aux fichiers de l'assurance maladie ou de l'assurance vieillesse, est le NIR (ou un dérivé), que les chercheurs et les autorités sanitaires ne sont habilités à utiliser qu'après un décret en Conseil d'État pris après avis motivé et publié de la CNIL (article 27) ou une autorisation délivrée par la CNIL (article 25), selon que l'organisme est un organisme public ou privé. Les textes actuels peuvent ainsi avoir pour effet d'alourdir les procédures et d'allonger les délais en matière d'exploitation des bases médico-administratives.

Consciente des enjeux que soulève cette question et de la nécessité de maintenir le niveau de la recherche sur le plan international, la Commission a pris l'initiative, dès 2010, de saisir les services du Premier ministre pour attirer leur attention sur la nécessité d'élaborer un décret en Conseil d'État « cadre », qui prévoie et détermine une politique d'accès encadré au NIR pour les chercheurs et les autorités sanitaires. Les dispositions combinées du IV de l'article 26 et du III de l'article 27 de la loi du 6 janvier 1978 modifiée devraient en effet permettre de procéder par un « acte réglementaire unique » à ces fins, tout en encadrant les conditions d'utilisation du NIR.

Au-delà de cette proposition, les travaux en cours menés par le ministère de

[1] *L'INS-C, en effet, ne permet pas d'apporter la garantie absolue de non collision et d'absence de doublon et tous les bénéficiaires de l'assurance maladie n'en seront pas dotés (les enfants en particulier).* / [2] *Délibération n° 2010-4449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du DMP.*

la Santé à la suite de la remise du rapport de M. Pierre-Louis Bras sur « la gouvernance et l'utilisation des données de santé », et auxquels la CNIL est étroitement associée, devraient être finalisés au printemps 2014 et pourraient conduire à une adaptation des textes en la matière.

En l'attente d'une évolution des textes, la CNIL est saisie, ponctuellement, de projets de décrets pour autoriser, au cas par cas, l'utilisation du NIR à des fins de recherche et d'études de santé publique.

INFOS +

SNIIRAM

Le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) est une base nationale instituée par la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale (CSS, art. L. 161-28-1), qui recense tous les actes médicaux, les prestations effectuées et les pathologies en ville et à l'hôpital, pour mieux connaître l'évolution des dépenses de santé. Il est géré par la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS). Il repose sur le principe de l'anonymat des bénéficiaires, obtenu, en particulier, par un double dispositif de hachage du numéro de sécurité sociale et des éléments d'identité de l'assuré, par le principe de l'absence de croisement des variables dites « sensibles » et par l'absence d'affichage de résultats en dessous d'un seuil de dix individus. L'accès au SNIIRAM est strictement encadré par l'arrêté actuellement en vigueur du 19 juillet 2013, pris après avis motivé de la CNIL et approuvant un protocole qui définit ses modalités de gestion et de renseignement. Sa particularité est d'être une base nationale, liée à l'assurance santé obligatoire ; elle est de ce fait unique, et d'une richesse sans équivalent en Europe, et peut s'avérer particulièrement utile pour effectuer des études de santé publique. C'est pourquoi la CNIL s'est prononcée favorablement sur les évolutions du SNIIRAM depuis sa création au fil des arrêtés modificatifs successifs dès lors qu'elles étaient compatibles avec le cadre juridique existant. Elle estime cependant nécessaires une réévaluation des mesures de sécurité mises en œuvre et une évaluation du risque de ré-identification des personnes lié à l'extension progressive des accès au SNIIRAM.

Une ligne de partage de plus en plus difficile à tracer entre la santé et le social

Il existe une proximité croissante entre le secteur social et le secteur de la santé, qui conduit à tempérer la doctrine du cantonnement du NIR à la seule sphère sociale et son exclusion de la sphère médicale.

Dans la mesure où le NIR est par nature l'identifiant des fichiers de sécurité sociale, et où il est nécessaire pour les opérations de remboursement des soins par l'assurance maladie, il figure dans toutes les applications des professionnels de santé, organismes ou établissements dispensant à des assurés sociaux ou à leurs ayants droit des actes ou prestations pris totalement ou partiellement en charge par l'assurance maladie. La mise en place, depuis 1996, de la procédure de télétransmission des feuilles de soins électroniques a généralisé le développement d'applications informatiques gérant tout à la fois le dossier administratif et le dossier médical des patients.

De son côté, l'assurance maladie détient des informations d'une très grande précision sur la santé des assurés sociaux.

Cette évolution, initiée en 1996 par l'instauration du codage des actes, des prescriptions et des pathologies dans les feuilles de soin électronique, s'est accentuée encore avec la mise en place de la tarification à l'activité (T2A).

Ces données médico-sociales sont utilisées à des fins de prise en charge médicale des patients ou de santé publique et cette utilisation est appelée à croître.

Pour preuve de cette tendance, le Web médecin (ou « historique des remboursements »), créé par le législateur en 2004, est un service proposé par l'assurance maladie qui permet aux professionnels de santé, à l'occasion des soins qu'ils délivrent, d'accéder, à partir du NIR des bénéficiaires de l'assurance maladie (qui figure dans leur carte Vitale), à l'ensemble des informations médicales relatives aux actes et prestations qui leur ont été remboursés au cours des douze derniers mois. Ce dispositif, utile à la coordination des soins, permet de limiter les risques d'incompatibilité médicamenteuse et de réduire les examens redondants.

La CNIL a d'ailleurs émis un avis favorable en 2012 sur un projet de décret permettant l'utilisation du NIR par les services en santé de la CNAMTS dans le cadre de ses programmes d'accompagnement des personnes atteintes de maladie chronique, après la phase d'expérimentation du programme « SOPHIA »[3].

Les données médico-sociales sont également de plus en plus utilisées pour des finalités de santé publique.

M. Bras propose d'ailleurs, dans son rapport précité, de modifier toute l'économie du SNIIRAM, conçu initialement à des fins de maîtrise des dépenses, pour en faire un outil utilisé à des fins de santé publique. Il propose donc de modifier l'article L. 161-28-1 du Code de la sécurité sociale pour que la loi traduise clairement cette évolution et de rebaptiser le SNIIRAM en « Système National d'Information Santé ».

La CNIL, quant à elle, a accepté depuis longtemps que le NIR issu des ▸▸▸

[3] Décret n° 2012-1249 du 9 novembre 2012 autorisant la création de traitements de données à caractère personnel par la mise en œuvre de programmes de prévention et d'accompagnement en santé des assurés sociaux.

fichiers des caisses d'assurance maladie puisse être utilisé pour convoquer des assurés sociaux à des opérations de dépistage du cancer par les organismes chargés de ces campagnes[4].

Elle a accepté également que le NIR soit utilisé par l'Institut de radioprotection et de sûreté nucléaire à des fins de surveillance de l'exposition des travailleurs des centrales nucléaires aux rayonnements ionisants, au motif que les doublons peuvent avoir pour effet de sous-estimer la dose radioactive subie par une personne[5].

Elle s'est prononcée favorablement sur les évolutions du SNIIRAM depuis sa création au fil des arrêtés modificatifs successifs, dès lors qu'elles étaient compatibles avec le cadre juridique existant.

Par ailleurs, comme indiqué précédemment, la CNIL se prononce régulièrement en faveur d'une utilisation du NIR dans le cadre de projets de recherche ponctuels compte tenu de l'intérêt général des usages envisagés et moyennant des conditions de sécurité effectives et de haut niveau.

C'est ainsi qu'elle s'est prononcée favorablement, le 19 juillet 2012, sur un projet de décret en Conseil d'État autorisant le traitement informatique du NIR dans le cadre de l'étude « Nutrinet-Santé » menée par l'INSERM[6], le 14 février 2013 dans le cadre de l'étude « Esteban » menée par l'Institut de veille sanitaire (InVS)[7] et le 18 juillet 2013 dans le cadre de la « Cohorte FCCSS » coordonnée par l'INSERM[8], après un examen approfondi des mesures de sécurité mises en œuvre (chiffrement et/ou codage des données, accès sélectif en fonction des habilitations de chacun, recours à un tiers de confiance, etc.).

La modernisation des systèmes d'information de santé et l'élévation du niveau de sécurité

Le cadre technique et institutionnel de la *e-santé* a connu d'importantes évolutions depuis 2007, dans le sens d'un renforcement de la sécurité des systèmes d'information et, notamment, de la protection de la confidentialité des données personnelles.

Ainsi, la création de l'Agence des Systèmes d'information partagée de santé (ASIP Santé) en 2009 répond à l'objectif de créer et de mettre en œuvre les conditions favorables au déploiement de systèmes d'information partagés de santé, en cohérence avec un cadre national respectueux des exigences de sécurité.

Les établissements de santé ont l'obligation de respecter un ensemble de référentiels de sécurité et de confidentialité lorsqu'ils hébergent leur propre système d'information.

La Commission n'a toujours pas été saisie officiellement de l'arrêté qui doit définir les référentiels imposés par le décret « confidentialité » du 15 mai 2007[9]. Ce décret doit, toutefois, être aujourd'hui interprété à l'aune des dispositions de la loi « Hôpital Patient Santé Territoires »[10] et des référentiels de sécurité déjà définis par l'Agence des systèmes d'information partagés (ASIP Santé).

De même, la loi n°2002-303 du 4 mars 2002 relative aux droits des malades, complétée par le décret du n° 2006-6 du 4 janvier 2006, n'autorise l'externalisation des données de santé auprès d'un organisme distinct du professionnel ou de l'établissement de santé qui soigne le malade qu'à la condition que l'hébergeur soit préalablement agréé. La CNIL a, ainsi, examiné 142 dossiers de candidature depuis 2009, effectué de nombreux contrôles dans ce domaine depuis 2010 et 64 agréments ont, à ce jour, été délivrés.

La CNIL travaille également, en concertation avec les pouvoirs publics et l'ensemble des acteurs concernés, à l'élaboration d'une politique générale de sécurité des systèmes d'information de santé (PGSSI-S) qui conduira à une amélioration progressive de la sécurité dans l'ensemble des systèmes d'information de santé, ainsi qu'à une modification du régime juridique actuel. D'autres référentiels sont en cours d'élaboration dans le cadre de groupes de travail auxquels la CNIL participe activement. À terme, un ensemble de référentiels permettra à tout professionnel et organisme de santé de se mettre en conformité avec un niveau d'exigence défini.

Dans ces conditions, les renforcements de la sécurité informatique pourraient rendre le risque de croisements illicites de données à partir du NIR inférieur aux risques sanitaires que ferait courir aux patients un identifiant national mal maîtrisé. ■

[4] Délibération n°95-036 du 21 mars 1995 portant avis sur la gestion informatisée de la nouvelle campagne de dépistage de masse du cancer colorectal dans le département du Calvados. / [5] Décret n° 2004-1489 du 30 décembre 2004. / [6] Délibération n° 2012-260 du 19 juillet 2012 portant avis sur un projet de décret en Conseil d'État relatif à la mise en œuvre d'un traitement de données à caractère personnel dans le cadre d'une recherche en santé humaine dénommée « Nutrinet-Santé ». [7] Délibération n° 2013-040 du 14 février 2013 portant avis sur un projet de décret en Conseil d'État portant création d'un traitement de données à caractère personnel dénommé « Esteban ». / [8] Délibération n° 2013-221 du 18 juillet 2013 portant avis sur un projet de décret en Conseil d'État portant création d'un traitement de données à caractère personnel dénommé « Étude du devenir global à long terme des survivants d'une tumeur solide de l'enfant diagnostiquée avant 2000 en France (FCCSS) ». [9] Délibération n° 2007-960 du 15 mai 2007 relatif à la confidentialité des données médicales. / [10] L. n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

VERS UNE ÉVOLUTION POSSIBLE DE LA POSITION DE LA CNIL MOYENNANT UN CANTONNEMENT DU NIR À LA SPHÈRE « MÉDICO-SOCIALE »

Compte tenu de l'ensemble de ces éléments et sans préjuger de l'avis qu'elle rendra sur le projet de décret dont elle sera saisie, la CNIL s'est montrée ouverte à une évolution de sa position sur la question de l'utilisation du NIR dans la sphère de la santé où il s'est progressivement répandu.

Toutefois, les spécificités du NIR, et notamment son caractère signifiant, justifient que le recours à cet identifiant reste strictement encadré par la loi du 6 janvier 1978 modifiée et cantonné aux finalités pour lesquelles son utilisation est permise.

Le NIR ayant été utilisé dès l'origine dans le secteur de la sécurité sociale[11], la CNIL a admis qu'il soit enregistré dans l'ensemble des fichiers des organismes en relation avec ce secteur, dont le cercle s'est élargi sous l'effet des lois sociales successives (employeurs, Pôle Emploi, organismes d'assurance maladie obligatoires et complémentaires, professionnels et établissements de santé, etc.). Cependant, les décrets intervenus pour autoriser de telles utilisations ont veillé à ce que leur objet demeure cantonné aux relations avec les organismes de sécurité sociale.

En revanche, dans les autres domaines, les administrations ont dû se doter d'identifiants spécifiques.

La CNIL a ainsi obtenu que l'éducation nationale, qui avait recours au NIR, y substitue en 1992 un identifiant spécifique (le NUMEN)[12]. De même, la Direction Générale des Impôts (DGI) a renoncé à utiliser le NIR comme identifiant fiscal et a utilisé à cette fin un numéro spécifique (le SPI). Elle n'est fondée à utiliser le NIR que comme instrument de fiabilisation du SPI et dans les échanges entre l'administration des finances et d'autres entités autorisées, quant à elles à utiliser le NIR.

La CNIL a enfin manifesté son opposition au recours au NIR comme identifiant pour la création d'un registre national des crédits aux particuliers, également appelé « fichier positif »[13], en rappelant la nécessité du recours à des identifiants sectoriels dans le cadre des téléservices de l'administration électronique[14].

Lors de la séance plénière du 15 octobre 2013, la Commission a considéré que le NIR pourrait être utilisé comme identifiant du dossier médical, à la condition que des garanties très strictes soient mises en place sous son contrôle pour en circonscrire l'utilisation à la seule nouvelle finalité ainsi définie.

Un tel élargissement aurait pour conséquence que le NIR resterait strictement cantonné à la sphère « médico-sociale », moyennant une étanchéité renforcée avec les autres secteurs.

Cette position suppose, au préalable, qu'une évaluation rigoureuse soit effectuée, en lien avec l'INSEE, pour s'assurer que le NIR présente bien les qualités requises pour constituer un identifiant national de santé efficace. En effet, les cartes Vitale ne comportent pas, à ce jour, les NIR des mineurs de moins de 16 ans. En outre, se pose la question de l'unicité du NIR, compte tenu de l'élévation de l'espérance de vie.

Cette solution suppose également qu'une évaluation soit effectuée de la possibilité de cantonner l'usage du NIR à la sphère médico-sociale, compte tenu des utilisations déjà admises dans d'autres secteurs.

L'ensemble de ces travaux permettront à la Commission de se prononcer utilement quand elle sera saisie du projet de décret fixant la nature de l'INS. Il lui appartiendra de prévoir toutes les garanties nécessaires pour assurer le respect de la loi du 6 janvier 1978 et la protection des données personnelles de santé des citoyens. Le défi est de parvenir au développement de systèmes d'information de santé qui présentent un niveau de sécurité maximal, sans pour autant paralyser la production et la qualité des soins. ■

> Le NIR resterait strictement cantonné à la sphère « médico-sociale », moyennant une étanchéité renforcée avec les autres secteurs.

[11] *Recommandation du 29 novembre 1983 aux termes de laquelle la CNIL reconnaît le principe que les* « fichiers de sécurité sociale étaient appelés, de par leur essence même, à utiliser le NIR comme identifiant ». / [12] *Délibération n° 92-063 du 23 juin 1992 relative à un projet d'arrêté présenté par le ministre de l'Éducation nationale concernant un traitement de préliquidation de la paie et de gestion des emplois, des postes et de personnels de l'enseignement de second degré (E.P.P.).*

[13] *Délibération n° 2013-088 du 11 avril 2013 portant avis sur un projet de loi instaurant un registre national de crédits aux particuliers.* / [14] *Délibération n° 2013-054 du 7 mars 2013 portant avis sur un projet d'arrêté autorisant la mise en œuvre, par les collectivités locales, les établissements publics de coopération intercommunale, les syndicats mixtes et les établissements publics locaux qui leur sont rattachés ainsi que les groupements d'intérêt public et les sociétés publiques locales dont ils sont membres, de traitements automatisés de données à caractère personnel ayant pour objet la mise à disposition des usagers d'un ou plusieurs téléservices de l'administration électronique.*

LES DONNÉES PERSONNELLES À L'HEURE DU NUMÉRIQUE

DROIT À L'EFFACEMENT OU DROIT À L'OUBLI ?

Le développement des réseaux sociaux témoigne d'une propension croissante des individus à partager des informations et donc à exposer leur vie privée. Il révèle aussi plus simplement le désir d'avoir une vie publique, de partager ses idées, ses passions et certains événements de sa vie. Toutefois, la circulation d'informations concernant une personne peut avoir de graves conséquences sur sa vie privée et professionnelle, parfois plusieurs années après les faits (stigmatisation sociale, difficulté de retour à l'emploi, etc.).

Grâce notamment à l'action menée depuis plusieurs années par la CNIL, une majorité d'internautes a pris conscience de la nécessité de protéger ses données personnelles, d'en encadrer la diffusion sur Internet et ainsi de soigner sa réputation numérique. Lorsque les personnes ne parviennent pas à obtenir la suppression des informations qui les concernent auprès des éditeurs de sites Internet ou des moteurs de recherche, elles recourent ainsi de plus en plus souvent aux services de la CNIL qui reçoit tous les ans environ 1 000 plaintes liées à ces problématiques (suppression de textes, photographies ou vidéos en ligne).

Réaffirmée par les nouveaux usages du monde numérique et des réseaux, la question de l'oubli dans le monde numérique est aussi ancienne que la loi « Informatique et Libertés ». Dès sa création, la CNIL a abordé la question du droit à l'oubli dans la plupart de ses rapports annuels. Dans son 19ème rapport d'activité de 1998, la Commission précisait, par exemple, que « *jusqu'à l'informatisation d'une société, l'oubli était une contrainte de la mémoire humaine. Avec l'informatisation, l'oubli relève désormais du seul choix social. Le "droit à l'oubli" n'est pas nouveau ; il n'est pas né avec la loi du 6 janvier 1978, qui d'ailleurs ne le consacre pas, même s'il inspire toute notre législation. Ce droit est né avec l'idée même d'équilibre. C'est cet équilibre qu'une démocratie doit sans cesse rechercher* ».

Le droit à l'oubli résulte de l'application combinée de plusieurs principes de la loi « Informatique et Libertés »[1] et de la convention 108 du Conseil de l'Europe du 28 janvier 1981. Au-delà des principes de finalité, de loyauté, d'exactitude et de mise à jour des données, il s'agit de l'obligation de définir et de respecter des durées de conservation conformes à la finalité poursuivie et de prendre en compte les demandes de droit d'opposition.

La CNIL a décliné le concept de droit à l'oubli ainsi entendu dans un certain nombre de domaines, notamment à l'égard des fichiers liés à la santé, à l'éducation et, bien sûr, des fichiers de police. À partir de 1998 et de la généralisation de l'utilisation d'Internet, elle s'est évidemment préoccupée des conséquences pouvant résulter des possibilités offertes par les moteurs de recherche. Dès 2001, elle adoptait ainsi une recommandation relative à l'anonymisation des données de jurisprudence diffusées sur Internet[2].

Le droit à l'oubli numérique sur Internet serait donc la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie en ligne, qu'elle soit privée ou publique. Nécessité humaine et sociétale, ce droit ne doit cependant pas être interprété comme un impératif absolu d'effacement des données et informations. En effet, il est nécessaire de trouver un équilibre entre le droit à l'oubli d'une part, et la liberté d'expression, le devoir de mémoire ou encore la constitution de preuves d'autre part.

De surcroît, le caractère transnational du réseau Internet révèle une certaine difficulté de maîtrise des informations publiées et de l'application du droit des internautes. Il apparaît alors essentiel que les autorités de protection des données, en concertation avec les professionnels, les acteurs de la société civile et les citoyens, agissent pour que le droit à l'oubli numérique puisse être effectif.

Pistes de réflexion avancées par la Commission

Des pistes de solutions juridiques et techniques innovantes ont été soumises à consultation publique par la Commission. Si elles ne sont pas toutes généralisables, elles présentent une gamme d'outils susceptibles d'offrir aux

Le droit à l'oubli numérique sur Internet serait donc la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie en ligne.

[1] *Dans sa rédaction initiale comme dans celle issue de la transposition de la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles.*
[2] *http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653503&fastReqId=901231488&fastPos=1*

personnes concernées des moyens efficaces de maîtriser la diffusion de leurs données personnelles.

L'élaboration d'un référentiel standard

La CNIL suggère une réflexion au niveau européen pour définir un référentiel standard de durées de conservation des données. L'idée serait de mettre à disposition des responsables de traitement un guide de référence, leur permettant de savoir combien de temps ils peuvent conserver des données à caractère personnel pour une finalité déterminée. Un tel document permettrait également d'harmoniser les durées de conservation des données contenues dans des traitements similaires.

Une meilleure maîtrise de la publication des données

Une autre piste de réflexion est de mettre à disposition des outils offrant aux internautes de mieux maîtriser la publication de leurs données, par exemple : des outils permettant aux auteurs de définir une date limite de diffusion de leurs publications ou de les modifier et de les supprimer. Toutefois, en l'absence de dispositif de restriction d'accès (accès restreint par identification, partage limité sur un réseau social, etc.), toute publication sur Internet est accessible à tous et à tout moment. Il est alors nécessaire de responsabiliser les internautes sur la portée de leurs publications et la possible difficulté de leur effacement intégral.

Améliorer les systèmes de référencement

Tout internaute peut effectuer une simple recherche à partir des nom et prénom d'une personne sur un moteur de recherche, révélant parfois des informations personnelles à son sujet. Ainsi, il est possible d'identifier des particuliers à partir d'informations relatives à leur parcours personnel rendues publiques (inscription sur un site de rencontre, mariage, médaille décernée, condamnation pénale, décès, etc.). De même, les recruteurs n'hésitent pas à utiliser les moteurs de recherche pour recueillir toute information référencée sur les candidats à l'embauche, ce qui peut influencer les chances de recrutement et de réinsertion sociale. Cette problématique est abordée à travers la charte du recrutement invitant les professionnels recruteurs à respecter l'éthique professionnelle qui consiste à ne prendre en compte que les seules compétences des candidats.

Pour cette raison, l'effectivité du droit à l'oubli pourrait donc être complétée par une obligation juridique de déréférencement sans délai à la charge des moteurs de recherche, dès lors que l'internaute a obtenu l'effacement de l'information initiale.

Une consultation publique à destination des internautes et des professionnels

Afin de développer des solutions pratiques et pragmatiques, la CNIL a lancé de mai à octobre 2013 des consultations publiques en ligne auprès des particuliers et des professionnels. Il s'agissait de recueillir l'avis des internautes et les observations des professionnels sur les pistes de réflexion avancées par la Commission dans le domaine du droit à l'oubli.

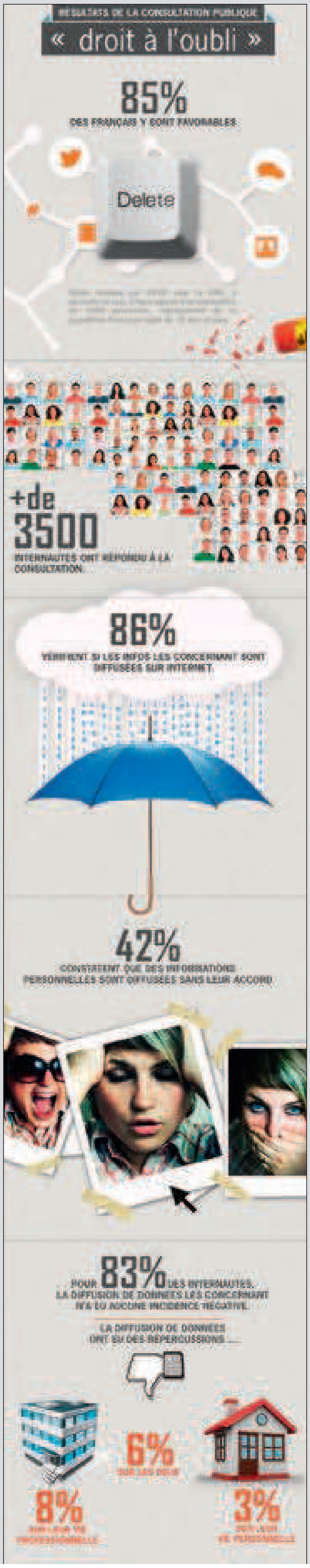
Le point de vue des internautes

Cette consultation a permis de recueillir l'avis de plus de 3500 internautes sur leur perception du droit à l'oubli, leurs attentes, leurs craintes et les problèmes éventuellement rencontrés. Il ressort notamment que :

• 86 % vérifient si des informations les concernant sont diffusées sur Internet ;
• 42 % constatent que des informations personnelles sont diffusées sans leur accord ;
• 17 % considèrent que la diffusion des données les concernant a eu une incidence négative sur leur vie professionnelle ou personnelle.

Pour obtenir la suppression des informations, 90 % des personnes contactent directement la personne ou le site Web à l'origine de la publication. Pourtant, cette démarche a semblé difficile à une grande majorité d'entre eux et moins de 70 % parviennent à faire disparaître ces informations.

Les internautes recherchent ainsi, avant tout, la maîtrise de leur identité numérique. Ils plébiscitent les mécanismes qui permettraient :
• d'obtenir sans délai la possibilité de déréférencement d'une information supprimée du site d'origine ;
• de pouvoir fixer des « dates de péremption » sur leurs propres publications ;



• de choisir d'indexer ou non dans les moteurs de recherche les informations qu'ils publient.

Le point de vue des professionnels

Les professionnels soulignent le nécessaire respect de la liberté d'expression, du droit de la presse, du droit des archives, de la liberté d'entreprendre et du devoir de mémoire. Une très large majorité des acteurs consultés considère que le terme de « droit à l'effacement » est préférable à celui de « droit à l'oubli ». Leur souhait est de ne pas induire les personnes en erreur sur l'étendue des droits dont ils disposent et sur l'efficacité de la maîtrise de leurs données.

Certains acteurs soulignent la nécessité de faire une distinction en fonction de la nature des données (par exemple, des messages dans un forum de discussion ou un débat public) et de l'auteur de la publication (la personne concernée ou un tiers), afin de ne pas consacrer un droit à la censure.

Certains professionnels ont pointé d'une part, les difficultés dans l'élaboration d'un référentiel de durée de conservation des données au regard des spécificités de chaque secteur et d'autre part, la nécessaire réflexion au niveau mondial et non uniquement européen. Si en grande majorité les professionnels et associations de consommateurs consultés ont souligné l'intérêt d'outils permettant aux internautes de mieux maîtriser leurs publications, ils ont aussi identifié les risques de leur déresponsabilisation.

Enfin, concernant la possibilité d'agir auprès de l'hébergeur du site, la très grande majorité des professionnels interrogés considère qu'il revenait aux tribunaux, et non aux hébergeurs, de se prononcer sur la publication et la diffusion d'une telle information.

L'ensemble des organismes consultés sur le droit à l'oubli numérique s'accorde sur la nécessité d'éduquer, d'informer et de former les utilisateurs, en amont de leurs usages.

En effet, la première des protections reste la vigilance individuelle. C'est pourquoi la CNIL propose depuis plusieurs années, des outils pédagogiques et des bonnes pratiques pour mieux gérer sa vie en ligne et ses traces. La CNIL poursuit sa réflexion sur le sujet en vue d'élaborer des propositions concrètes pour l'ensemble des acteurs en 2014. ■

LA RECOMMANDATION SUR LES COOKIES DE DÉCEMBRE 2013

Rappel du cadre légal

Le développement considérable des services en ligne et des applications sur téléphone mobile s'est accompagné du profilage des personnes qui y ont recours. En effet, lorsqu'ils naviguent sur Internet ou accèdent à des services depuis leurs mobiles, les utilisateurs sont suivis par une multitude d'acteurs. Il peut s'agir d'éditeurs de service, de régies publicitaires, de réseaux sociaux qui analysent leur navigation, leurs déplacements ou leurs habitudes. Le but est notamment de leur proposer des publicités ciblées ou des services personnalisés.

Afin que ce profilage ne soit pas réalisé à l'insu des personnes concernées, le législateur européen a modifié la directive 2002/58/CE par l'adoption de la directive 2009/136/CE, dans le cadre de la modification du « paquet télécom ». Désormais, le stockage d'informations sur l'équipement d'un utilisateur ou l'accès à des informations déjà stockées, ne doit être mis en œuvre qu'avec le consentement préalable de l'utilisateur, sauf si ces actions visent exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques ou si elles sont strictement nécessaires au fournisseur pour la délivrance du service expressément demandé par l'abonné ou l'utilisateur. Ce principe a été transposé en droit français par l'ordonnance n° 2011-1012 du 24 août 2011, qui a modifié l'article 32-II de la loi du 6 janvier 1978.

Afin de déterminer les modalités pratiques permettant aux internautes d'exercer leur choix et compte tenu de la diversité des technologies utilisées et du nombre d'acteurs en présence, la CNIL a organisé une concertation avec les principaux professionnels concernés pendant plusieurs mois. Le but a été de trouver une solution pragmatique pour concilier nécessités économiques, complexité technique, expérience utilisateur et garantie des droits.

Soucieuse d'accompagner au mieux les professionnels, la CNIL a mis à leur disposition une panoplie d'outils pour leur permettre de se mettre en conformité : une recommandation, des fiches pratiques et du code informatique. Elle a également souhaité proposer des outils à destination des citoyens pour qu'ils puissent mieux comprendre l'utilisation qui est faite de leurs données personnelles (vidéo pédagogique et outil de visualisation CookieViz).

Une recommandation ayant vocation à s'inscrire dans le temps

En pratique, l'éditeur d'un service qui utilise des traceurs devra préalablement obtenir le consentement des utilisateurs. Les traceurs, principalement ceux liés aux opérations relatives à la publicité ciblée, ceux permettant d'effectuer de la mesure d'audience (sauf exception limitative) et ceux liés aux « boutons de partage des réseaux sociaux », nécessitent un consentement préalable.

> Un consentement nécessaire quelle que soit la technologie de traçage utilisée (utilisation de cookies ou de la technologie de fingerprinting par exemple) et quel que soit le terminal utilisé (ordinateur, smartphone, télévision connectée, console de jeu connectée...).

À cet égard, comme la recommandation adoptée par la CNIL a vocation à s'inscrire dans le temps, il est nécessaire de poser des principes sans nécessairement viser une technologie particulière. C'est la raison pour laquelle la recommandation couvre toute lecture ou écriture d'information dans un terminal, sans considération des procédés techniques utilisés.

Concrètement, la recommandation concerne les cookies mais aussi des technologies telles que les *local shared objects* (appelés parfois les cookies « flash »), les pixels invisibles et l'identification par calcul d'empreinte du terminal (technologie de *fingerprinting*). En outre, les principes contenus dans la recommandation s'appliquent aussi bien aux cookies déposés et lus, lors de la consultation d'un site Internet, que lors de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile, quels que soient le système d'exploitation, le navigateur ou le terminal utilisés (par exemple un ordinateur, une tablette, un « smartphone », une télévision connectée, une console de jeux vidéos connectée au réseau Internet). Le traçage multi-terminal, qui tend à se développer, est également visé par la recommandation.

Il existe cependant des cookies nécessaires à la fourniture du service demandé par l'utilisateur. Pour ces usages précis, il est donc possible de lire ou d'écrire des informations dans le terminal de l'utilisateur sans recueillir le consentement des personnes. Il s'agit principalement de ceux nécessaires à la fourniture d'un service expressément demandé par l'utilisateur (panier d'achat, session, langue) et de ceux permettant d'effectuer de la mesure d'audience mais uniquement dans certaines conditions spécifiques.

> Pas de dépôt et de lecture de traceurs avant d'avoir recueilli le consentement.

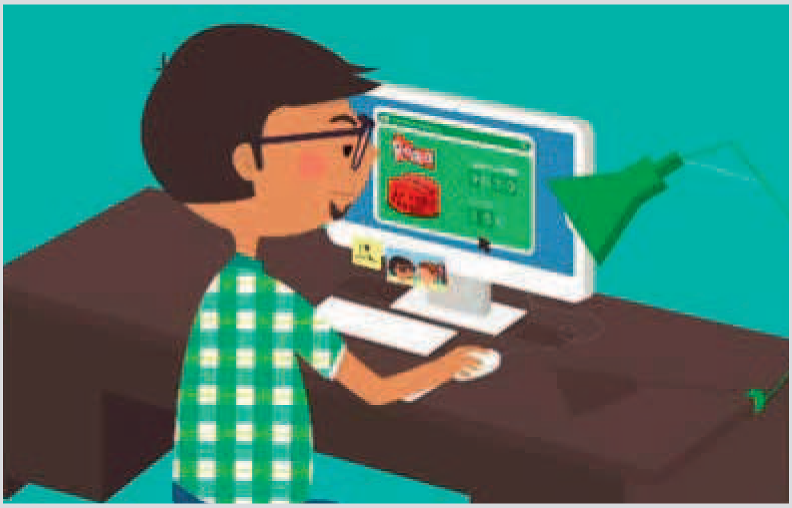
Un consentement permettant d'exercer un choix, informé et résultant d'une action positive

Le consentement ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix. L'utilisateur ne doit donc pas être exposé à des conséquences négatives importantes s'il refuse de donner son consentement. En pratique, la personne qui refuse d'être tracée doit pouvoir continuer à bénéficier du service (accès à un site Internet par exemple). Cette interprétation est d'ailleurs partagée par le G29, le groupe des autorités de protection des données européennes.

Pour qu'il soit éclairé, le consentement de l'utilisateur ne peut se faire sans une information préalable. Le renforcement de l'information des utilisateurs quant à l'utilisation de traceurs est donc un point essentiel de la recommandation.

En outre, le consentement doit se manifester par le biais d'une action positive de la personne préalablement informée des conséquences de son choix et disposant des moyens de l'exercer. L'acceptation de conditions générales d'utilisation ne peut donc être une modalité valable de recueil du consentement.

Vidéo pédagogique expliquant le fonctionnement des cookies



Une recommandation détaillant des modalités pratiques

Afin de déterminer les modalités pratiques permettant aux internautes d'exercer leur choix, une procédure de recueil du consentement en deux étapes a été proposée.

Dans la première étape, l'internaute qui se rend sur le site d'un éditeur doit être informé, par l'apparition d'un bandeau :
- des finalités précises des cookies utilisés ;
- de la possibilité de s'opposer à ces traceurs et de changer les paramètres en cliquant sur un lien présent dans le bandeau ;
- du fait que la poursuite de sa navigation vaut accord à l'utilisation des traceurs.

Ce bandeau ne doit pas disparaître tant que la personne n'a pas poursuivi sa navigation, c'est-à-dire tant qu'elle ne s'est pas rendue sur une autre page du site ou n'a pas cliqué sur un élément du site (image, lien, bouton « rechercher »).

Sauf consentement préalable de l'internaute, le dépôt et la lecture de cookies ne doivent donc pas être effectués :
- si l'internaute se rend sur le site (page d'accueil ou directement sur une autre page du site à partir d'un moteur de recherche par exemple) et ne poursuit pas sa navigation ;
- s'il clique sur le lien présent dans le bandeau lui permettant de paramétrer les cookies et, le cas échéant, refuse le dépôt de cookies.

Dans la seconde étape, indissociable de la première, les personnes doivent être informées de manière simple et intelligible des solutions mises à leur disposition pour accepter ou refuser tout ou partie des cookies nécessitant un recueil du consentement :

▸▸▸

- pour l'ensemble des technologies visées par l'article 32-II de la loi « Informatique et Libertés » ;
- par catégories de finalités : notamment la publicité, les boutons des réseaux sociaux et la mesure d'audience.

Enfin, les personnes ayant donné leur consentement au dépôt ou la lecture de certains cookies doivent être en mesure de le retirer à tout moment.

Une responsabilité partagée

Lorsque plusieurs acteurs interviennent dans le dépôt et la lecture de cookies (par exemple lorsque les éditeurs facilitent le dépôt de cookies qui sont ensuite lus par des régies publicitaires), chacun d'entre eux doit être considéré comme coresponsable des obligations découlant des dispositions de l'article 32-II précité. C'est le cas pour les éditeurs de sites Internet (ou des éditeurs d'application mobile par exemple) et de leurs partenaires (régies publicitaires, réseaux sociaux, éditeurs de solutions de mesure d'audience, etc.).

Les éditeurs de sites web et d'applications mobiles sont en contact direct avec les utilisateurs, contrairement aux acteurs tiers tels que les régies publicitaires. Ils sont mieux positionnés pour informer les utilisateurs et obtenir leur consentement avant l'utilisation de technologies de traçage. Néanmoins, cette obligation incombe également à leurs partenaires qui utilisent pour leur propre compte les données collectées par l'intermédiaire des cookies, en cas de défaut des éditeurs.

Le nécessaire respect des autres dispositions de la loi « Informatique et Libertés »

L'ensemble des dispositions de la loi du 6 janvier 1978 modifiée s'applique également lorsque des données à caractère personnel sont traitées, qu'elles soient directement identifiantes (par exemple, une adresse électronique) ou indirectement identifiantes (par exemple, l'identifiant unique d'un cookie, une adresse IP, un identifiant du terminal ou d'un composant du terminal de l'utilisateur, le résultat du calcul d'empreinte dans le cas du « fingerprinting » ou encore l'identifiant généré par un logiciel ou un système d'exploitation).

Des fiches pratiques et du code source mis à disposition des professionnels

Certains acteurs avaient commencé à informer les utilisateurs qu'ils déposaient des cookies à l'aide de bandeaux d'information. Cette information pouvait représenter une avancée en termes de transparence, mais elle ne permettait pas toujours aux utilisateurs de prendre la mesure du traçage sur Internet et d'exercer un réel choix en toute connaissance de cause.

De surcroît, l'apparition de ces bandeaux était souvent concomitante au dépôt de cookies.

Afin d'accompagner tous les professionnels, qu'il s'agisse de start-ups ou de multinationales, en plus de sa recommandation, la CNIL a mis à disposition sur son site web différents outils.

Il s'agit de fiches pratiques mais aussi de code source à ajouter dans les pages web, pour permettre au site de respecter les exigences de la loi.

Les fiches pratiques sont à destination de différents publics. Ainsi, tant les professionnels du droit, les webmasters et les directions informatiques trouveront des réponses adaptées à leurs questions.

Le code source mis à disposition gratuitement peut être inclus très facilement par les éditeurs dans leurs sites Internet afin de respecter les obligations légales et de renforcer la confiance des visiteurs, en les informant, en recueillant leur consentement et en conditionnant le dépôt de cookies au recueil du consentement.

Ces outils de conformité couvrent diverses technologies, qu'il s'agisse de solutions de mesure d'audience, des boutons sociaux ou de la publicité.

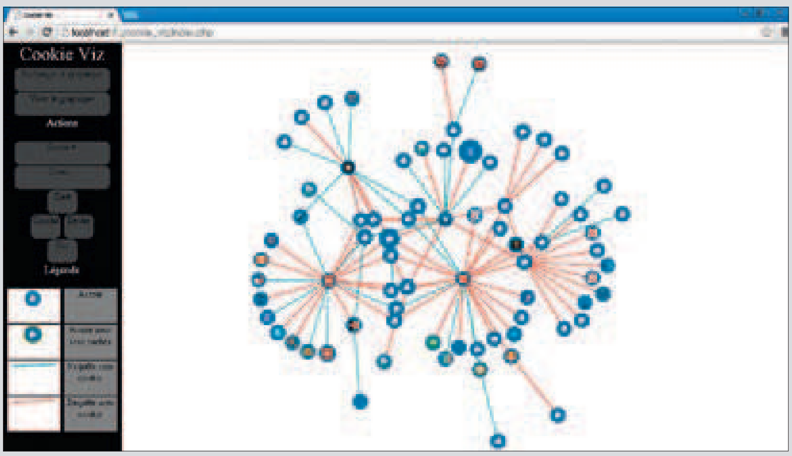
Des conseils pour les internautes

Afin de permettre aux internautes de mieux comprendre ce que sont les cookies et pourquoi ils sont utilisés, la CNIL a publié une vidéo pédagogique expliquant leur fonctionnement. La vidéo présente par exemple les mécanismes qui sont utilisés pour offrir de la publicité ciblée en fonction des navigations précédentes.

La CNIL a aussi développé un outil nommé CookieViz qui peut être téléchargé. Cet outil permet de découvrir la face cachée du fonctionnement d'un navigateur et des interactions entre acteurs d'Internet. Cet outil est mis à disposition dans un but pédagogique pour faire prendre conscience aux utilisateurs de l'ampleur du phénomène que représente l'usage des cookies lors de la navigation. CookieViz est un outil « opensource », cela signifie que le code de l'application est librement accessible et peut être modifié ou enrichi par toute personne qui souhaiterait contribuer.

L'outil CookieViz, développé par la CNIL, sera amené à évoluer durant l'année 2014. Parmi les pistes d'amélioration possibles, la CNIL envisage de mettre à disposition une version en anglais, de faire des versions pour Mac et Linux, et de permettre aux utilisateurs de contrôler l'usage des cookies directement par l'intermédiaire de cet outil. ■

Capture d'écran de l'outil CookieViz



L'APPLICATION EXTRATERRITORIALE DES LOIS DES ÉTATS TIERS ET LA PROTECTION DES DONNÉES PERSONNELLES : ENJEUX ET PERSPECTIVES

Plusieurs gouvernements dans le monde se sont dotés de législations de portée extraterritoriale visant à permettre à leurs services d'accéder à des informations et données personnelles à des fins administratives diverses. Toutefois, l'application de ces lois peut entrer en conflit avec les règles de protection des données personnelles en vigueur en France et dans l'Union européenne. Les conditions d'accès d'autorités publiques étrangères aux données personnelles de citoyens européens soulèvent ainsi des questions majeures, notamment dans un contexte marqué par le développement du *Cloud computing* et, plus généralement, la délocalisation du stockage des données.

Confrontée à l'émergence de ces questions, la CNIL a, dès le début de l'année 2013, constitué un groupe de travail pour se pencher sur les implications des législations étrangères autorisant les autorités de ces pays tiers à collecter ou à accéder à des données personnelles de citoyens français.

La CNIL a ainsi examiné plus précisément certaines lois créant et imposant aux administrations et aux entreprises l'obligation de vérifier la non-inscription de leurs salariés, fournisseurs ou sous-traitants sur des « listes noires » aux finalités diverses. Les révélations de M. Snowden au cours de l'été 2013 ont confirmé l'intérêt de ces travaux, qui ont donné lieu à des réflexions communes dans le cadre du G29.

LES LISTES NOIRES

Depuis plusieurs années certains États, comme les États-Unis, cherchent à se prémunir contre divers risques (par exemple en matière de lutte contre le financement du terrorisme et d'exportations stratégiquement sensibles) au moyen de législations prévoyant des sanctions d'exclusion commerciale ou encore certaines restrictions.

La gestion de ces risques a donné lieu à la création et à l'utilisation de listes noires internationales ou nationales désignant certains États, personnes physiques ou morales, organismes ou groupes d'entreprises comme devant faire l'objet d'une sanction d'interdiction (par exemple, de commercer) ou comme devant faire l'objet d'une attention particulière. Ces législations imposent souvent que chaque opération impliquant directement ou indirectement ces pays, personnes, organismes ou groupes soit contrôlée.

Une application extraterritoriale à articuler avec la protection des données personnelles des citoyens européens

Dans un contexte de mondialisation des activités, les lois d'un pays établissant une liste noire des sociétés ou des États avec lesquelles cet État s'interdit et interdit à ses entreprises de commercialiser, sont de plus en plus souvent susceptibles d'avoir des conséquences sur d'autres pays. En effet, ces lois peuvent en pratique donner lieu à une application extraterritoriale étendue.

La CNIL est parfaitement consciente de la nécessité de lutter contre certains dangers et menaces graves en se dotant d'outils permettant de les contrer (en particulier, par exemple, dans le domaine de la lutte contre le finance- ▸▸▸

ment du terrorisme). Néanmoins, elle souligne que la portée extraterritoriale potentielle de certaines listes noires soulève plusieurs difficultés quant à leur compatibilité avec la législation de protection des données de la France et de l'Union européenne.

Effet extraterritorial indirect d'une décision interne à une entreprise multinationale

Ainsi, dans le cadre d'une entreprise multinationale et par souci de se conformer aux exigences de son droit national, un siège situé en dehors de l'Union européenne peut être amené à imposer à l'ensemble de ses filiales dans le monde l'obligation d'appliquer les procédures de vérifications auquel il est tenu (souvent sous peine d'amende administrative).

Ce type de décision interne prise par la maison-mère d'un groupe peut conférer, pour certaines listes, un caractère extraterritorial par ricochet à l'application de règles définies au niveau national, plaçant ainsi les filiales européennes en situation délicate vis-à-vis de la législation de protection des données.

Amalgame de finalités différentes par l'agrégation de listes noires

La multiplicité et la diversité des listes noires entraînent également une complexification des exigences de conformité pour les entreprises et ont par conséquent généré une offre de services ciblée par des prestataires spécialisés. Face à l'obligation de vérifier de nombreuses listes régulièrement mises à jour, les entreprises peuvent ainsi opter pour des services proposés par des tiers prestataires.

Il s'agit de logiciels de vérification utilisant des listes agrégées, issues de la fusion de plusieurs, voire de la totalité des listes d'exclusion existantes. Or, chaque liste poursuit un objectif distinct (lutte contre le financement du terrorisme, lutte contre le blanchiment d'argent, prévention de la fraude, blocus d'un pays, protection des exportations stratégiques, etc.).

Collecte en ligne de données personnelles

Des prestataires ou administrations de certains pays proposent aux organismes désireux de procéder à une vérification la saisie en ligne de noms ou de listes de noms directement sur un site Internet, sans préciser ce qu'il advient des données personnelles ainsi collectées, ni de quelle manière celles-ci sont protégées.

Compatibilité des traitements de vérification et des éventuels transferts de données liés aux listes noires avec la loi « Informatique et Libertés »

Les traitements consistant à procéder au rapprochement de données relatives à des personnes physiques (clients, fournisseurs, salariés ou candidats à l'embauche) aux personnes et organismes inscrits sur une liste noire soulèvent plusieurs difficultés, concernant notamment :

- **l'absence de base légale** dans le droit d'un pays membre de l'Union européenne pour l'application à des sociétés européennes de certaines listes noires ;
- **le risque de violation du principe de finalité** par l'utilisation de bases de données compilant plusieurs listes entre elles. En effet, dès lors que les individus et entités fichés sur ces listes ne le sont pas pour les mêmes raisons, l'utilisation de listes agrégées sans tenir compte de leurs finalités spécifiques respectives risque de rendre les traitements de vérification incompatibles avec le principe de finalité des traitements ;
- **le risque de violation du principe de proportionnalité** par la vérification de la situation d'un groupe de personnes trop large (clients, fournisseurs, salariés). À titre d'exemple, la vérification de la situation de l'ensemble des salariés, alors même que la législation nationale n'exigerait la vérification de la situation que des dirigeants et cadres, présenterait indubitablement un caractère disproportionné ;
- **les droits des personnes concernées** (droit à l'information, droits d'accès et de rectification, ainsi que la durée de conservation des données) ne sont pas clairement garantis. Enfin, les éventuels transferts, dans le cadre des procédures de vérification de données vers un pays tiers (et qui plus est à une autorité administrative gouvernementale de ce pays), lorsque ce dernier n'offre pas un niveau de protection adéquat au sens de la législation européenne, soulèvent la question de leur régularité et de leur encadrement.

Les limites des listes noires européennes au regard de la CEDH

En pratique, les modalités mêmes de constitution des listes noires ne sont pas sans poser des difficultés. La diversité des listes (d'origine internationale et nationale) ainsi que leur caractère parfois arbitraire peuvent engendrer des contradictions, des insuffisances, voire des lacunes, récemment pointées par la jurisprudence de la Cour européenne des droits de l'Homme.

Celle-ci, dans un arrêt de grande chambre du 12 septembre 2012[1], a ainsi estimé que les conditions de mise en œuvre par la Suisse des résolutions des Nations unies dans le cadre de la lutte contre le terrorisme violaient les articles 8 (droit au respect de la vie privée et familiale) et 13 (droit à un recours effectif) de la Convention Européenne des droits de l'Homme.En effet, aucune audition ne précédait l'inscription d'une personne sur la liste, et les personnes listées n'étaient pas informées des griefs à leur encontre, alors qu'un simple soupçon de lien avec le terrorisme peut suffire à justifier une telle inscription.

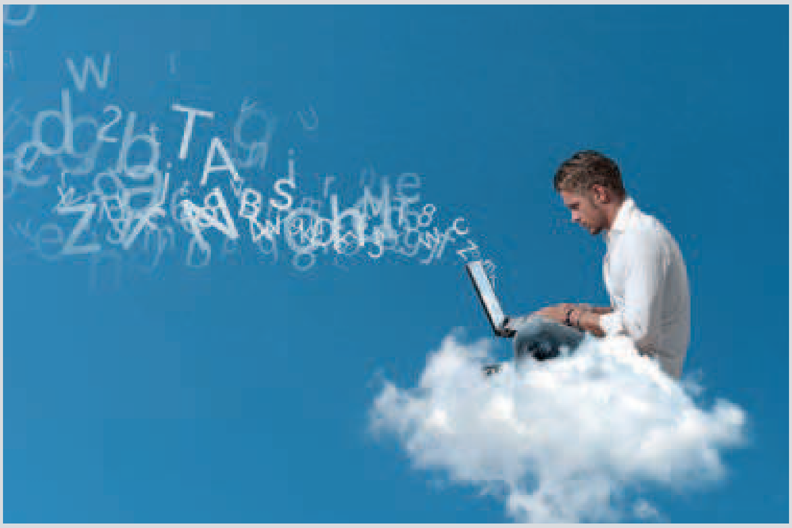
Les pistes de solution

La CNIL poursuit ses travaux sur le thème des listes noires, compte tenu du risque d'éventuelles dérives dans l'utilisation de ces dernières. Sous réserve de l'adoption d'une position définitive, la Commission recommande, dans un premier temps, qu'un certain nombre de précautions minimales soient prises concernant l'utilisation de telles listes.

> L'enjeu est de garantir aux citoyens européens le maintien d'une protection effective de leurs données.

[1] *Voir l'arrêt de la Cour européenne des droits de l'Homme dans l'affaire N. c/. Suisse du 12 septembre 2012 (requête no°10593/08).*

- En premier lieu, les entreprises devraient vérifier si la loi étrangère leur est bel et bien applicable.
- Elles devraient ensuite procéder au travail d'analyse préalable nécessaire à la détermination exacte de la portée des obligations prévues dans les lois étrangères instaurant ces listes noires.
- Par ailleurs, la réalisation des opérations de vérification sur le territoire français, par la société (ou la filiale) elle-même aurait le mérite d'éviter tout transfert de données vers une autorité administrative (ou une société mère) située dans un pays tiers n'offrant pas un niveau de protection adéquat au regard du niveau de protection des données personnelles exigé par l'Union européenne. ■



L'ACCÈS PAR DES AUTORITÉS DE PAYS TIERS AUX DONNÉES PERSONNELLES DES CITOYENS EUROPÉENS

Dans de nombreux domaines, la coopération internationale implique que les autorités administratives des États s'échangent des informations, le plus souvent sur la base du principe de réciprocité et au moyen de conventions bilatérales ou multilatérales. En effet, la résolution du conflit entre ces lois nationales étrangères et les règles de protection des données en vigueur au sein de l'Union européenne ne peut être recherchée que par la négociation d'un accord international.

Un des principaux enjeux pour les États-membres de l'Union européenne, tout comme pour leurs autorités de protection des données, est ici de garantir aux citoyens européens le maintien d'une protection effective de leurs données.

La problématique n'est pas nouvelle pour la CNIL, qui a eu l'occasion dans le passé de se prononcer (ainsi que ses homologues dans le cadre du G29) sur des difficultés similaires d'accès aux données européennes par des autorités étrangères, notamment sur les accords internationaux entre l'Union européenne et les États-Unis en matière de données passagers et de lutte contre le financement du terrorisme (accords dits « PNR » et « TFTP »).

Une illustration : l'accord de coopération entre autorités de supervision de l'activité des commissaires aux comptes

À la suite des scandales financiers ENRON et WORLDCOM, la loi américaine Sarbanes-Oxley (SOX) a réformé de manière radicale les règles applicables, entre autres, au contrôle des comptes des sociétés faisant appel à l'épargne sur les marchés américains.

Au titre de ces nouvelles mesures, les États-Unis ont instauré un nouvel organisme, le *Public Company Accounting Oversight Board* (PCAOB), placé sous l'autorité de la *U.S. Securities and Exchange Commission* (SEC). Il est chargé de la supervision des commissaires aux comptes (ou « auditeurs ») qui certifient les comptes de sociétés cotées sur les marchés aux États-Unis. Sa mission consiste notamment à vérifier que le contrôle des comptes de ces sociétés, tel qu'il est effectué en dehors des États-Unis, est fiable, et par conséquent que la supervision de la profession des commissaires aux comptes dans les pays concernés l'est également.

Pour répondre à cet effet extraterritorial de la loi Sarbanes-Oxley, la France a institué, par une loi n° 2003-706 du 1er août 2003, une autorité publique indépendante intitulée le Haut conseil du commissariat aux comptes (« H3C »), désormais homologue français du PCAOB, et avec lequel celui-ci a vocation à coopérer. Le PCAOB a souhaité pouvoir diligenter des contrôles, menés conjointement avec les autorités nationales compétentes, pour se satisfaire de la manière dont ses homologues travaillent sur le terrain avant que puisse prévaloir une logique de confiance mutuelle et de réciprocité.

À l'occasion de ces contrôles conjoints menés sur le territoire des États concernés, le PCAOB demande à accéder non seulement aux rapports d'audit, mais également à l'ensemble de la documentation ayant servi à l'élaboration de ces rapports. C'est dans ce cadre que des données à caractère personnel sont susceptibles d'être transmises vers les États-Unis d'Amérique.

Le PCAOB étant un organisme américain, pays non adéquat au sens de la Directive 95/46/CE, le H3C a négocié un accord spécifique (adossé à l'accord principal réglant les modalités de coopération entre les deux autorités) et relatif à la protection des données ainsi transférées.

C'est dans ce contexte que la CNIL a pu assister le Haut conseil du commissariat aux comptes français dans la négociation d'un accord bilatéral de ▸▸▸

coopération avec le PCAOB comportant des dispositions encadrant les transferts de données vers les États-Unis.

La CNIL a ainsi autorisé le transfert de données à caractère personnel sur la base de l'insertion dans ces accords d'un certain nombre de **garanties**, telles que :

• **une clause de mise en œuvre** des principes d'anonymisation et de minimisation des données transférées ;

• **l'engagement des parties** à ce que toute transmission de données à caractère personnel respecte les principes de : limitation des finalités (aux seules finalités de supervision en application des dispositions de la loi Sarbanes-Oxley), pertinence et proportionnalité des données, transparence, sécurité et confidentialité, interdiction de transférer des données sensibles sans le consentement préalable des personnes.

En outre, la CNIL a relevé que ces accords comportent des dispositions garantissant aux personnes concernées leur droits d'accès, de rectification, de suppression et d'opposition, leur droit à réparation, ainsi que la limitation du transfert ultérieur des données aux seuls cas prévus par l'accord de coopération.

La révélation de systèmes de surveillance électronique de masse

Il existe dans le monde des pays s'étant dotés de lois à portée extraterritoriale autorisant notamment leurs agences de renseignements à collecter des données personnelles hors de leur territoire national. De telles lois sont susceptibles non seulement d'impacter la protection des données à caractère personnel en France et en Europe, mais aussi de mettre en cause la souveraineté des États, de même que le respect des droits de l'Homme dans les sociétés démocratiques.

Consécutivement aux révélations d'Edward Snowden sur les programmes de surveillance des États-Unis, plusieurs initiatives ont été engagées au niveau des institutions européennes.

Le groupe d'experts Union européenne/ États-Unis

En juillet 2013, un **groupe d'experts Union européenne/ États-Unis**, composé d'experts de la Commission européenne, des États membres et du G29 a été constitué afin d'établir l'exactitude des faits révélés dans la presse début juin 2013.

Le rapport publié par la Commission européenne en novembre 2013 sur les conclusions des travaux de ce groupe d'experts a confirmé l'existence et les principaux éléments de certains aspects des programmes de surveillance, notamment le caractère secret de la procédure devant la Cour sur les renseignements étrangers (FISC). Il constate par ailleurs que la législation américaine est utilisée comme base légale par certaines autorités de ce pays afin de procéder, à des fins de renseignement, à la collecte et au traitement à grande échelle de données relatives à des citoyens étrangers.

Le rapport confirme qu'il existe des différences entre les garanties applicables aux citoyens de l'UE et celles applicables aux citoyens des États-Unis, ces derniers étant les seuls protégés par le 4ème amendement de la Constitution américaine. Par ailleurs, les législations américaines ne permettent pas aux citoyens européens d'exercer leurs droits d'accès, de rectification ou d'avoir accès à des voies de recours judiciaires ou administratives.

En outre, différents niveaux de protection sont appliqués en fonction de la nature des données (données de connexion, données de contenu), tandis que d'autres éléments restent flous tels que, notamment, le nombre de citoyens de l'UE concernés et la portée géographique de ces programmes de surveillance.

L'enquête de la Commission LIBE du Parlement européen

De son côté, la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du **Parlement européen** a ouvert une enquête sur le sujet et plusieurs auditions importantes ont été organisées.

Ces auditions ont notamment porté sur : les travaux du groupe d'experts UE-US, l'applicabilité du droit de l'Union européenne, l'analyse des instruments d'encadrement des transferts de données (*Safe Harbor*, Clauses contractuelles type et *Binding Corporate Rules*), l'efficacité de la surveillance aux fins de lutte contre la criminalité organisée et le terrorisme, les programmes de surveillance dans les États-membres de l'Union européenne, le rôle des parlements dans le contrôle démocratique des agences de renseignement, ainsi que les allégations publiées dans la presse sur le piratage des sociétés SWIFT et Belgacom par des autorités étrangères.

Le projet de rapport du Parlement comporte plusieurs recommandations telles que l'interdiction du traitement massif et indiscriminé de données à caractère personnel, le refus de toute collaboration avec les États qui n'appliqueraient pas cette interdiction, ou le renforcement du contrôle des activités des services de renseignement ainsi que de l'encadrement du *cloud computing*.

Sur la base de ces recommandations, la Commission LIBE propose l'adoption d'un *Habeas Corpus* du numérique dont le Parlement Européen serait le gardien. Il s'articulerait autour de propositions phares, parmi lesquelles figure notamment la conclusion d'un accord-cadre Union Européenne - États-Unis pour les transferts de données sur décision judiciaire, qui garantisse l'existence de recours adéquats aux citoyens européens victimes de surveillance. Son rapport final devrait être adopté au cours de l'année 2014.

Les actions menées par la CNIL

Dès le mois de mars 2013, et avant même la publication des révélations d'Edward Snowden dans la presse, la CNIL a créé un groupe de travail chargé de réfléchir à la question de l'accès par des autorités étrangères aux données des citoyens européens.

Les diverses auditions menées dans le cadre de ce groupe de travail ont notamment permis de mettre en lumière que les sociétés recevant des demandes émanant des autorités américaines fondées sur la législation FISAA[1] sont, de par cette loi, soumises à une obligation de discrétion très stricte leur interdisant de communiquer sur ce sujet.

Par ailleurs, les entreprises semblent avoir bien pris la mesure du risque induit par une exposition juridique aux demandes de communication d'autori-

[1] *Foreign Intelligence and Surveillance Amendments Act.*

tés étrangères. En outre, elles se sont dotées de fonctions dédiées (directeur des interceptions) et mettent en œuvre des procédures internes spécifiques afin de gérer ces demandes.

Il est également ressorti des auditions que la protection offerte par les techniques de chiffrement pour la sécurisation des données est limitée. En effet, certaines techniques de chiffrement auraient été compromises, tandis que les législations de certains pays exigent la remise par les sociétés des clefs de déchiffrement.

La CNIL participe activement aux travaux menés au niveau européen sur les programmes de surveillance électronique de masse. Elle a ainsi reçu ses homologues dès juillet 2013 afin de travailler sur ce sujet. Par ailleurs, la Présidente de la CNIL a été auditionnée en octobre 2013 par la Commission LIBE du Parlement Européen lors des discussions organisées sur la pertinence des outils juridiques d'encadrement des transferts dans l'affaire PRISM.

Ainsi, les analyses de la CNIL concernant ces outils (*Safe Harbor*, Clauses contractuelles type et *Binding Corporate Rules*) contribuent à alimenter les travaux menés par le G29 sur ce sujet.

En premier lieu, il ressort de cette analyse que lorsqu'un transfert ou un transfert ultérieur est effectué vers une agence de renseignement étrangère, il appartient au responsable des données de vérifier que l'ensemble des principes de protection des données est respecté. Cependant, la communication massive de données personnelles à une autorité d'un pays tiers à des fins de surveillance disproportionnée ne peut en aucun cas être considérée comme respectant les principes de la directive 95/46/CE, pas plus que ceux imposés par les outils d'encadrement des transferts. En effet, une telle surveillance serait en contradiction avec le principe de proportionnalité, le principe de transparence ou encore le principe de limitation des finalités.

Si ces outils comportent des clauses prévoyant certaines exceptions aux principes de protection des données, notamment en matière de sécurité nationale, ces dernières doivent nécessairement être interprétées de manière stricte et ne peuvent en tout état de cause, s'appliquer à un nombre illimité de personnes. Une application large de ces exceptions serait ainsi contraire au principe de proportionnalité inscrit notamment à l'article 8 de la Convention européenne des droits de l'Homme.

Par ailleurs, quand bien même le transfert respecterait les principes de protection des données, il n'en demeure pas moins qu'une autorité publique étrangère doit également, en vertu des articles 25 et 26 de la directive, offrir un niveau de protection adéquat. Or, en aucun cas les outils d'encadrement des transferts actuels ne permettent à ces autorités publiques étrangères de garantir un tel niveau de protection.

Par conséquent, l**es outils actuels ne sauraient fournir une base légale suffisante pour justifier un accès à des données personnelles par des agences gouvernementales d'une ampleur équivalente à celle de la surveillance massive** et structurelle révélée par la presse.

Les entreprises doivent, de leur côté, prendre conscience des risques inhérents au transfert de données personnelles en dehors du territoire de l'Union européenne, par exemple lorsqu'elles recourent aux services d'un fournisseur de *cloud computing* disposant de serveurs situés hors Union européenne, et potentiellement exposés à un accès gouvernemental étranger.

La problématique n'est pas uniquement reliée à la protection des données, mais soulève des considérations excédant les limites des pouvoirs des autorités de protection des données nationales. Pour ces raisons, la seule solution envisageable semble la création d'un outil spécifique, prenant la forme d'un accord international propre à garantir que les agences de renseignement du pays tiers offrent un niveau de protection adéquat.

Cependant, en aucun cas, un tel accord intergouvernemental ne pourrait légitimer un programme de surveillance électronique massive tel que Prism, dans les contours qui semblent être les siens compte tenu des informations rendues publiques. Un tel accord devrait en effet être conforme à la Charte des droits fondamentaux de l'Union européenne et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH). Ceci implique notamment que toute atteinte à la vie privée des citoyens doit être strictement et évidemment nécessaire, justifiée par un but légitime et proportionnée.

Par ailleurs, la CNIL soutient la réintroduction dans le texte du projet de Règlement européen sur la protection des données, de l'ancien article 42 figurant dans le projet initial. Ce texte prévoyait en effet que les transferts de données vers des pays tiers à l'Union européenne opérés aux fins de répondre à une demande d'une autorité étrangère ne peuvent avoir lieu qu'avec l'autorisation de l'autorité nationale de protection des données.

Le G29

Le G29 a décidé d'évaluer l'impact exact des différents programmes révélés par Edward Snowden sur la protection de la vie privée et des données des citoyens européens. Il a donc adressé, le 13 août 2013, un courrier à la vice-présidente de la Commission européenne, Mme Viviane Reding, afin que celle-ci demande des clarifications sur la législation américaine en matière de surveillance des citoyens européens. Le G29 a également annoncé que les législations nationales des États membres de l'Union européenne devront faire l'objet d'un examen plus précis.

Un avis du G29 sur ce sujet est en cours de préparation. Il devrait être adopté au cours du premier semestre 2014. ■

LA PROPOSITION DE RÈGLEMENT EUROPÉEN

Présentée par la Commission européenne le 25 janvier 2012, la proposition de règlement de l'Union européenne (UE) sur la protection des données personnelles vise à uniformiser la législation des États membres en l'adaptant au nouveau contexte numérique. Pour être adoptée, dans le cadre de la procédure de codécision, le Parlement européen et le Conseil de l'UE doivent définir leurs positions respectives, négocier un compromis puis ensuite l'approuver définitivement.

LES ENJEUX DE LA RÉFORME

La proposition de règlement a fait en 2013 l'objet de débats intenses, au Parlement européen comme au Conseil de l'UE. Il est vrai que les enjeux sont multiples et importants, pour les citoyens, pour les entreprises comme pour les autorités.

Enjeu technologique. Le cadre normatif existant doit être adapté au nouveau contexte technologique. Les nouvelles technologies et leurs applications, qui sont entrées dans le quotidien des citoyens et développées par des opérateurs mondiaux, ne connaissent plus de frontières physiques. Le futur cadre réglementaire doit assurer une protection efficace du citoyen, tout en ayant la nécessaire flexibilité pour répondre aux évolutions futures.

Enjeu politique. Les révélations, au cours de l'été 2013, sur les programmes de surveillance massive de la NSA, ont provoqué une véritable onde de choc. Il en résulte une tension politique de l'UE avec les États-Unis au sujet de l'utilisation des données des citoyens européens recueillies par les géants américains de l'Internet, cela au moment même où s'engagent les négociations pour un traité de libre-échange transatlantique. Ces révélations ont aussi provoqué une prise de conscience de l'importance de la protection des données par les citoyens et consommateurs, qui appellent à une meilleure protection de leurs données personnelles à l'heure de l'économie numérique.

Enjeu économique. L'économie numérique revêt une importance croissante pour les acteurs économiques comme pour les États. Les données personnelles sont généralement décrites comme son « carburant » et un lobbying des entreprises particulièrement intense fait valoir l'argument que le législateur ne devrait pas entraver le potentiel de l'économie numérique et, d'une manière plus générale, la reprise économique. Les entreprises mesurent aussi l'importance stratégique, en termes de compétitivité, d'une approche responsable des données personnelles.

Enjeu international. La proposition de règlement européen se situe dans un contexte international mouvant, avec

> Des enjeux divers et majeurs autour de la protection d'un droit fondamental.

> L'Europe doit agir de manière décisive pour mettre en place un cadre rigoureux en matière de protection des données, qui servirait ensuite d'étalon-or pour le monde entier. Sinon, d'autres agiront avant nous et nous imposeront leurs normes.
>
> *(Viviane Reding, Vice-présidente de la Commission européenne et Commissaire à la Justice, aux Droits fondamentaux et à la Citoyenneté, à l'occasion de la journée européenne de la protection des données, 2014).*

plusieurs réformes concomitantes dans différentes régions du monde. Le Conseil de l'Europe procède à la révision de la Convention n° 108 sur la protection des données ; l'OCDE vient d'actualiser ses lignes directrices en la matière ; l'APEC (Coopération économique pour l'Asie-Pacifique) développe son propre cadre en matière de transferts internationaux de données. Compte tenu des enjeux évoqués ci-avant, le défi pour l'UE est de rester un modèle de référence pour façonner la future gouvernance mondiale de la protection des données.

Toute la difficulté pour le législateur européen est de trouver le juste équilibre pour garantir une protection des données personnelles à la mesure de ces enjeux. Dans la recherche de cet équilibre, il conviendra de retenir que la protection des données, est avant tout un droit fondamental des personnes. ■

> Cette législation introduit des règles européennes globales sur la protection des données, qui remplacent l'ensemble existant de lois nationales.
>
> **Jan Albrecht, Rapporteur du Parlement européen, à l'issue du vote de la Commission LIBE.**

ÉTAT DES LIEUX

Au Parlement européen

En janvier 2013, M. Albrecht, rapporteur de la commission pilote du Parlement européen (Libertés civiles, Justice et Affaires intérieures, ci-après « LIBE ») a présenté son projet de rapport. Ce projet était favorable aux positions de la CNIL, en particulier en ce qui concerne la compétence des autorités dans des situations transnationales, le renforcement des droits des personnes et un meilleur encadrement des transferts de données vers des pays hors UE.

Le projet de rapport LIBE intervenait peu après l'adoption des avis défavorables de la Commission de l'Industrie, de la Recherche et de l'Énergie (« ITRE ») et celle du Marché intérieur et de la protection des consommateurs (« IMCO »). Quant à la Commission de l'Emploi et des Affaires sociales, son avis devait rester marginal dans sa portée dans la mesure où, loin de porter sur l'ensemble du texte comme les autres avis, il se concentrait sur la relation employeur-employés.

L'avis de la Commission des Affaires juridiques, rendu en mars après d'âpres discussions, a joué un rôle important : sensiblement plus modéré dans la prise en compte des intérêts économiques que les avis d'ITRE et IMCO, il a déterminé la volonté de LIBE de parvenir à un meilleur équilibre entre les intérêts en présence.

Signe des enjeux de la réforme, l'action d'influence des parties prenantes – des entreprises en particulier – et la mobilisation des parlementaires ont été particulièrement intenses. Il en a résulté le dépôt de quelque 4000 amendements toutes commissions confondues – un record pour un texte examiné au Parlement européen.

Le nombre exceptionnel de réunions organisées par le rapporteur et les rapporteurs « fictifs » (représentant les autres groupes politiques) pour négocier des amendements de compromis avant le vote explique un glissement de calendrier de sept mois : ce n'est que le 21 octobre 2013, après trois reports de date, que LIBE a adopté son rapport.

Au demeurant, malgré d'intenses négociations autour d'amendements souvent défavorables à la protection des données personnelles, le rapport est jugé globalement positif par la CNIL.

En adoptant son rapport à une très forte majorité, LIBE a donné aux représentants du Parlement un mandat fort pour négocier avec la présidence du Conseil le moment venu.

Au Conseil de l'UE

Conduits respectivement sous présidence irlandaise jusqu'en juin, puis sous présidence lituanienne jusqu'en décembre 2013, et malgré le rythme soutenu des discussions tout au long de l'année, les travaux du Conseil de l'UE n'ont pas permis d'arriver à un consensus sur les aspects fondamentaux du projet de règlement, tels que les définitions des concepts clés, la compétence des autorités de contrôle et la coopération.

La présidence irlandaise a souhaité axer ses réflexions sur le développement d'une approche fondée sur les risques.

Cette approche, soutenue notamment par l'industrie dans une perspective de réduction des coûts et de la charge de travail, vise à moduler plus largement l'application des obligations pesant sur les responsables de traitement et les sous-traitants en fonction des risques sur la vie privée. Ainsi, par exemple, l'obligation de tenir une documentation ou celle de notifier des failles de sécurité à la personne concernée et à l'autorité de protection dépendraient du risque, autant que celle d'effectuer une analyse d'impact sur la protection des données.

La présidence irlandaise a également formulé des propositions concernant le champ d'application territorial et matériel du projet, l'insertion de nouvelles définitions (données pseudonymes, profilage, etc.) et l'expression du consentement (celui-ci devrait être non ambigu, plutôt qu'explicite). Elle s'est aussi attachée à favoriser le recours à d'autres outils de régulation, tels que les codes de conduite et la certification.

Si les délégations ont, dans l'ensemble, au cours du Conseil Justice et Affaires intérieures (JAI) des 6 et 7 juin 2013 réunissant les ministres des États Membres, salué les progrès accomplis, elles ont toutefois indiqué, « qu'il ne peut y avoir d'accord sur une partie du projet de règlement tant qu'il n'y a pas d'accord sur l'ensemble du texte ».

La présidence lituanienne s'est quant à elle attachée à étudier ces problématiques majeures que sont la compétence, les pouvoirs et la coopération.

S'agissant plus particulièrement du **guichet unique**, les propositions formulées se fondaient sur les éléments suivants : ▸▸▸

• une compétence des autorités de protection basée sur un double critère : le lieu de l'établissement du responsable de traitement ou du sous-traitant, ou le lieu où se situent les citoyens affectés par le traitement ;
• l'exercice de compétences exclusives par l'autorité de protection de l'établissement principal dans certains domaines (autorisations, mesures correctives) ;
• une implication et une consultation des autres autorités de protection concernées dans le cadre de l'élaboration des mesures par l'autorité de l'établissement principal, avec une possibilité d'opposition des autorités concernées au projet de mesures ;
• un recours juridictionnel exercé par la personne concernée contre la décision de son autorité de protection devant la juridiction de sa résidence.

Le Conseil JAI des 5 et 6 décembre 2013 n'a pas, non plus, permis d'arriver à un consensus sur cet aspect essentiel, de nombreuses délégations ayant mentionné l'incompatibilité des propositions avec le respect du principe de proximité du citoyen avec l'autorité de protection des données ou le juge national dont il dépend.

Des axes de convergence

Les travaux menés par les deux institutions communautaires tout au long de l'année 2013 ont toutefois permis de dégager plusieurs axes de convergence, préfigurant les futures orientations de la réforme. Ces orientations s'articulent autour des points suivants :
• la confirmation d'un champ d'application territorial large du règlement ;
• l'introduction de nouvelles définitions comme celles de profilage et de données pseudonymes ;
• un renforcement des droits des personnes ;
• un allègement des formalités préalables ;
• l'introduction d'un principe d'*accountability* modulé en fonction des risques pour les droits et les libertés des personnes ;
• la création d'un statut légal pour les sous traitants ;
• le développement de la certification et des codes de conduite européens ;
• une approche plus protectrice de l'encadrement des transferts de données hors de l'UE ;
• un nouveau système de gouvernance s'appuyant sur la désignation d'un guichet unique pour les entreprises, et dont il reste à voir dans quelle mesure il tiendra compte du besoin de proximité du citoyen dans l'exercice de ses droits de recours ;
• une harmonisation des pouvoirs des autorités de protection et des sanctions renforcées. ■

L'ACTION DE LA CNIL

Les travaux du législateur européen ont fait l'objet d'une grande vigilance de la part de la CNIL, soucieuse d'un cadre juridique équilibré, efficace et protecteur des droits des citoyens au niveau national et européen.

Pour exprimer son point de vue sur la réforme, la CNIL a agi par divers canaux tout au long de l'année 2013 :

▸ En faisant régulièrement part de ses préoccupations et recommandations aux contacts clés du **Parlement européen**, notamment aux rapporteurs et « rapporteurs fictifs » des commissions parlementaires saisies, et en participant aux événements divers (conférences, déjeuners thématiques, etc.) au sein ou autour du Parlement. La CNIL elle-même a organisé un séminaire à Bruxelles en février à l'attention des assistants parlementaires des rapporteurs.

> Des contacts réguliers avec les acteurs clés du Parlement européen.

▸ Au travers d'échanges réguliers avec le **Gouvernement** français (SGAE et ministère de la Justice) avant la tenue des groupes de travail du Conseil de l'UE (DAPIX). La CNIL a ainsi pu faire part de son analyse sur les propositions élaborées par la présidence du **Conseil de l'UE**. Dans ce cadre et à l'invitation de la délégation française, la CNIL a assisté, pour la première fois, à plusieurs réunions du DAPIX ;

▸ En poursuivant ses contacts auprès de ses interlocuteurs à la **Commission européenne** (Direction générale de la Justice, des Droits fondamentaux et de la Citoyenneté), notamment pour réitérer ses motifs de préoccupation visant le système de guichet unique et tenter de trouver un compromis à ce sujet.

▸ Par une participation active aux travaux du sous-groupe « futur de la vie privée » du **G29**, où se détermine la position commune du groupe des « CNIL » européennes sur le projet de réforme.

▸ En dialoguant avec des organisations de la **société civile** qui suivent de près la réforme. Pour l'essentiel, ces échanges ont concerné des organisations européennes représentant le point de vue des citoyens, mais aussi leurs membres français. Au travers de ces contacts, la CNIL s'est efforcée de sensibiliser ses interlocuteurs au risque d'éloignement de la protection des données pour les citoyens dans le modèle de guichet unique proposé dans le texte de la Commission européenne.

▸ En communiquant auprès d'organisations représentant le point de vue des **entreprises**, mais aussi de groupes de réflexion spécialisés. La CNIL a été plusieurs fois sollicitée au cours de l'année, pour présenter la réforme et ses enjeux ou pour participer à des débats contradictoires à ce sujet.

La CNIL a aussi tenu à s'exprimer par voie de communiqué de presse à diverses étapes du processus législatif, notamment suite à la publication du projet de rapport LIBE, en janvier, et suite à l'adoption du rapport final de LIBE, en octobre. Dans un communiqué d'avril, la CNIL soulignait l'importance des enjeux de la réforme pour la France. ■

> La CNIL associée aux réflexions du gouvernement français.

LES PRINCIPAUX SUJETS DE PRÉOCCUPATION DE LA CNIL

Le modèle de gouvernance

Élément clé du projet de règlement, la compétence des autorités de protection et la manière dont elles coopèrent entre elles a fait l'objet d'une attention particulière de la part de la CNIL.

La CNIL estime que s'il est légitime que les entreprises implantées dans plusieurs États membres puissent disposer d'un interlocuteur unique pour les traitements de données mis en œuvre dans ces pays, cette nécessité pratique ne doit pas pour autant remettre en cause la protection tout aussi légitime des droits des citoyens, telle qu'elle est assurée par les autorités nationales de contrôle, ni porter atteinte à l'exercice des garanties qui sont offertes aux citoyens.

En effet, le modèle tel que proposé par la Commission européenne de par sa complexité et les difficultés pratiques, linguistiques et financières qu'il engendre, ne garantit pas un droit à un recours effectif comme l'exigent la Charte des droits fondamentaux de l'UE (article 47) et la Convention européenne des droits de l'homme (articles 6 et 13).

Par ailleurs les propositions formulées par la Commission LIBE et la présidence du Conseil de l'UE ne répondent pas complètement à ces exigences.

En effet, le rapport LIBE, en prévoyant que l'autorité chef de file est la seule à pouvoir prendre des mesures contraignantes à l'encontre des responsables de traitement et des citoyens, ne permet pas à ces derniers d'exercer leurs recours devant leur juridiction nationale. Par ailleurs, la possibilité pour une autorité de protection d'intenter une action contre une autre autorité (l'autorité chef de file) ne contribue pas à une bonne coopération entre les autorités de protection.

Les propositions formulées par la présidence lituanienne au Conseil de l'UE n'apparaissent pas davantage satisfaisantes.

En effet, en conférant des compétences exclusives à l'autorité de l'établissement principal en matière d'autorisation et de pouvoirs correctifs, l'indépendance des autres autorités de protection se voit remise en cause.

> Une concertation étroite avec le Gouvernement pour un modèle de guichet unique dans l'intérêt de tous.

La CNIL s'est donc attachée à promouvoir **un modèle de gouvernance égalitaire, efficace et protecteur des droits des citoyens** dans des situations nationales et transnationales.

À cette fin elle a conçu, en étroite **concertation avec le Gouvernement français**, une solution alternative et crédible au modèle de guichet unique proposé par la Commission européenne.

Ce nouveau schéma de gouvernance répond à un **triple objectif** :
- assurer une meilleure protection du citoyen en lui garantissant un contrôle « de proximité », c'est-à-dire sur le territoire de sa résidence, par son autorité de protection ;
- prendre en compte le besoin des entreprises d'un « guichet unique » ;
- garantir une interprétation et une application uniforme du droit.

Cette proposition alternative, présentée aux autres délégations au sein du DAPIX en septembre 2013, prévoit :
- **une compétence conjointe et partagée sur les traitements « transnationaux »** entre les autorités du pays de résidence des personnes visées par le traitement et l'autorité du pays de l'établissement principal de l'entreprise ;
- **une organisation de la coopération entre les autorités de protection par la désignation d'une autorité chef de file sur le critère de l'établissement principal.** Cette autorité chef de file constitue l'interlocuteur unique des entreprises ;
- **une adoption des décisions dans le cadre d'une procédure de codécision.** L'autorité chef de file prend des décisions avec l'accord des autres autorités de protection compétentes et la décision est mise en œuvre par chaque autorité sur son territoire national. Afin d'assurer l'efficacité du dispositif, un système de décision implicite d'acceptation des autorités compétentes dans un délai strict est prévu. Les autorités de protection sont donc impliquées dans un processus décisionnel égalitaire, équilibré et respectueux de leur indépendance ;
- **un recours juridictionnel effectif,** pour les personnes visées par le traitement, devant le juge de l'État de leur résidence contre les décisions de leur autorité et, pour les responsables de traitement, devant le juge de l'État de l'autorité chef de file dont dépend leur établissement principal ;
- **un nouveau rôle pour le Comité européen de la protection des données (CEPD).** Celui-ci est chargé de régler les différends entre les autorités de protection (par exemple pour la désignation de l'autorité chef de file ou en cas d'inaction d'une autorité de contrôle) et il est le garant d'une interprétation uniforme des dispositions du règlement.

Les données pseudonymes

Le rapport LIBE ainsi que le dernier document de travail du Conseil confirment une orientation dangereuse des travaux législatifs, à savoir une considération particulière pour les données pseudonymes.

Avec le développement de la société de l'information, des pseudonymes « numériques » sont de plus en plus utilisés comme forme alternative d'identification. Ils permettent à des entreprises de singulariser des individus, sans avoir besoin de connaître leur identité civile, par le recours à d'autres identifiants ▸▸▸

(un login, un code lié au téléphone, à l'ordinateur ou à une carte à puce, une empreinte digitale…). Ces identifiants permettent d'obtenir et de rassembler des informations précises sur les habitudes de consommation, les déplacements, l'emploi, le niveau de vie etc. des personnes, qui sont ainsi singularisées. Ces traitements ont pour finalité directe de traiter les individus de manière individuelle, en leur communicant une information personnalisée, en leur offrant un prix différencié, en leur ouvrant (ou non) l'accès à certains services, etc. Il existe donc une possibilité de discrimination.

Ces pseudonymes numériques sont à distinguer des données pseudonymisées, où un processus de minimisation a remplacé les données identifiantes par un code. Le processus de pseudonymisation vise, non pas à prendre des mesures individualisées envers l'une ou l'autre personne en particulier, mais à permettre la poursuite d'un objectif légitime (scientifique, statistique ou historique) lorsque cet objectif ne peut pas être atteint au moyen de données anonymes. Dans ce cas de figure, la pseudonymisation apparaît comme une mesure de sécurité justifiant un régime distinct, dans le respect des exigences de proportionnalité.

Or, un amalgame est créé à dessein entre les données pseudonymes et les données pseudonymisées avec l'idée d'établir une sous-catégorie de données personnelles qui, au motif que leur traitement présenterait moins de risques, serait soumise à **un régime de protection allégé**. Notamment, le traitement de données pseudonymes serait présumé légitime, et l'obligation du responsable de traitement d'informer le sujet et de garantir son droit d'accès et de rectification serait limitée.

Pour la CNIL, l'inclusion dans le règlement d'une définition de données pseudonymes, alors même qu'elles restent des données à caractère personnel et que les capacités croissantes de croisement des données rendent la protection contre une ré-identification du sujet toute relative, ne ferait que brouiller la distinction entre données personnelles et données anonymes.

La CNIL met donc en garde contre un régime allégé pour les données pseudonymes qui aurait pour effet, dans la pratique, de soustraire une part croissante des données personnelles traitées à la protection qu'elles méritent. Certains ont justement évoqué un « cheval de Troie » pour la protection des données.

> Un cheval de Troie pour la protection des données.

L'approche par les risques

La Commission LIBE ainsi que le Conseil de l'UE ont formulé de nombreuses propositions visant à appliquer une approche fondée sur les risques notamment sur le principe d'*accountability* et sur les outils permettant de décliner ce principe.

Ainsi, cette approche conduit à moduler l'application du principe et des obligations pesant sur les responsables de traitement (et les sous traitants) en fonction des risques identifiés sur les droits et les libertés des personnes (ex : la tenue de la documentation, la notification des failles de sécurité, la conduite d'analyse d'impact). L'utilisation de données pseudonymes dans le cadre de cette approche, notamment afin de réduire les risques, doit également faire l'objet d'une attention particulière, puisque les traitements ne présentant pas de risques pourraient faire l'objet d'une exemption du principe d'*accountability* ou de l'application de ces outils de conformité.

La CNIL estime que l'approche par le risque ne doit en aucun cas conduire à exonérer le responsable de traitement de son obligation générale de conformité aux dispositions du règlement. Néanmoins, elle considère que la mise en œuvre des outils d'*accountability* (comme les analyses d'impact et le système de notification des failles de sécurité, par exemple) pourrait être modulée en fonction des risques pour les droits et libertés fondamentales pour la personne concernée. ■

INFOS +

Le principe d'*accountability* signifie que tout responsable de traitement a l'obligation d'être en conformité avec les dispositions du règlement et être en capacité de le démontrer à la demande des autorités et/ou des citoyens concernés.

LES TRAVAUX DU G29

La CNIL s'est attachée aussi à défendre ses positions dans le cadre du G29, en particulier dans la cadre du sous-groupe « Futur de la vie privée ».

Sur la compétence

L'avis du 27 février 2013, qui se concentre sur la question de la compétence des autorités de protection, précise les exigences considérées comme essentielles pour l'ensemble des membres du G29 concernant le guichet unique. Accompagné de propositions d'amendements, il préconise :
- une compétence territoriale des autorités de contrôle fondée sur les critères d'établissement et de ciblage ;
- l'instruction des cas transfrontaliers confiée à une autorité désignée comme « chef de file » agissant au nom et pour le compte des autres autorités de protection ;
- le caractère contraignant que doit nécessairement revêtir la décision de l'autorité « chef de file » ;

• le droit pour le citoyen de former un recours sur son propre territoire contre la décision adoptée par l'autorité « chef de file ».

L'avis du 13 décembre 2013 revient sur la question de la compétence (parmi d'autres points) en exprimant le soutien du G29 pour la désignation d'une autorité chef de file agissant comme point de contact unique pour le responsable de traitement, tout en soulignant la nécessaire participation des autorités de protection concernées dans le processus décisionnel.

Les propositions de la CNIL décrites plus haut sont en cohérence avec ces avis.

Sur les autres aspects

Accompagné d'un communiqué de presse insistant sur l'urgence d'adopter le projet de règlement avant les échéances législatives européennes, l'avis du 11 décembre 2013 aborde, entre autre, les problématiques suivantes :

Les données pseudonymes

Le G29 relève les risques d'un recours à cette notion visant à appliquer un régime juridique allégé pour les responsables de traitement. Il souligne que si la pseudonymisation est utile pour renforcer la protection des données, elle ne change pas pour autant la nature des données - qui restent des données personnelles - dans la mesure où il existe une possibilité de ré-identification avec des moyens raisonnables susceptibles d'être utilisés par le responsable de traitement ou une tierce partie.

Les concepts clés

Après avoir défendu le maintien du caractère explicite du consentement, le G29 soutient également le respect du principe de finalité en supprimant la possibilité de traiter ultérieurement des données à des fins non compatibles avec la finalité première.

Les transferts et l'accès aux données par les autorités publiques de pays tiers

Le G29 indique qu'une surveillance générale, massive et systématique des citoyens de l'UE est inacceptable et qu'à cet égard, la proposition de la Commission LIBE d'introduire un nouvel article concernant l'accès aux données par les autorités publiques de pays tiers est la bienvenue. Toutefois, cette proposition n'est pas suffisante pour assurer une protection réelle et effective des citoyens européens et doit être accompagnée par la mise en place d'instruments internationaux afin d'encadrer efficacement ce type de transferts.

Le G29 mentionne également les risques liés à la suppression de la mention des règles internes d'entreprises (BCR) pour les sous-traitants, lesquelles permettent aux sous-traitants d'assurer une protection adéquate lorsqu'ils effectuent des transferts de données hors de l'UE.

Le G29 salue la suppression de la possibilité d'encadrer les transferts de données hors de l'UE par des instruments juridiques non contraignants.

Les pouvoirs des autorités de protection

Le G29 salue également le montant accru des sanctions qui peuvent être infligées par les autorités de protection et qui constitue un outil dissuasif et approprié. ■

2.

BILAN D'ACTIVITÉ

Informer le grand public et les professionnels

Conseiller et réglementer

Accompagner la conformité

Protéger les citoyens

Contrôler et sanctionner

Gros plan
Vidéo protection : bilan de trois ans de contrôles

Anticiper et innover

Participer à la régulation internationale

INFORMER LE GRAND PUBLIC ET LES PROFESSIONNELS

La CNIL est investie d'une mission générale d'information des personnes sur les droits et les obligations que leur reconnaît la loi Informatique et Libertés. Elle répond au public, qu'il s'agisse des professionnels ou des particuliers, elle mène des actions de communication et s'est particulièrement investie en 2013 en matière d'éducation au numérique. Elle est présente dans la presse, sur Internet, sur les réseaux sociaux où elle met à disposition des outils pédagogiques. Directement sollicitée par de nombreux organismes, sociétés ou institutions pour conduire des actions de formation et de sensibilisation, la CNIL participe aussi à des colloques, des salons ou des conférences pour informer et s'informer.

LA CNIL VOUS INFORME AU QUOTIDIEN

Partenariat France Info

Le partenariat débuté en 2007 a été renouvelé en 2013. Au total, ce sont 350 sujets qui ont été diffusés depuis 2007. 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. En 2013, les 50 chroniques diffusées portaient sur des sujets tels que : le droit à l'oubli, l'usurpation d'identité, la communication politique, les tarifs sociaux de l'énergie, la réalité augmentée, les listes noires, le *cloud computing*, la surveillance au travail, les objets connectés, etc.

Les publications à destination des professionnels

À l'occasion de la journée européenne de la protection des données, la CNIL a publié le 28 janvier 2013 une série de fiches pratiques destinées à accompagner les salariés et les employeurs dans leur gestion des données personnelles au travail. Recrutement, contrôle des horaires, de l'utilisation d'Internet et de la messagerie, géolocalisation, vidéosurveillance : Quel est le cadre légal ? Quelles sont les erreurs à éviter ? Quels sont les droits des employés ? Ces 5 fiches pratiques ont été téléchargées 52 000 fois depuis leur mise en ligne.

Le site Internet www.cnil.fr

En 2013, la CNIL a procédé à une refonte graphique de sa page d'accueil et de son site, afin de rationnaliser et faciliter l'accès à l'offre de services et de contenus qu'elle propose. L'enjeu pour la CNIL était de clarifier auprès des internautes le périmètre de son action tout en prenant en compte l'état de l'art. La nouvelle page d'accueil a vocation à mettre en avant l'actualité et les dernières mises à jour, en proposant des accès directs aux téléservices (plaintes, déclarations).

En moyenne sur l'année 2013, 237 000 pages vues ont été consultées par 38 191 visiteurs uniques par semaine, soit une progression de 18,8 %. La durée moyenne de la visite est de 5 minutes et 13 secondes.

La présence sur les réseaux sociaux

En 2013, le compte Twitter de la CNIL a gagné près de 10 000 followers et la page Facebook a quant à elle dépassé le cap des 10 000 fans. Présente sur les principaux réseaux sociaux, la CNIL dialogue avec les internautes et délivre des conseils, bonnes pratiques et recommandations, quel que soit le niveau de connaissance de la loi Informatique et Libertés. La plupart des questions porte sur les usages numériques et sur les droits.

L'image de la CNIL

Depuis 2004, la CNIL mesure sa notoriété ainsi que la connaissance des droits. Le baromètre de l'IFOP porte sur un échantillon de 967 personnes, représentatif de la population française âgée de 18 ans et plus. Les interviews ont eu lieu en face à face au domicile des personnes interrogées du 4 au 9 décembre 2013. ■

11 200
FANS SUR FACEBOOK

28 000
ABONNÉS SUR TWITTER

54 %
DES PERSONNES CONNAISSENT LA CNIL CONTRE 32 % EN 2004

35 %
DES PERSONNES ONT LE SENTIMENT D'ÊTRE SUFFISAMMENT INFORMÉES À PROPOS DE LEURS DROITS EN MATIÈRE DE PROTECTION DES INFORMATIONS PERSONNELLES

190
ÉVÉNEMENTS À L'OCCASION DESQUELS LA CNIL EST INTERVENUE

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 particuliers et les professionnels.

- **35 524 courriers reçus**
- **124 595 appels téléphoniques**
- **92 351 dossiers de formalités traités**
- **93 % des formalités sont effectuées en ligne**

En 2013, la CNIL a traité 92 351 dossiers de formalités qui se décomposent de la façon suivante :

- 50 832 déclarations simplifiées,
- 35 931 déclarations normales,
- 1 501 demandes d'autorisation,
- 1 359 demandes d'avis,
- 656 demandes d'autorisation de recherche médicale,
- 215 demandes d'autorisation d'évaluation de soins,
- 659 demandes de modification effectuées par courrier.

En 2013, la CNIL a délivré les récépissés dans un délai moyen de 48 h pour les déclarations simplifiées et de 5 jours calendaires pour les déclarations (soit 32 737 récépissés de déclarations délivrés).

En 2014, la CNIL engage une réflexion sur l'amélioration de la relation de l'institution avec ses usagers pour mieux répondre à leurs attentes et développer une offre de réponse en ligne. ■

INFOS +

Les usagers sont-ils satisfaits ?

L'enquête de satisfaction réalisée par l'IFOP en octobre 2013 auprès de 1 012 usagers montre que :

- **93 % sont satisfaits de l'accomplissement des formalités préalables**
- **86 % sont satisfaits du contact avec la CNIL**

43 %

DES FRANÇAIS CONSIDÈRENT NE PAS MAÎTRISER L'UNIVERS D'INTERNET

28 %

DES FRANÇAIS AFFIRMENT NE JAMAIS UTILISER INTERNET

83 %

DES FRANÇAIS ESTIMENT QUE L'ÉDUCATION AU NUMÉRIQUE DOIT ÊTRE UNE PRIORITÉ DANS LES ANNÉES À VENIR

Source : IFOP « Les Français et l'éducation au numérique », échantillon de 1000 personnes âgées de 18 ans et plus, octobre 2013.

ÉDUCATION AU NUMÉRIQUE : MISE EN PLACE D'UN COLLECTIF POUR CHANGER D'ÉCHELLE

Le numérique est aujourd'hui omniprésent dans nos vies et il constitue une source d'innovations et d'opportunités inédites pour accéder à de nouveaux services, simplifier les démarches administratives ou encore améliorer la compétitivité des entreprises. Or, une partie importante de la population fait état d'un rapport distant, voire inexistant, à Internet. La CNIL a considéré qu'il était urgent d'élargir les actions de sensibilisation au-delà des plus jeunes pour toucher tous les publics afin qu'ils puissent devenir de véritables citoyens numériques, responsables dans leurs usages et attentifs aux nouveaux risques.

> L'objectif est d'offrir à tous les publics une culture générale du numérique.

L'éducation au numérique relevant d'une responsabilité partagée entre les acteurs publics et privés, 51 organismes d'envergure nationale et internationale ont constitué en 2013, à l'initiative de la CNIL, un collectif. Il s'agit d'une mobilisation sans précédent d'associations, de fédérations professionnelles, d'institutions autour d'un projet et de valeurs communes en faveur de l'éducation au numérique. En mutualisant leurs moyens pour s'adresser à tous les publics, les membres du collectif ont déposé un dossier auprès des services du Premier ministre pour obtenir le label de grande cause nationale en 2014. Si le label « grande cause nationale » n'a finalement pas été attribué à cette thématique, la mobilisation des membres continuera en 2014 grâce à différentes actions communes.

Au plan international, la CNIL a mis l'éducation au numérique à l'ordre du jour de la 35ème Conférence internationale des Commissaires à la Protection des données et de la Vie privée (Varsovie du 23 au 26 septembre 2013) qui réunit plus de 50 pays dans le monde. Une résolution sur « Une éducation au numérique pour tous » a été adoptée et la CNIL est chargée d'animer le groupe de travail international destiné à mettre en œuvre de façon opérationnelle les recommandations à destination des divers publics et à faire émerger les meilleures pratiques en matière d'éducation aux nouvelles technologies. ■

CONSEILLER ET RÉGLEMENTER

La régulation de la protection des données personnelles passe par différents outils : déclarations, autorisations, conseils, accompagnement, mise en œuvre de pouvoirs répressifs. Dans toute cette gamme d'activités, la CNIL veille à la recherche permanente d'un juste équilibre, au service du citoyen, entre la protection des libertés publiques, la production d'outils opérationnels de mise en conformité des administrations et organismes publics et privés, et la nécessaire diffusion de la culture « Informatique et Libertés » auprès de l'ensemble de ces acteurs.

Parmi les outils à sa disposition, la CNIL peut :

• délivrer des autorisations de mettre en œuvre des traitements,
• rendre des avis sur des projets de textes d'origine gouvernementale impliquant des données personnelles ou créant de nouveaux fichiers,
• élaborer des cadres juridiques simplifiant l'accomplissement des formalités préalables,
• adopter des recommandations permettant de fixer sa doctrine dans certains domaines,
• répondre aux demandes de conseils des responsables de traitement, dans des proportions de plus en plus importantes, notamment par l'intermédiaire des correspondants Informatique et Libertés.

Le bilan de l'activité 2013 témoigne d'une activité en nette augmentation par rapport à l'année précédente, avec près de 2 500 décisions et délibérations adoptées (hors décisions de sanction), soit une hausse de près de 20 %. ■

LES AVIS OU AUTORISATIONS

Afin de répondre aux demandes sans cesse croissantes des responsables de traitement, la CNIL organise des ▸▸▸

FOCUS

Avis sur la transparence des liens d'intérêts dans le secteur de santé

La CNIL a rendu plusieurs avis sur la transparence des liens d'intérêts et des avantages consentis, qui constitue un des moyens permettant de renforcer la confiance dans le système de sécurité sanitaire du médicament. La loi du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé a posé l'obligation de publication des liens entre les entreprises de produits de santé et de cosmétiques et les professionnels de santé. Par ailleurs, la législation dite « anti-cadeaux » visant à prévenir l'octroi de cadeaux à ces mêmes professionnels, a été renforcée. Le décret du 21 mai 2013 dit « *Sunshine act* » à la française ou « Décret Transparence », détermine la nature des informations et les modalités de publication de ces liens d'intérêt.

La CNIL s'est prononcée par avis, sur le projet de décret, ainsi que sur l'arrêté pris pour son application.

Sont concernées principalement : les entreprises du médicament, les établissements de santé et les professionnels de santé. Doivent être rendus publics les avantages ou liens d'intérêt (en espèces ou en nature, d'une valeur supérieure ou égale à 10 euros), quelle que soit leur forme (par exemple un repas, une invitation, un livre, etc.), ainsi que l'existence de conventions (par exemple des conventions de recherche ou de collaboration). La publication de ces données (notamment identité de la personne bénéficiaire et de l'entreprise concernée) sera centralisée sur un site Internet public unique.

Compte tenu de cette centralisation, et afin d'assurer un équilibre entre transparence et protection de la vie privée des personnes, la CNIL a demandé que des mesures techniques soient prises pour empêcher l'indexation par les moteurs de recherche externes. Concrètement, il s'agit d'empêcher l'indexation systématique de ces données par les grands moteurs de recherche de l'Internet. En effet, à partir du moment où une information a été indexée par un moteur de recherche, il est très difficile de s'assurer du respect des durées de conservation prévues par les textes et, pour les personnes concernées, d'exercer leur droit de rectification.

2500

DÉCISIONS ET DÉLIBÉRATIONS ADOPTÉES (+20% PAR RAPPORT À 2012)

401

DÉLIBÉRATIONS PORTANT AVIS OU AUTORISATION ADOPTÉES EN SÉANCE PLÉNIÈRE

1307

AUTORISATIONS DE TRANSFERTS DE DONNÉES HORS UNION EUROPÉENNE

611

DÉCISIONS D'AUTORISATION DE RECHERCHE EN MATIÈRE DE SANTÉ

148

AUTORISATIONS D'ÉVALUATION DU SYSTÈME DE SANTÉ

FOCUS

Avis sur le projet de loi de programmation militaire

La CNIL a été saisie en urgence, en juillet 2013, des dispositions des articles 8 à 12 du projet de loi de programmation militaire. Elle a rendu son avis dans une délibération en date du 18 juillet 2013. En revanche, elle n'a pas été saisie des dispositions de l'article 13 du projet, relatives à l'accès en temps réel aux données de connexion par des agents des services de renseignement des ministères de l'Intérieur, de la Défense et du Budget. Cet article, devenu l'article 20 de la loi, permet à ces agents d'accéder aux données conservées par les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs. Concrètement, la réquisition de données de connexion dans un cadre d'enquête administrative pourra être effectuée pour la recherche de renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et la reconstitution ou le maintien de groupements dissous.
Réunie le 19 décembre 2013 en séance plénière, la Commission a souhaité faire part de sa position à la suite de la promulgation de la loi de programmation militaire, notamment son article 20. Elle a regretté de ne pas avoir été saisie de ces dispositions par le Gouvernement lors de l'examen du projet de loi qui lui a été soumis ; à ce titre, elle a souhaité à l'avenir être systématiquement consultée pour tous les textes législatifs ou réglementaires concernant les données personnelles. Elle a déploré que la rédaction définitive du texte semble autoriser un accès aux données de contenu et non seulement aux données de connexion, ce qui ne saurait intervenir en vertu des autres dispositions législatives applicables en la matière. La CNIL sera très vigilante sur la rédaction des décrets d'application de la loi qui devront lui être soumis.

▸▸▸ séances plénières toutes les semaines. Elle a aussi mis en place des procédures d'autorisations déléguées auprès de la Vice-présidente déléguée, pour les traitements les plus courants, sur laquelle sa doctrine est clairement établie. L'objectif est de réduire les délais d'instruction, particulièrement en matière de recherche médicale. ■

LES OUTILS DE SIMPLIFICATION DES FORMALITÉS

La CNIL a adopté en 2013 une dizaine d'outils de simplifications, sous forme de décisions-cadres concernant des traitements visant une même finalité ou des catégories de données et de destinataires identiques (3 autorisations uniques, 6 avis concernant des actes réglementaires uniques, 2 normes simplifiées). Ces décisions-cadres permettent aux responsables de traitements d'accomplir une démarche volontaire d'engagement de conformité à des normes pré-établies, leur évitant ainsi de déposer des demandes d'autorisation ou des déclarations spécifiques, traitement par traitement. Elles constituent ▸▸▸

FOCUS

Avis sur le projet de loi relative à la consommation, dans ses dispositions prévoyant la mise en place d'un registre national des crédits aux particuliers (RNCP)

De nombreuses lois ont rythmé l'évolution de la prévention du surendettement en France depuis 1989. L'un des moyens avancés pour lutter contre le surendettement est la création d'un registre national des crédits aux particuliers, qui a fait l'objet de plusieurs propositions de lois restées sans suite jusqu'en 2014.

La Commission en tant que conseil du législateur a, depuis 2001, émis de fortes réserves quant à la mise en place en France d'une centrale de crédit susceptible de recenser des informations sur des encours de crédit et a réaffirmé la nécessité de ne pas utiliser le NIR ou numéro de sécurité sociale comme identifiant d'un tel fichier, si le législateur souhaitait néanmoins le mettre en place. Elle a notamment apporté son expertise aux travaux du comité de préfiguration du registre national des crédits aux particuliers. Ce comité, créé en 2010, était chargé d'examiner les modalités de création et de fonctionnement d'un tel registre afin de fournir au législateur des éléments concrets.

Saisie du projet de loi par le Gouvernement le 18 mars 2013, la CNIL a réitéré ses réserves sur la proportionnalité du dispositif et son opposition à l'utilisation du NIR (numéro de sécurité sociale) comme identifiant.

La proportionnalité du répertoire remise en cause

Dans sa délibération du 11 avril 2013, la Commission a considéré que le dispositif tel qu'envisagé par le Gouvernement n'était pas proportionné. En effet, l'efficacité d'un tel fichier pour empêcher les plus fragiles de « basculer » dans le surendettement pouvait être regardée comme peu probante au regard des expériences étrangères. En particulier, il apparaît que le surendettement n'est plus le fait seulement de souscriptions compulsives de crédits mais résulte, le plus souvent, d'une accumulation de causes extérieures (diminution des ressources dans un contexte économique tendu, chômage, divorce, etc.).

La consultation d'une centrale de crédit s'avère donc inopérante pour lutter contre la principale cause de surendettement constituée par les accidents de la vie ou le contexte économique : selon les chiffres de la Banque de France, seuls 20 000 à 30 000 cas de surendettement pourraient être évités par la création du registre, les autres cas étant liés à des accidents de la vie par nature imprévisibles.

La CNIL a toujours considéré qu'il était nécessaire de mettre en balance la protection de la vie privée et la lutte contre le surendettement, et de déterminer si cet objectif de lutte contre le surendettement ne pourrait pas être atteint par d'autres moyens. Dès lors, compte tenu de la nature et du volume des données collectées par le registre national envisagé, et de la diffusion d'informations sur des personnes n'ayant jamais manqué à leurs obligations contractuelles, la Commission a considéré que les bénéfices escomptés de la mise en place d'un tel fichier étaient limités et que les atteintes à la vie privée étaient disproportionnées.

Des difficultés liées aux modalités pratiques de mise en œuvre du fichier

La gestion d'un fichier d'une telle ampleur comporte, par nature, des risques importants d'erreurs et des difficultés récurrentes de mises à jour, comme en témoigne la gestion d'autres fichiers centraux, en particulier le FICP, qui porte pourtant sur un volume de données bien moindre.

Les problèmes d'identification sont également liés aux modalités d'identification. Dans certains cas, pour une seule requête, plusieurs réponses peuvent être renvoyées à l'établissement de crédit demandeur à charge pour ce dernier d'identifier la « bonne personne » par la recherche d'éléments complémentaires.

La CNIL a toutefois considéré que le recours au NIR, qui est un numéro signifiant et cantonné à la sphère sociale, comportait un risque important de détournement de finalité, compte tenu du nombre de personnes concernées et de destinataires des informations.

DERNIÈRE MINUTE

Une décision du Conseil constitutionnel dans le prolongement des réserves de la CNIL

Le Gouvernement avait pris en compte plusieurs observations de la CNIL et proposé un nouveau dispositif, afin notamment de restreindre le périmètre du répertoire, pour viser principalement les crédits à la consommation à l'exclusion des crédits immobiliers, et par là même réduire le nombre de personnes concernées, mais également d'abandonner définitivement le recours au NIR. Malgré les aménagements prévus par le législateur, le Conseil constitutionnel a considéré dans sa décision du 13 mars 2014 que l'atteinte au droit au respect de la vie privée était disproportionnée par rapport à l'objectif poursuivi, « eu égard à la nature des données enregistrées, à l'ampleur du traitement, à la fréquence de son utilisation, au grand nombre de personnes susceptibles d'y avoir accès et à l'insuffisance des garanties relatives à l'accès au registre ». Cette décision illustre à nouveau qu'un motif d'intérêt général, en l'espèce, la prévention du surendettement, ne saurait porter atteinte au droit au respect de la vie privée, droit « constitutionnellement protégé ».

51 000

ENGAGEMENTS DE CONFORMITÉ ONT ÉTÉ RÉALISÉS EN 2013 PAR LES RESPONSABLES DE TRAITEMENTS

donc des instruments permettant à la fois d'harmoniser les pratiques et de simplifier considérablement les démarches pour les organismes concernés.

En 2013, près de 51 000 engagements de conformité ont été réalisés par les responsables de traitements, par référence soit à des autorisations dites « uniques » pour les traitements les plus sensibles ou à risque, soit à des normes simplifiées, pour les traitements courants. Depuis l'élaboration de ces outils de simplification, plus de 420 000 engagements de conformité ont été reçus par la CNIL, dont près de 120 000 pour la norme simplifiée NS-48 (fichiers de prospection commerciale) et plus de 30 000 pour la seule gestion du personnel. ■

FOCUS

Dématérialiser l'administration : adoption d'un acte cadre pour simplifier la mise en place de téléservices locaux

Les collectivités locales, et plus largement les organismes en charge d'un service public, facilitent de plus en plus les démarches des administrés en leur permettant d'y accéder par voie électronique (carte à puce, application mobile ou site Internet). Cet accès est susceptible d'être multi-applicatif (plateforme ou « bouquet » de téléservices ; « carte de vie quotidienne », etc.) : il s'agit en effet de mutualiser les accès à différents services publics d'un même territoire (par exemple, transports publics, équipements sportifs, activités scolaires et péri-scolaires, etc.) ou de mutualiser une même catégorie de services entre différents territoires relevant de la responsabilité de divers acteurs publics (par exemple, le transport multimodal à travers une région). Ces applications, dès lors qu'elles sont appelées à traiter des données à caractère personnel, sont soumises au respect de la loi « Informatique et Libertés ».
La CNIL a contribué, en collaboration avec plusieurs représentants de collectivités (au sein de l'Instance nationale partenariale dédiée aux enjeux numériques) et le SGMAP (Secrétariat général à la modernisation de l'action publique) à l'élaboration d'un acte réglementaire unique destiné à simplifier les démarches des collectivités et des usagers.
Ce cadre (dit « RU-030 ») résulte d'un arrêté publié le 13 juillet 2013 après avis de la CNIL.

LES RECOMMANDATIONS

En 2013 la CNIL a élaboré trois 3 recommandations. Véritables lignes directrices qui viennent préciser les conditions de mise en œuvre de la loi, elles facilitent la mise en conformité par les responsables de traitements. Les thèmes retenus ont été les cookies et autres traceurs (cf. supra), les conditions de conservation de numéros de cartes bancaires par les commerçants, et les coffres-forts numériques. ■

FOCUS

Recommandation sur les coffres-forts électroniques

À l'issue d'une concertation avec des acteurs du secteur, la CNIL a adopté une recommandation le 19 septembre 2013 relative aux services de coffres-forts numériques destinés aux particuliers. Elle a souhaité rappeler aux fournisseurs les bonnes pratiques à adopter, notamment en matière de sécurité. Les services de coffre-fort numérique doivent tout particulièrement garantir l'intégrité, la disponibilité et la confidentialité des données stockées et impliquer la mise en œuvre des mesures de sécurité telles que décrites dans la recommandation. Concrètement, la CNIL recommande que les données soient chiffrées à toutes les étapes du processus (transfert vers et depuis un coffre d'une part, stockage d'autre part). De même, les fournisseurs de ce type de service ne doivent pas être techniquement en mesure d'accéder au contenu d'un coffre-fort, ni à ses éventuelles sauvegardes, sans le consentement exprès de l'utilisateur concerné. La CNIL propose que l'appellation « coffre-fort numérique «, ou « coffre-fort électronique «, soit réservée à une forme spécifique d'espace de stockage numérique, dont l'accès est limité à son seul utilisateur et aux personnes physiques spécialement mandatées par ce dernier. Plus récemment, afin de proposer un véritable indicateur de confiance en la matière, la CNIL a décidé, sur la base de ses recommandations, d'élaborer un nouveau référentiel sur les services de coffre-fort numérique. Le label permettra ainsi aux utilisateurs d'identifier et de privilégier les services de coffre-fort numérique qui garantissent un haut niveau de protection de leurs données personnelles grâce notamment à des mesures de sécurité appropriées.

ACCOMPAGNER LA CONFORMITÉ

Face à un environnement technologiquement de plus en plus complexe, caractérisé par de très nombreux acteurs aux interactions multiples, la place et le rôle de la CNIL évoluent nécessairement. Il lui appartient de pouvoir appréhender cet univers, identifier les conséquences qui en résultent pour les professionnels en termes de traitement de données personnelles, répondre aux besoins qui s'expriment et proposer un nouveau mode de régulation.

L'objectif est de proposer une « boîte à outils » de la conformité prenant appui sur les divers leviers d'action dont dispose la CNIL : les correspondants Informatique et Libertés qui constituent le réseau privilégié des experts, le développement des labels et des règles internes d'entreprise ou BCR qui encadrent le transfert des données des multinationales hors Union européenne, la création de « packs de conformité » qui sont des référentiels sectoriels, couvrant un secteur d'activité ou une branche professionnelle dans son intégralité.

Accompagner la conformité signifie tout à la fois

- **une nouvelle méthode de travail** : en associant pleinement les acteurs d'un secteur d'activité afin d'identifier les bonnes ou mauvaises pratiques, les problèmes rencontrés, les demandes des usagers, les spécificités du secteur concerné et les questions qui se posent sur le terrain.
- **un nouveau mode de régulation pour la CNIL** : en élaborant des référentiels sectoriels comprenant des outils juridiques et pratiques adaptés.

Un double objectif

- simplifier les formalités autant que la loi actuelle le permet ;
- sécuriser juridiquement les professionnels en donnant des indications concrètes sur la façon de respecter les textes et des modes opératoires précis. Il s'agit d'aider les professionnels à s'approprier les moyens de respecter la loi « Informatique et Libertés » en intégrant le principe d'*accountability*, tel que mis en avant dans le projet de règlement européen. ■

LE CORRESPONDANT : UN ACTEUR AU CŒUR DE LA CONFORMITÉ

À l'heure où le numérique fait partie de notre quotidien, les CIL (correspondants Informatique et Libertés) sont devenus des acteurs incontournables pour agir au sein des organismes publics ou privés qui traitent des données personnelles. Assurer de manière optimale la protection des données personnelles constitue non seulement une obligation légale, mais aussi un enjeu de crédibilité vis-à-vis des usagers ou des clients. En 2013, ce sont ainsi près de 13 000 organismes qui ont choisi de se doter d'un CIL pour renforcer la sécurité juridique et technique de leur patrimoine informationnel, contre 8 500 en 2011.

Le CIL, acteur de la co-régulation

De par ses missions, le CIL intervient en amont de la mise en œuvre des traitements de données et prévient son organisation des éventuels manquements qui pourraient naître de mauvaises pratiques. Son intervention permet ainsi, dès la conception des traitements, de prendre en compte la protection des données.

Lors de sa prise de fonction, le CIL a notamment pour mission de recenser et cartographier les traitements de données mis en œuvre qu'il reportera dans la liste des traitements qu'il doit tenir (le registre). Pour autant, les missions du CIL s'apprécient sur le terrain : le CIL doit au quotidien s'assurer, parfois accompagné des équipes en charge du contrôle interne, que les données personnelles sont utilisées conformément à la loi.

La richesse de la désignation d'un CIL s'apprécie particulièrement à l'occasion de l'instruction d'une plainte, d'un contrôle de la CNIL ou des conseils qu'il délivre lors de la mise en place d'un nouveau projet impliquant le traitement de données personnelles de clients, patients, usagers, etc.

Un accompagnement renforcé par la CNIL : permanence juridique et information régulière

Depuis 2005, l'accompagnement de la CNIL n'a cessé de progresser. Avec un service dédié à ces professionnels, la CNIL propose une permanence téléphonique afin d'apporter immédiatement les réponses aux questions des CIL. À ce titre, le service des CIL a répondu à 4 688 appels téléphoniques en 2013 (+13 % par rapport à 2012). Quand ▸▸▸

▸▸▸ les questions nécessitent une recherche approfondie, la réponse est apportée par courrier. 2 414 demandes de conseils juridiques ont été traitées à ce titre en 2013 (+16 % par rapport à 2012).

Pour permettre l'accès à un socle de connaissances essentielles, la CNIL propose en outre des ateliers d'information qui connaissent toujours plus de succès chaque année (cf focus).

En 2013, la CNIL a créé une lettre d'information ACTUS CIL qui a vocation à délivrer une actualité de la protection des données et apporter des réponses aux questions les plus fréquemment posées par les CIL.

Le besoin de créer cette lettre trimestrielle est né du constat que certains CIL peuvent se sentir isolés au sein de leur organisme et n'ont pas toujours réponse aux questions qu'ils se posent. Ainsi, en complément de son offre d'accompagnement, la CNIL apporte **directement l'information aux CIL** tout en proposant une variété de sujets permettant de toucher le plus grand nombre.

Avec l'évolution envisagée par le législateur européen, le CIL, véritable acteur de la conformité dans son organisme, est au cœur du dispositif règlementaire à venir. Le concept d'*accountability* fera entrer le CIL, futur *data protection officer*, dans une nouvelle phase de la co-régulation. La CNIL se prépare à la conduite de ce changement et sera aux cotés des CIL pour les accompagner dans cette transition.


Cette lettre d'information est destinée à l'ensemble de la communauté des CIL afin de les accompagner dans leurs missions

Actus CiL

LA LETTRE D'INFORMATION DU CIL

PAROLES DE CIL

Le numérique apprenons à en profiter

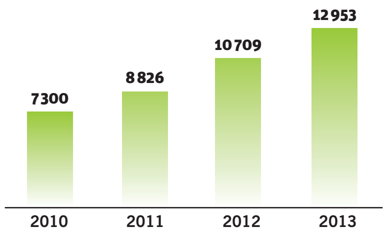
ÉDUCATION AU NUMÉRIQUE GRANDE CAUSE NATIONALE 2014 ?

PRÉPARER LES MUNICIPALES 2014

Bénéficier de l'expérience des CIL

Grâce à leur parcours professionnel et à l'exercice de leurs missions, les CIL sont de bons connaisseurs des impératifs de leur secteur d'activité et des pratiques des organismes qui les ont désignés. À l'occasion de révision de normes, comme dans la préparation de nouvelles méthodologies, la CNIL a sollicité en 2013 les CIL ainsi que les associations de CIL (SUPCIL, Club CIL de l'APRONET) ou les réseaux de professionnels (AFCDP) pour recueillir leurs avis. Par exemple, un panel de CIL a été contacté dans le cadre de la refonte de la norme simplifiée n° 16 concernant la gestion des contrats d'assurances ; les CIL ont été sollicités dans le cadre des réflexions sur l'*open data* ainsi qu'à l'occasion d'une expérimentation des supports pédagogiques pour les organismes souhaitant mettre en œuvre des dispositifs biométriques. ■

Nombre d'organismes ayant désigné un CIL entre 2010 et 2013



> L'efficacité d'un CIL est directement liée à son niveau de formation et aux moyens et ressources affectés par le responsable de traitement à ses missions.

PLUS DE
1200
PARTICIPANTS
AUX 37 ATELIERS
D'INFORMATION

12953
ORGANISMES
ONT DÉSIGNÉ
UN CIL
SOIT 3679 CIL

4688
APPELS
TÉLÉPHONIQUES
ET 2180 DEMANDES
DE CONSEIL
JURIDIQUE

FOCUS

Évolution des ateliers CIL

La CNIL propose des ateliers d'information dédiés aux CIL. Ces ateliers sont variés afin de couvrir le plus large champ des besoins de cette communauté. Des ateliers relatifs aux grands principes et notions clés de la loi Informatique et Libertés (les fondamentaux), aux ressources humaines, à la santé, à la sécurité, aux collectivités locales sont proposés.
Chaque journée d'information attire entre 40 et 60 participants. En 2013, ce sont 37 ateliers qui ont accueilli 1251 CIL.
Proposé par cycle et par niveau, l'ambition de ces ateliers est de répondre aux exigences du terrain en proposant au-delà de la présentation des principes et concepts, de nombreux cas pratiques et mises en situation (fondamentaux III) ainsi que la réalisation de quiz effectués à chaque atelier aux fins de vérification des connaissances acquises.
En 2013, une refonte de ces ateliers a été initiée pour prendre en compte la variété des profils et les exigences des participants. En effet, les profils juridiques diminuent au profit des métiers de la sécurité informatique, de la conformité ou de la qualité, etc. L'objectif de cette évolution est de permettre une plus grande interactivité de ces ateliers d'information. Cette orientation se poursuivra dans les prochains mois.

LE LABEL : UN GAGE DE CONFIANCE

En 2013, le processus de labellisation de la CNIL s'est développé. Au-delà du nombre croissant des demandes, deux nouveautés ont vu le jour :

Le dépôt des demandes en ligne

La CNIL propose désormais sur son site Internet un espace de dépôt sécurisé pour le formulaire de demande de délivrance de label mais également pour les compléments qui pourraient être à adresser dans le cadre de l'instruction du dossier.

Les retours d'expérience

La CNIL doit s'assurer que les conditions qui ont permis la délivrance du label sont bien maintenues après la délivrance et pendant toute la durée de vie du label. C'est pourquoi elle a la possibilité d'aller vérifier sur place, d'interroger les organismes labellisés ou de demander tout autre document de nature à le prouver. Pour ce faire, dans chaque délibération portant délivrance d'un label CNIL, la Commission prévoit l'élaboration par l'organisme labellisé d'un bilan annuel d'activité aux termes de la première année. Ce bilan doit être transmis à la CNIL. Cette demande a pour but de :

- vérifier que les procédures labellisées sont mises en œuvre conformément au référentiel auquel elles se rapportent ;
- contrôler que le logo Label CNIL est utilisé conformément au règlement d'usage de la marque collective ;
- mesurer l'impact du Label CNIL.

Un nouveau référentiel pour les services de coffre-fort numérique

À l'heure où les offres de stockage dématérialisées et sécurisées se multiplient, nombreux sont les particuliers désireux de stocker en ligne leurs bulletins de salaires, factures et pièces d'identités. Or, chaque prestataire de service de coffre est aujourd'hui libre de déclarer qu'il garantit l'intégrité, la disponibilité et la confidentialité des données stockées, sans que les utilisateurs n'aient les moyens de le vérifier.

C'est pourquoi, afin de proposer un véritable indicateur de confiance en la matière, la CNIL a décidé, sur la base de ses recommandations adoptées le 19 septembre 2013, d'élaborer un nouveau référentiel sur le sujet. Le label permettra ainsi aux utilisateurs d'identifier ▸▸▸

Le label CNIL est perçu comme un véritable indicateur de confiance pour les usagers, garant d'un haut niveau de protection des données personnelles.

et de privilégier les services de coffre-fort numérique qui garantissent l'intégrité, la disponibilité et la confidentialité des données stockées et mettent en œuvre les mesures de sécurité appropriées.

La CNIL a adopté le 23 janvier 2014 un nouveau référentiel lui permettant de délivrer des labels aux services de coffre-fort numérique. Après ses deux labels « formation » et « audit », elle adopte donc son premier label « produit ».

Le nouveau référentiel comprend vingt-deux exigences qui vont au-delà de ce que prévoit la loi. Il comprend des exigences sur :

- les données traitées, notamment sur le stockage de données de santé ;
- l'accès aux données ; à ce titre, la CNIL précise que le coffre-fort numérique se distingue du simple espace de stockage par le fait que les données conservées ne sont accessibles qu'au seul titulaire du coffre et, le cas échéant, aux personnes physiques que le titulaire a spécifiquement habilitées à cet effet ;
- la conservation limitée des données ;
- l'information détaillée des personnes ; à ce titre la CNIL demande notamment que le prestataire de service de coffre-fort informe les personnes de tout transfert de données à caractère personnel envisagé, à destination d'un État non membre de la Communauté européenne, en indiquant si cet État, sur la base de sa propre législation, pourrait effectuer des demandes visant à accéder directement aux données conservées ;
- la gestion des risques ;
- des mesures de sécurité appropriées dans le cadre d'un service de coffre-fort numérique garantissant la confidentialité des données, notamment grâce à des mesures de chiffrement et des mécanismes d'authentification. ■

2012
LANCEMENT DU PREMIER RÉFÉRENTIEL

3
RÉFÉRENTIELS EXISTANTS

46
DEMANDES DE DÉLIVRANCE DE LABELS

29
LABELS DÉLIVRÉS

5 MOIS 1/2
DÉLAI MOYEN DE DÉLIVRANCE

LE DEVELOPPEMENT DES « PACKS DE CONFORMITÉ »

Les packs de conformité contiennent :

- Des outils juridiques de simplification et d'allégement des procédures (autorisations uniques, normes simplifiées) ;
- Des outils pour promouvoir les bonnes pratiques « Informatique et Libertés » adaptés au secteur.

Le secteur des assurances

L'année 2013 a été riche pour le secteur des assurances : une série de réunions avec les organisations professionnelles, FFSA, GEMA, CTIP, FNMF, CSCA a permis de mettre à plat l'ensemble des traitements du secteur dans le double objectif de :

- simplifier les formalités autant que la loi actuelle le permet,
- sécuriser juridiquement les professionnels en donnant des indications concrètes sur la façon de respecter les textes et des modes opératoires précis.

Les normes simplifiées : partie 1 du « pack conformité »

La CNIL a procédé à une refonte de la norme simplifiée n° 16 qui n'avait pas été mise à jour depuis 1981 et à l'adoption d'une nouvelle norme simplifiée n° 56 relative à la gestion commerciale des clients et prospects. Désormais, pour la gestion des contrats d'assurance et la gestion commerciale des clients, les opérations de prospection, ou encore l'élaboration de statistiques commerciales, les organismes d'assurance pourront procéder à un engagement de conformité auprès de la CNIL.

Les autorisations uniques : partie 2 du « pack conformité »

Poursuivant cette logique de simplification des formalités préalables, la Commission a adopté le 23 janvier 2014 le second volet du « pack conformité » relatif aux autorisations uniques pour la collecte des données comportant le numéro de sécurité sociale « NIR » (AU n° 31) et pour la collecte des données d'infractions, de condamnations ou des mesures de sûretés (AU n° 32). L'autorisation unique « NIR » vise tant la collecte et le traitement du NIR dans le cadre des activités d'assurance le justifiant que l'accès au RNIPP (Répertoire national d'identification des personnes physiques) pour la gestion des contrats en déshérence. Par ailleurs, des traitements de données relatifs aux infractions, aux condamnations ou aux mesures de sûreté peuvent s'avérer nécessaires lors de la passation, de la gestion et de l'exécution des contrats d'assurance, de réassurance, de capitalisation et d'assistance. Il s'agit des fichiers de gestion du contentieux mais aussi de l'application de certaines dispositions du code des assurances. Par exemple, les données relatives aux infractions et condamnations font parties des antécédents du contrat d'assurance de l'assuré et permettent notamment à l'assureur d'évaluer les risques. Lors de l'exécution du contrat, des données d'infractions peuvent également être utilisées pour prouver que les conditions de garantie sont remplies et que le risque n'a pas été aggravé.

Le « pack conformité » Assurance sera parachevé avec l'adoption d'une autorisation unique en matière de lutte contre la fraude.

Chacune de ces normes ou autorisations uniques s'accompagne d'une fiche explicative détaillant plus précisément certaines notions spécifiques aux traitements mis en œuvre.

Le secteur du logement social

À la suite des contrôles menés en 2012 (rapport annuel 2012 p. 43), les nombreux échanges et consultations avec les acteurs du secteur du logement social au cours de l'année 2013 ont permis à la CNIL de mieux appréhender les difficultés que ces derniers peuvent rencontrer pour mettre en application les dispositions de la loi « Informatique et Libertés ».

Le pack de conformité qui résulte de ces travaux comprend :

▸ **trois outils de simplification** des formalités à accomplir auprès de la CNIL, à savoir :
- une refonte de la norme simplifiée n° 20 relative aux traitements de données à caractère personnel visant à enregistrer et instruire les demandes de logement social et à assurer une gestion courante du patrimoine immobilier ;
- une nouvelle autorisation unique autorisant les bailleurs sociaux à mettre en œuvre des traitements comportant des appréciations sur des difficultés sociales des résidents aux fins d'attribution, d'adaptation et de mutation des logements ou, si les personnes concernées le souhaitent, de mise en place d'un suivi social personnalisé ;
- une nouvelle autorisation unique concernant la gestion du précontentieux et du contentieux et permettant également de traiter des décisions de justice lorsqu'elles ont une incidence sur un lieu de résidence ;

▸ **un guide pratique et pédagogique** élaboré pour aider les bailleurs à mettre concrètement en application les principes « Informatique et Libertés ». Ce guide aborde les thèmes suivants :
- l'information des résidents ;
- les destinataires des données et les tiers autorisés ;
- la durée de conservation des données et l'archivage ;
- la bonne utilisation des zones de commentaires ;
- le traitement d'appréciations sur des difficultés sociales, d'infractions ou de condamnations, ou encore de données relatives à la santé.

Le secteur des collectivités locales

Un premier volet a été traité en 2013, s'agissant des traitements de données dans le cadre de la prévention de la délinquance.

Les travaux ont consisté à réaliser des « visites sur place » et des auditions téléphoniques auprès des différentes structures concernées, au niveau local, départemental et national : Conseil local de sécurité et de prévention de la délinquance (CLSPD) et ses sous-groupes, Conseil des droits et devoirs des familles (CDDF), groupe de zone de sécurité prioritaire (ZSP), ainsi que d'autres structures créées par les collectivités.

L'objectif était de connaître les **besoins des acteurs de terrain** qui mettent localement en œuvre une politique nationale. Ces visites et auditions ont été révélatrices de la disparité tant des pratiques que de l'application des textes par les municipalités.

En parallèle, la CNIL a été sollicitée par le CIPD (Comité interministériel de prévention de la délinquance). Elle participe au groupe de travail mensuel sur l'échange d'informations dans le cadre de la prévention de la délinquance, qui envisage courant 2014 la rédaction d'une charte et d'un guide pratique.

Dans le cadre de ces travaux, la CNIL a des contacts avec le comité éthique du Conseil supérieur des travailleurs sociaux pour évoquer l'étendue des échanges d'information et de leurs éventuels traitements ainsi qu'avec les ministères de l'Intérieur, de la Justice, et de la Ville.

Courant 2014, la CNIL examinera un projet d'autorisation unique pour « le suivi des personnes faisant l'objet de mesures dans le cadre des politiques de prévention de la délinquance gérées par le maire ».

Si tous les secteurs d'activité ont vocation à être concernés par cette démarche, le déploiement progressif de ces outils concernera en 2014 le pack collectivités locales qu'il est prévu de compléter, le secteur bancaire, le secteur social et médico-social. ■

PROTÉGER LES CITOYENS

VERS UNE STABILISATION DU NOMBRE DE PLAINTES

5640
PLAINTES EN 2013

Le nombre de plaintes reçues pour non-respect de la loi « Informatique et Libertés » se stabilise en 2013. Cette évolution s'explique par la mise en ligne sur le site de la CNIL des fiches pratiques qui permettent aux personnes et aux organismes de désamorcer en amont des situations qui auparavant auraient généré des plaintes à la CNIL. Il s'agit par exemple des fiches « travail » et « vidéosurveillance / vidéoprotection », qui, cumulées, ont été téléchargées plus de 100 000 fois. De plus, la CNIL a modifié son mode de fonctionnement interne afin d'accélérer le traitement de demandes relatives aux modalités d'exercice des droits, qui ne sont plus qualifiées en tant que telles de plaintes. Il en est de même lorsque la CNIL réoriente les usagers vers les autres organismes dont la saisine ne relève pas de la loi Informatique et Libertés (escroquerie, litige commercial, etc.).

Quasiment la moitié des plaintes reçues sont adressées *via* le service de « plainte en ligne » accessible depuis le site de la CNIL (www.cnil.fr). Un élargissement de ce service est prévu en 2014.

▸ Les plaintes du secteur **d'Internet/Télécom** représentent **34 %** des demandes adressées à la CNIL. **Les demandes concernent souvent le droit d'opposition et la maîtrise par les internautes de leur e-réputation** : suppression d'un compte créé sur un réseau social, de photographies ou de vidéos, de commentaires ou encore de coordonnées, déréférencements par les moteurs de recherche, faux profils… Face à la pratique de plus en plus étendue de rechercher des personnes sur les moteurs de recherche, la maîtrise de son « e-réputation » (ce qui est diffusé sur soi sur les réseaux sociaux, les blogs, les sites web…) est un enjeu essentiel.

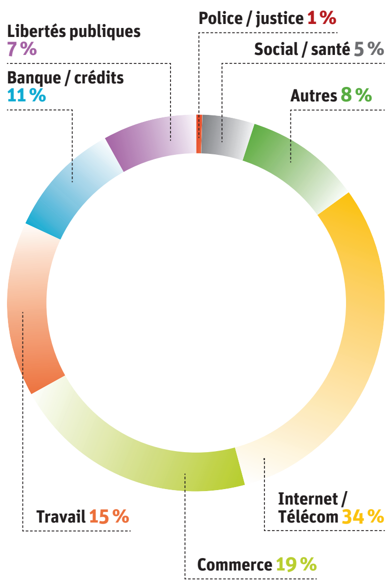
Un nombre important de plaintes porte sur la réutilisation de données publiquement accessibles sur Internet rediffusées sur d'autres sites à d'autres fins. Une préoccupation montante concerne le devenir des données des personnes décédées en particulier sur leur compte Facebook.

▸ Le secteur du **commerce** représente **19 %** des plaintes reçues (radiation de fichiers publicitaires, conservation des coordonnées bancaires, gestion des fichiers clients, défaut de confidentialité des données…). Sur l'année 2013, **l'opposition à recevoir des courriels publicitaires** (signal spam) est le principal motif de saisine de la CNIL, par ordre décroissant, viennent ensuite les sollicitations par téléphone et les publicités postales.

Les plaintes de ce secteur reflètent aussi les inquiétudes des clients face aux pratiques des sites marchands s'agissant tant de la mise en place de fichiers de lutte contre la fraude que de la conservation de leurs coordonnées bancaires.

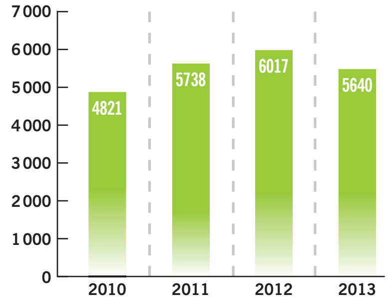
▸ Un nombre important de plaintes concerne le secteur du **travail** (**15 %**).

Répartition des plaintes par secteur



Les demandes émanent généralement de salariés ou de syndicats. Elles portent souvent sur la légitimité des fichiers et des dispositifs de contrôle mis en œuvre (vidéosurveillance, géolocalisation des véhicules, cybersurveillance), sur l'absence d'information des salariés et sur les difficultés rencontrées dans l'exercice du droit d'accès au dossier professionnel.

Nombre de plaintes reçues par la CNIL entre 2010 et 2013



> Le principal motif de plainte est l'exercice du droit d'opposition à figurer dans un fichier ou l'exercice du droit d'accès, qui est l'une des composantes du « droit à l'oubli ».

... HISTOIRES VÉCUES

Aurélie découvre qu'un faux profil associé à une fausse adresse électronique a été créé à ses nom et prénom. Elle saisit la CNIL. Afin d'obtenir la suppression du profil et du compte concernés, la CNIL lui conseille, dans un premier temps, d'exercer son droit d'opposition directement auprès des responsables du site et de la messagerie électronique, et de conserver des justificatifs de ses demandes. En effet, la CNIL intervient uniquement dans un second temps, si ses demandes ne sont pas prises en compte. La CNIL l'informe qu'elle peut aussi déposer plainte pour usurpation d'identité auprès du commissariat, de la gendarmerie ou du procureur de la République.

Samuel, qui était en poste mais envisageait de changer d'employeur, s'est inscrit auprès d'un cabinet de recrutement. À la suite d'un entretien, le cabinet a communiqué à son employeur actuel (qui ignorait les démarches de Samuel) le compte rendu détaillé de son entretien d'embauche, alors même que la charte de déontologie du cabinet de recrutement interdit de transmettre à des tiers les CV ou les références des candidats sans leur accord. La CNIL a adressé un courrier au cabinet afin de lui rappeler son obligation en matière de sécurité et de confidentialité des informations qu'il détient sur les candidats. La société a effectué une campagne d'information auprès de ses collaborateurs afin de leur rappeler l'interdiction de diffuser des informations relatives aux candidats sans leur consentement.

Jérémy découvre à l'occasion d'une demande de prêt à la consommation qu'il est toujours inscrit au FICP (Fichier des incidents de remboursement des crédits aux particuliers) par son ancienne banque alors qu'il est certain d'avoir réglé son découvert bancaire. Les banques doivent demander la radiation de l'inscription auprès de la Banque de France dès que l'incident de paiement est intégralement remboursé. La CNIL a adressé un courrier à cette banque afin de connaître les raisons du maintien de l'inscription du client. L'établissement financier a reconnu avoir omis de faire le nécessaire dans le délai légal et a donc procédé au « défichage » de Jérémy.

Madame E. a saisi la CNIL car elle n'arrivait pas à obtenir la copie de son dossier d'allocataire auprès de la CAF, et ce, malgré plusieurs demandes. La CNIL a adressé un courrier à l'organisme ainsi qu'au correspondant Informatique et Libertés (CIL) pour lui rappeler ses obligations en matière de droit d'accès des allocataires. Le CIL de la Caisse nationale des allocations familiales est alors intervenu auprès de la CAF concernée pour qu'une réponse soit adressée à Madame E., ce qui a été fait quelques jours plus tard. À la suite de cette plainte, le CIL s'est également engagé à effectuer un rappel des droits des allocataires en matière de droit d'accès auprès des directeurs des CAF.

11 % des plaintes concernent le secteur **banque/crédit**. Le principal motif de plainte est la contestation de l'inscription dans l'un des fichiers de la banque de France (Fichier national des Incidents de remboursement des Crédits aux Particuliers, Fichier central des chèques...)

Les plaintes relatives aux **libertés publiques et aux collectivités locales** (**7 %**) demeurent importantes, elles sont pour partie liées à l'actualité politique et aux scrutins organisés (élections, presse en ligne, mise en ligne de documents publics par les collectivités...).

Le devenir des données personnelles des personnes décédées sur les réseaux sociaux

Les personnes interrogent souvent la CNIL afin de savoir s'il est possible d'accéder au compte Facebook d'un membre de leur famille décédé ou de faire fermer le compte. Facebook affecte un statut spécial au compte du défunt qui peut soit être transformé en compte de commémoration, soit être supprimé. La procédure de demande de suppression de compte est réservée à la famille proche du défunt et à ses ayants droit, sous réserve de présenter un justificatif du lien de parenté ou une copie du testament.

Toutefois, les dispositions de la loi « Informatique et Libertés » ne permettent pas à la famille du défunt d'avoir accès aux données contenues sur le compte. En effet, le droit d'accès conféré aux personnes (art. 39) est un droit personnel, qui ne se transmet pas aux héritiers. La seule possibilité ouverte aux ayants droit par la loi « Informatique et Libertés » est la mise à jour des données (article 40).

Ils peuvent donc exiger du responsable du réseau social qu'il prenne en compte le décès du proche dans ses fichiers. Enfin, les comptes inactifs sont en principe effacés. ■

LE DROIT D'ACCÈS INDIRECT : MAINTIEN D'UNE FORTE CROISSANCE DES DEMANDES

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

4305 personnes se sont adressées à la CNIL en 2013 pour exercer leur droit d'accès indirect, ce qui représente **une** ▸▸▸

INFOS +

Le droit d'accès indirect, comment ça marche ?

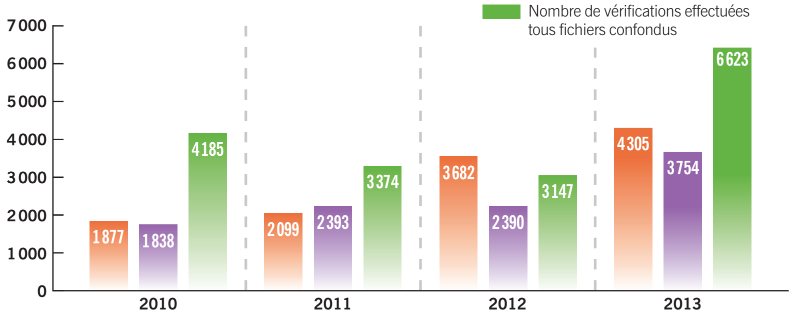
Une fois reçue la demande accompagnée d'une copie d'un titre d'identité, un magistrat de la CNIL appartenant ou ayant appartenu au Conseil d'État, à la Cour de Cassation ou à la Cour des Comptes est alors désigné pour mener les investigations utiles et faire procéder, le cas échéant, aux modifications 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.

4 305

DEMANDES DE DROIT D'ACCÈS INDIRECT

SOIT + 17 % PAR RAPPORT À 2012

Évolution des demandes de droit d'accès indirect 2010-2013



▸▸▸

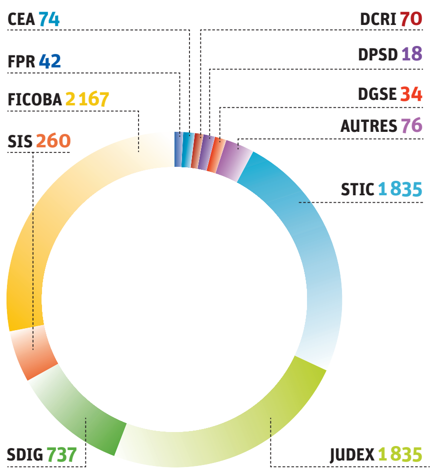
augmentation de 17% par rapport à 2012, année qui avait été marquée par une importante progression (+ 75 %) liée principalement aux sollicitations portant sur le fichier FICOBA de l'administration fiscale dans le cadre du règlement de successions.

Chaque demande de droit d'accès indirect implique, à titre général, des vérifications dans plusieurs fichiers afin de répondre à l'ensemble des attentes de la personne concernée. Ainsi, **les 4 305 demandes reçues au cours de l'année 2013 représentent un total de 7 148 vérifications** à mener qui concernent, au premier rang, le fichier FICOBA ainsi que les fichiers d'antécédents judiciaires de la police et de la gendarmerie nationales (*Système de traitement des infractions constatées (STIC) de la police et Système judiciaire de documentation et d'exploitation (JUDEX) de la gendarmerie*) fusionné au sein d'un fichier unique au 1er janvier 2014 : le Traitement des antécédents judiciaires (TAJ).

44 % des vérifications menées en 2013 ont porté sur les fichiers d'antécédents judicaires. Leurs résultats démontrent toute l'importance de l'action de la Commission pour assurer la mise à jour de ces fichiers et confortent le sens des recommandations émises au terme de son deuxième rapport de contrôle en date du 13 juin 2013.

Dans environ 45 % des dossiers de personnes « mises en cause » examinés par un magistrat de la Commission, la personne a ainsi pu bénéficier soit de l'effacement pur et simple de son enregistrement, soit d'un ajout de mention pour l'ensemble des faits la concernant (article 230-8 du code de procédure pénale) qui, tout en la maintenant dans le fichier, a néanmoins pour effet de l'en rendre inconnue sous son mode de consultation administrative (enquêtes menées pour la délivrance d'une carte professionnelle, d'une autorisation d'accès à certains sites sensibles, de la nationalité française ou d'un titre de séjour...). ■

Demandes de droit d'accès indirect 2013 : répartition par fichiers des vérifications à effectuer



FICOBA : Fichier des comptes bancaires et assimilés / STIC : Système de traitement des infractions constatées / SDIG : Services de l'information générale du ministère de l'intérieur / JUDEX : Système judiciaire de documentation et d'exploitation / SIS : Système d'information Schengen / FPR : Fichier des personnes recherchées / CEA : Direction centrale de la sécurité du commissariat à l'énergie atomique / DCRI : Direction centrale du renseignement intérieur / DGSE : Direction générale de la sécurité extérieure / DPSD : Direction de la protection de la sécurité de la défense / Autres : Fichier des courses et jeux (FICOJ), Fichier des interdits de stades (FNIS), Système de gestion informatisée des détenus en établissement pénitentiaire (GIDE), Europol...

Principaux résultats des vérifications des fichiers STIC et JUDEX effectuées en 2013

	STIC	JUDEX
Nombre de vérifications individuelles effectuées	1144	1756
Nombre de personnes inconnues	318	1385
Nombre de personnes enregistrées uniquement en tant que victimes	223	113
Nombre de fiches de personnes « mises en cause » vérifiées	603	258
dont nombre de fiches supprimées	21 %	17 %
dont nombre de fiches mises à jour par mention de la décision judiciaire favorable intervenue (classement sans suite, non-lieu, relaxe…) rendant la personne inconnue du fichier sous profil de consultation administrative (enquêtes administratives)	26 %	29 %
dont nombre de fiches rectifiées ayant eu pour effet de réduire le délai global de conservation de l'enregistrement	< 1 %	< 1 %
dont nombre de fiches examinées avec maintien de l'enregistrement de la personne (fiches exactes, rectifications mineures sans incidence sur la durée de conservation, défaut de réponse des parquets sur les suites judiciaires intervenues)	52 %	53 %

FOCUS

Vers la reconnaissance légale du droit pour les notaires d'obtenir directement, auprès de l'administration fiscale, les données FICOBA nécessaires au règlement des successions ?

Le nombre important de demandes relatives au fichier FICOBA dont la Commission est destinataire, qui induit actuellement un délai moyen de traitement de l'ordre de plusieurs mois, est lié au fait que l'exercice de ce droit constitue la seule faculté pour les héritiers et les notaires agissant en leur nom, d'obtenir un recensement des comptes bancaires dans le cadre du règlement des successions.
En effet, les notaires ne disposent pas, à la différence d'autres professionnels tels que les huissiers de justice ou les officiers de police judiciaire, de la qualité de « tiers autorisé » qui leur conférerait la possibilité de solliciter directement l'administration fiscale pour obtenir les données, issues de ce fichier, qui leur sont nécessaires à cette fin.
Sur la base d'un rapport de la Cour des Comptes sur les avoirs bancaires et assurances-vie en déshérence, publié en juillet 2013, et d'une mission d'information parlementaire sur le même sujet, une proposition de loi a été déposée le 13 novembre 2013 à l'Assemblée Nationale, qui prévoit l'instauration non seulement d'un droit, mais aussi d'une obligation pour les notaires de consulter le fichier FICOBA pour le règlement des successions.
Si cette évolution législative devait être entérinée par le Parlement, le droit d'accès indirect ne serait plus la voie exclusive d'accès à ce fichier.

LES RECOURS JURIDICTIONNELS EN MATIÈRE DE DROIT D'ACCÈS INDIRECT : LA COMPÉTENCE DU TRIBUNAL ADMINISTRATIF EN PREMIER RESSORT

L'exercice du droit d'accès indirect n'emporte pas pour la personne un droit à communication des données la concernant enregistrées dans les fichiers qui y sont soumis. Conformément aux dispositions combinées de l'article 41 de la loi du 6 janvier 1978 et de l'article 88 de son décret d'application, en cas d'opposition de l'administration gestionnaire, la CNIL est tenue de se limiter à indiquer à la personne que les vérifications ont été réalisées, sans lui apporter de plus amples précisions, hormis l'indication des voies de recours qui lui sont ouvertes pour contester ce refus.

Si, conformément à l'article R 311-1 alinéa 4 du Code de justice administrative (CJA), le Conseil d'État est compétent pour connaître en premier et dernier ressort des recours dirigés contre les décisions prises par la Commission au titre de ses missions de contrôle et de régulation, tel n'est pas le cas en matière de droit d'accès indirect. C'est à ce titre que le Conseil d'État a été appelé à confirmer, à plusieurs reprises en 2013, qu'il était incompétent « pour juger en premier et dernier ressort, dès lors que la lettre de la présidente de la CNIL apparaît comme la simple transmission de la décision du ministre [responsable du fichier] dont le contentieux relève, en premier ressort, de la compétence du Tribunal Administratif ».

Aussi, les personnes souhaitant contester le refus de communication des données les concernant, doivent dans les deux mois à compter de la date de réception de la lettre de la CNIL, engager un recours contre le ministère à l'origine de ce refus devant le tribunal administratif du ressort duquel il dépend, en l'occurrence celui de Paris (article R 312-1 du code de justice administrative). ■

CONTRÔLER ET SANCTIONNER

LA MISE EN CONFORMITÉ : OBJECTIF PREMIER

Les plaintes

Ces trois dernières années la CNIL a reçu chaque année entre 5000 et 6000 plaintes émanant principalement de particuliers, de représentants du personnel ou d'associations de consommateurs. Dans une très large mesure, l'instruction d'une plainte se déroule par échanges de courriers avec l'organisme mis en cause. En effet, au vu des faits décrits par le plaignant, la CNIL interroge l'organisme et lui rappelle les différentes dispositions légales qu'il doit respecter. Ces courriers suffisent la plupart du temps pour que l'organisme se mette en conformité (c'est le cas de 99% des plaintes instruites en 2013).

Une fois en possession des éléments lui permettant de s'assurer que l'organisme s'est mis en conformité (copie du document d'information, formulaire de déclaration, etc.) la CNIL procède alors à la clôture du dossier et en informe le plaignant.

Exemple de la vidéosurveillance : la CNIL a obtenu la mise en conformité de nombreux dispositifs de vidéosurveillance par des organismes qui, après réception de son courrier, ont procédé à l'information des salariés et effectué les formalités préalables adéquates.

La décision de contrôle

Néanmoins, il peut arriver soit que l'organisme mis en cause ne réponde pas aux demandes de la CNIL, soit que ses réponses soient partielles ou insatisfaisantes. Dans ces hypothèses, la Présidente de la Commission peut décider de procéder à un contrôle dans les locaux de l'organisme concerné.

C'est pourquoi plus d'un tiers des contrôles effectués par la CNIL en 2013, résultent de plaintes (plaintes datant de 2011, 2012 et 2013), toutes problématiques confondues. Notons qu'il peut également arriver que des plaintes donnent directement lieu à un contrôle sur place, sans échange préalable avec l'organisme ; il s'agit de cas rares, le plus souvent liés à des manquements graves, et nécessitant une action rapide sur le terrain. C'est par exemple le cas des failles de sécurité, qui compromettent de manière importante la confidentialité des données.

Exemple de la vidéosurveillance : des délégations de la CNIL se sont rendues à plusieurs reprises en 2013 auprès d'organismes mettant en œuvre des dispositifs de vidéosurveillance afin de vérifier les modalités d'information des salariés, l'orientation des caméras, la sécurisation des images et leur durée de conservation.

Les suites du contrôle : 89 % de mises en conformité

S'agissant des suites données aux contrôles, elles sont déterminées sur le fondement de nombreux critères. Ainsi, il est tenu compte du nombre et de la nature des manquements, ainsi que de la volonté affichée de l'organisme de se mettre ou non en conformité.

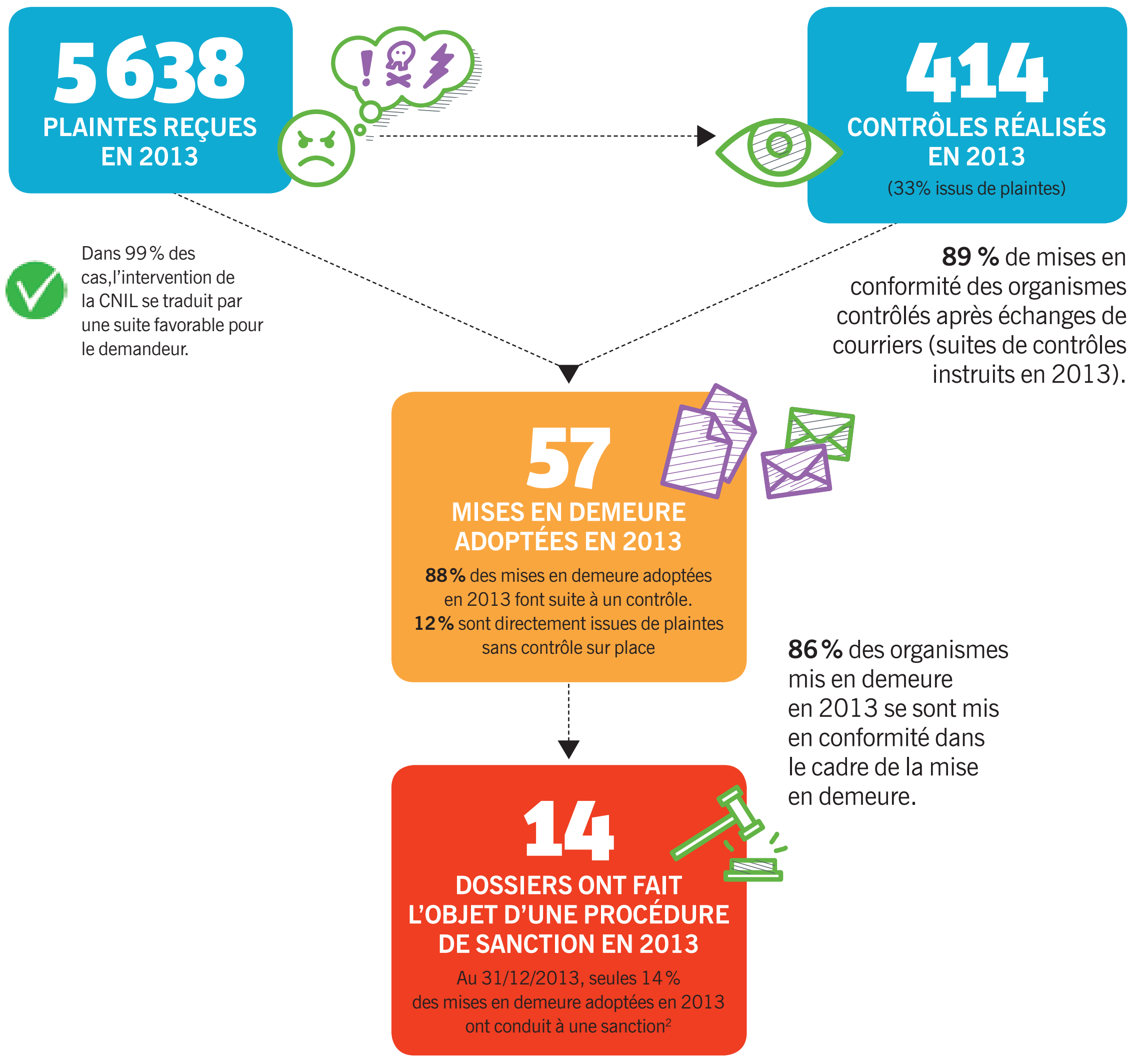
Dans l'hypothèse où le contrôle ne révèle aucun manquement, un courrier est adressé à l'organisme l'informant de la clôture de la procédure. Si des manquements relativement mineurs sont constatés, un courrier d'observation est alors envoyé demandant d'adopter les mesures permettant de se mettre en conformité (89% des contrôles dont les suites ont été instruites en 2013 se sont soldés par un courrier de clôture ou d'observation). L'instruction menée ici est assez similaire à celle d'une plainte : soit l'organisme se met en conformité et en apporte la preuve, soit il ne répond pas ou de manière insatisfaisante et il peut être alors proposé à la Présidente de la CNIL d'adopter une mise en demeure.

Les mises en demeure

En 2013, la Présidente de la CNIL a procédé à 57 mises en demeure. En pratique, la mise en demeure consiste en une décision qui énumère précisément les manquements reprochés à l'organisme ainsi que les mesures qu'il doit prendre pour se mettre en conformité. Le délai laissé à l'organisme varie entre 10 jours et 3 mois (renouvelable une fois), en fonction notamment de la complexité des mesures qu'il doit mettre en œuvre.

Là encore, les modalités d'instruction du dossier sont relativement similaires à ce qui est pratiqué pour les suites de plaintes ou de contrôles : soit l'organisme se met en conformité et en apporte la preuve, soit ses réponses sont insatisfaisantes et une procédure de sanction est engagée. À cet égard, il est à noter que dans 86% des mises en demeure dont les suites ont été instruites en 2013, les organismes se sont mis en conformité dans le cadre de la mise en demeure, après réception de la décision de la Présidente.

> Le pilotage de la conformité est au cœur des métiers de la CNIL.



Exemple de la vidéosurveillance : en 2013, la Présidente a mis en demeure 10 organismes sur cette thématique. Il s'agissait notamment de réorienter des caméras qui filmaient les lieux de pause des salariés, d'effacer des images conservées au-delà de 30 jours sans justification particulière et de sécuriser l'accès aux serveurs dans lesquels étaient stockées les images.

La procédure de sanction

Si une procédure de sanction est engagée, la Présidente désigne un rapporteur parmi les 11 commissaires[1] de la Commission à même de rapporter le dossier devant la formation restreinte, qui est composée de 5 membres et d'un Président distinct de la Présidente de la CNIL. Cette formation peut prononcer diverses sanctions à l'égard des organismes qui ne respectent pas la loi à l'issue d'une procédure contradictoire. En 2013, la formation restreinte a examiné 14 dossiers de sanction.

On relèvera ici que l'engagement d'une procédure de sanction ne nécessite pas toujours l'adoption au préalable d'une mise en demeure. En effet, la formation restreinte de la CNIL peut prononcer des avertissements, publics ou non publics, qui ne font pas suite à une mise en demeure demeurée infructueuse. Le plus souvent, la voie de l'avertissement est retenue pour des manquements passés, qui ont été corrigés par l'organisme en cause (cas d'une faille de sécurité par exemple).

Ainsi, apparaît-il clairement que la logique de la loi et de son application par la CNIL visent à la mise en conformité des organismes. Le processus mis en œuvre leur offre à plusieurs reprises cette possibilité, sachant qu'à chaque phase d'instruction, il leur est indiqué les mesures à prendre pour faire en sorte que la procédure engagée prenne fin. *In fine*, peu de cas ne sont pas résolus « à l'amiable ». ■

[1] Il faut exclure ici les 6 membres de la CNIL composant la formation restreinte. / [2] Les sanctions prononcées en 2013 ne font pas toutes suites à une mise en demeure adoptée en 2013.

CONTRÔLER

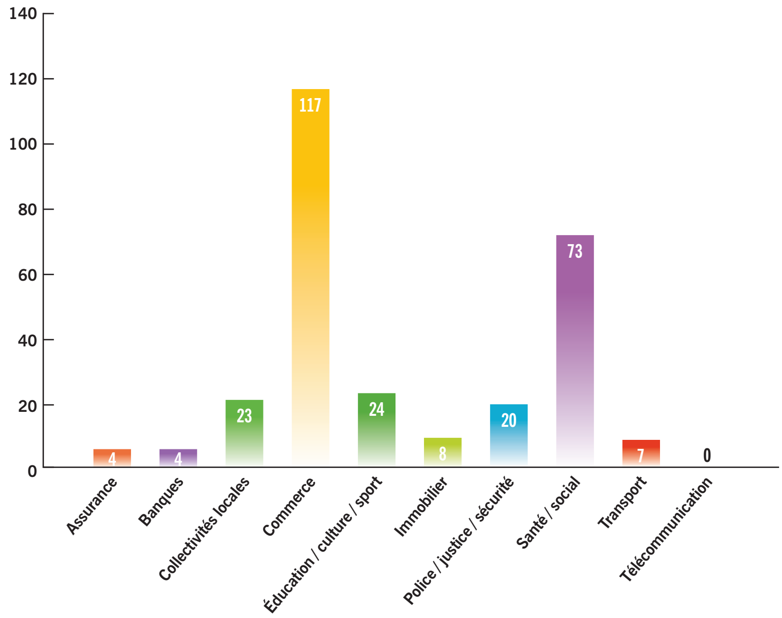
> Grâce aux contrôles, la CNIL est en prise avec la réalité des organismes et peut ainsi penser une régulation consciente des pratiques de terrain.

Avec 414 contrôles réalisés en 2013, le volume des vérifications effectuées sur place par la CNIL reste stable par rapport à l'année précédente. L'équilibre dans la répartition des contrôles est aussi respecté puisque 67 % des vérifications concernent des dispositifs relevant de la loi « Informatique et Libertés » et 33 % portent sur des systèmes vidéo. L'originalité de cette année réside dans les premiers audits en ligne menés par la CNIL qui préfigurent une évolution de son action.

Bilan des contrôles « Informatique et Libertés »

S'agissant des contrôles effectués sur des traitements relevant de la loi « Informatique et Libertés », **75 % d'entre eux ont été réalisés dans le secteur privé et 25 % dans le secteur public**. Dans 33 % des cas, ces missions de vérification ont été effectuées à la suite d'une plainte, l'objectif étant d'attester – ou non – les faits dénoncés par le plaignant. La CNIL a également procédé à des contrôles de sa propre initiative à hauteur de 27 % : il s'agit de vérifications en lien avec l'actualité ou l'innovation technologique. Une délégation de la Commission peut ainsi être envoyée auprès d'un organisme dont un article de presse révèle qu'il met en œuvre un fichier d'importance ou qu'il utilise un dispositif qui peut poser problème au regard de la loi. Des contrôles sont également réalisés à la suite de sanctions ou d'une première mission de vérification sur place. En 2013, 16 % des contrôles ont ainsi visé à s'assurer que des organismes déjà contrôlés ou sanctionnés avaient respecté leurs engagements et s'étaient mis en conformité avec la loi. Enfin, 24 % des investigations se sont inscrites dans le cadre du programme annuel des contrôles. En effet, chaque année la Commission choisit des thématiques

Répartition des contrôles Informatiques et Libertés par secteur d'activité (nombre de contrôles)



FOCUS

L'opération « *Internet Sweep Day* » : une première dans la coopération internationale

Au cours du mois de mai 2013, la CNIL et 18 autres autorités de protection des données ont évalué les sites Internet les plus visités dans leur pays respectif. C'est la première fois que la CNIL menait des audits en ligne. Au total, elle a examiné 250 sites concernant la qualité de l'information délivrée aux personnes sur les conditions de traitement de leurs données personnelles.

À cette occasion elle a notamment constaté que :

- **moins de 10 % seulement des sites web audités ne fournissent pas d'information sur leur politique de protection des données ;**
- **dans 50 % des cas, l'information n'est pas facilement accessible ;**
- **dans un tiers des cas, l'information n'est pas suffisamment claire et compréhensible.**

Les sites dont les mentions d'information étaient insuffisantes ont été invités à se mettre en conformité.

sur lesquelles elle estime nécessaire de connaître « la pratique du terrain », dans le but le plus souvent d'émettre des préconisations d'ensemble pour le secteur ou les acteurs concernés. Pour rappel, en 2013 le programme annuel était structuré autour des thèmes suivants :

- **Le traitement des données par les instituts de sondage** : la CNIL a procédé en 2013 à 8 contrôles auprès des organismes ayant une notoriété importante et/ou une expertise particulière. Les constatations effectuées ont permis d'observer les pratiques du secteur et de comprendre son fonctionnement. Les propositions de la CNIL pour parvenir à une réglementation pragmatique et respectueuse de la vie privée seront faites en 2014.
- **Les données traitées dans le cadre de l'Internet en libre accès** : les contrôles ont été menés auprès de 22 organismes et ont eu pour objet de vérifier si le cadre juridique relatif au traitement des données des utilisateurs était respecté. Les vérifications effectuées n'ont pas conduit à constater de manquements majeurs à la loi. La CNIL a néanmoins procédé à des rappels sur la nécessité d'informer les personnes, de procéder aux formalités préalables et d'appliquer des durées de conservation limitées aux données.
- **Le traitement par les collectivités locales des données relatives aux difficultés sociales des personnes** : l'objectif était de disposer d'une vue d'ensemble des pratiques des collectivités concernant la prise en charge sociale des personnes. La CNIL a ainsi réalisé 22 contrôles auprès de communes et de leur CCAS, choisies en fonction du nombre d'habitants, de leur situation socio-économique et de leur implantation géographique afin de disposer d'un panel représentatif. Ces derniers n'ont pas mis en évidence de manquements d'une particulière gravité. Néanmoins, il est apparu nécessaire de développer des outils de mise en conformité afin d'accompagner ces organismes, notamment concernant la sécurisation des systèmes d'information.

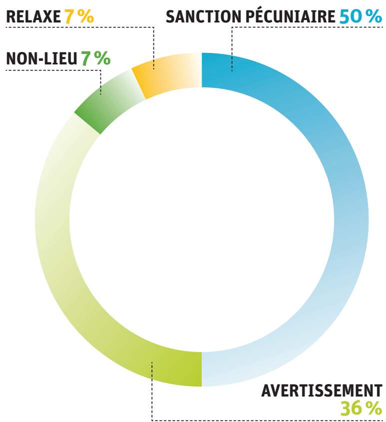
Le programme annuel 2013 prévoyait également la réalisation de vérifications concernant « ***les données des personnes détenues en établissements pénitentiaires*** ». Les contrôles sur cette thématique ont débuté fin 2013 et les conclusions sont attendues courant 2014. ■

INFOS +

Un pouvoir d'investigation renforcé grâce aux contrôles en ligne

La loi du 17 mars 2014 relative à la consommation donne à la CNIL la possibilité de procéder à des contrôles en ligne, lui permettant de constater à distance, depuis un ordinateur connecté à Internet, des manquements à la loi Informatique et Libertés. Ces constatations seront relevées dans un procès verbal adressé aux organismes concernés et leur seront opposables.
Cette modification crée les conditions juridiques qui permettent d'adapter le pouvoir d'investigation de la CNIL au développement numérique.
Elle lui offre l'opportunité d'être plus efficace et réactive dans un univers en constante évolution. La Commission pourra ainsi rapidement constater et agir en cas de failles de sécurité sur Internet. Elle pourra aussi vérifier la conformité des mentions d'information figurant sur les formulaires en ligne, ou des modalités de recueil de consentement des internautes en matière de prospection électronique.

Les sanctions prononcées en 2013



SANCTIONNER

Durant l'année 2013, la Présidente de la CNIL a adopté 57 mises en demeure dont 4 ont été rendues publiques, et 8 concernaient des manquements relatifs à la vidéoprotection pour lesquels la Commission ne peut prononcer de sanction.

Ces mises en demeure ont des origines diverses. Ainsi, 35 mises en demeure ont été adoptées à la suite d'un contrôle sur place, 15 mises en demeure faisaient ▸▸▸

57 MISES EN DEMEURE

14 PROPOSITIONS DE SANCTION

7 SANCTIONS PÉCUNIAIRES DONT 6 PUBLIQUES

5 AVERTISSEMENTS DONT 2 PUBLICS

1 RELAXE

1 NON-LIEU

suite à une plainte assortie d'un contrôle, et 7 mises en demeure étaient uniquement fondées sur une plainte.

En 2013, 86 % des mises en demeure adoptées ont donné lieu à une mise en conformité et ont été clôturées dans un délai d'instruction moyen de 5 mois. Une fois encore, l'année 2013 est marquée par l'efficacité de cet outil.

Cette stratégie d'accompagnement dans un délai déterminé explique le nombre peu élevé de sanctions prononcées par la formation restreinte.

En effet, 14 propositions de sanctions ont été examinées par la formation restreinte. Sur les 49 mises en demeure adoptées (hors vidéoprotection) susceptibles d'être soumises à la formation restreinte en cas de non mise en conformité, 7 sanctions pécuniaires (dont 6 publiques), 1 relaxe et 1 non-lieu ont été adoptés.

En outre, 5 avertissements dont 2 publics ont également été directement prononcés par la formation restreinte, cette sanction n'étant pas soumise à mise en demeure préalable. La plupart du temps, il s'agit de manquements qui, bien que révolus au jour du contrôle ou de la saisine de la Commission, nécessitent, au regard de leur gravité ou de la négligence dont a fait preuve le responsable de traitement, le prononcé d'une sanction par la formation restreinte pour alerter l'organisme ou le public concerné. ■

FOCUS

La mise en demeure publique contre Google du 10 juin 2013

Le 10 juin 2013, la Présidente de la CNIL a adopté une mise en demeure à l'encontre de la société Google Inc. Le bureau de la CNIL (la Présidente et les deux vice-présidents) a décidé de rendre publique cette décision en raison notamment du statut et de la taille de l'organisme en cause, et du nombre de personnes concernées par ses traitements. En effet, la société occupe la position de leader mondial sur le marché de la recherche d'information sur Internet et de la fourniture de services associés, lesquels sont utilisés par plusieurs millions d'internautes français.

Cette mise en demeure fait suite à la décision de Google Inc. de fusionner en une seule politique les différentes règles de confidentialité applicables à une soixantaine de ses services. Préalablement à cette action française, le « G29 », le groupe des CNIL européennes, avait vainement enjoint à la société de se conformer au cadre juridique européen relatif à la protection des données personnelles.

Dans sa décision, la Présidente de la CNIL a notamment retenu que Google Inc. n'informait pas suffisamment ses utilisateurs sur les conditions dans lesquelles étaient collectées leurs données personnelles. En pratique, la société ne permet pas à ses utilisateurs de comprendre les finalités de la collecte de données ni d'exercer les droits qu'ils détiennent au titre de la loi « Informatique et Libertés », et notamment leurs droits d'accès, d'opposition ou d'effacement.

Il a également été reproché à la société, au terme d'un contrôle de proportionnalité entre, d'une part, son intérêt légitime et, d'autre part, les droits et intérêts des internautes, de ne pas avoir recueilli le consentement des utilisateurs avant de procéder à la combinaison de leurs données. La Présidente a en effet retenu que l'ampleur et le caractère massif de la combinaison de données étaient susceptibles de méconnaître le droit des utilisateurs au respect de leur vie privée.

D'autres manquements relatifs à l'obligation de fixer une durée de conservation des données collectées ou encore d'informer les utilisateurs avant le dépôt de cookies sur leur terminal de connexion ont également été retenus.

INFOS +

Mise à jour 2014

Dans la mesure où la société ne s'est pas mise en conformité avec les prescriptions de la mise en demeure, une procédure de sanction a été engagée.

Le 3 janvier 2014, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 150 000 euros à l'encontre de la société GOOGLE Inc., estimant que les règles de confidentialité mises en œuvre par celle-ci depuis le 1er mars 2012 n'étaient pas conformes à la loi « Informatique et Libertés ». Elle a enjoint à Google de procéder à la publication d'un communiqué relatif à cette décision sur www.google.fr.

Le 14 janvier 2014, la société Google a sollicité la suspension partielle de la délibération de sanction rendue à son encontre par la formation restreinte de la CNIL le 3 janvier. Le juge des référés du Conseil d'État a rejeté cette demande par ordonnance en date du 7 février 2014. Google a donc procédé à la publication d'un bandeau sur www.google.fr faisant état de la sanction de la CNIL pendant 48 heures, les 8 et 9 février.

Liste des sanctions prononcées en 2013

Date	Nom ou type d'organisme	Décision adoptée	Manquement principal	Thème
10/01/2013	FÉDÉRATION SPORTIVE	Avertissement non public	Défaut de formalités préalables, inadéquation, non pertinence et caractère excessif, défaut de définition d'une durée de conservation, défaut d'information, défaut de sécurité	Gestion des licenciés, liste d'exclusion, vidéosurveillance
11/04/2013	TOTAL RAFFINAGE MARKETING*	Avertissement public	Défaut de sécurité des données	Vote électronique
30/05/2013	PS CONSULTING*	Sanction pécuniaire publique de 10 000 euros	Inadéquation, non pertinence et caractère excessif des données, défaut d'information, défaut de sécurité	Vidéosurveillance
28/03/2013	ADMINISTRATION	Avertissement non public	Défaut de coopération avec la CNIL, formalité préalable incomplète	Formalités préalables et coopération
19/06/2013	BNP PARIBAS	Avertissement public	Défaut de mise à jour des données	Maintien d'inscription au FICP malgré la régularisation de situation
19/06/2013	ÉTABLISSEMENT PUBLIC	Avertissement non public	Incompatibilité des données traitées et finalité du traitement, défaut de sécurité des données	Vote électronique
18/07/2013	ADMINISTRATION	Relaxe	Incompatibilité des données traitées et finalité du traitement	Sport/police
24/10/2013	AOCT	Sanction pécuniaire publique de 10 000 euros	Défaut de formalités préalables, défaut d'information, non réponse aux demandes de la CNIL	Vidéosurveillance
24/10/2013	NCT	Sanction pécuniaire publique de 10 000 euros	Défaut de formalités préalables, défaut d'information, non réponse aux demandes de la CNIL, défaut de sécurité	Vidéosurveillance
24/10/2013	SOCIÉTÉ	Non lieu	Droit d'accès et non réponse aux demandes de la CNIL	Droit d'accès au dossier personnel
23/11/2013	API	Sanction pécuniaire publique de 3 000 euros	non réponse aux demandes de la CNIL, non respect des engagements pris lors de l'accomplissement des formalités préalables	Géolocalisation
12/12/2013	ASC GROUPE	Sanction pécuniaire publique de 10 000 euros	Défaut de formalités préalables, défaut d'information, non réponse aux demandes de la CNIL	Vidéosurveillance

** recours CE en cours*

GROS PLAN

VIDÉOPROTECTION : BILAN DE TROIS ANS DE CONTRÔLES

Depuis la loi d'orientation et de programmation pour la performance et la sécurité intérieure du 14 mars 2011 (LOPPSI 2), la CNIL est compétente pour contrôler, sur place, les conditions de mise en œuvre des dispositifs dits « de vidéoprotection ». Ces dispositifs, soumis au code de la sécurité intérieure et non à la loi « Informatique et Libertés », sont ceux mis en place sur la voie publique ou dans les lieux ouverts au public (magasins, restaurants, etc.). Par ailleurs, la CNIL exerce depuis de nombreuses années le contrôle des dispositifs vidéo mis en place dans les lieux privés, qui relèvent eux de la loi « Informatique et Libertés ». Après trois années de vérifications sur le terrain, il est aujourd'hui possible pour la CNIL de dégager les principales conclusions de l'ensemble de ces contrôles.

LA CNIL : UN ACTEUR IMPORTANT ET RECONNU DANS LA MISE EN ŒUVRE DES DISPOSITIFS DE VIDÉOPROTECTION ET DE VIDÉOSURVEILLANCE

La CNIL est devenue un acteur essentiel, et reconnu, de ce secteur.

Cette reconnaissance est issue du résultat de l'investissement de la CNIL en matière de contrôle. En effet, depuis 2011, la CNIL a concentré près d'un tiers de ses contrôles sur ces systèmes, soit plus de 450 sur l'ensemble du territoire national. En particulier, au cours de l'année 2013, **elle a réalisé plus de 130 contrôles**. En tout, ce sont ainsi plusieurs dizaines de milliers de caméras qui ont pu être contrôlées.

La CNIL a également développé une méthodologie précise des contrôles qu'elle effectue afin que les garanties essentielles prévues par la loi (information des personnes, durée de conservation, limitation des zones filmées, sécurité du système, etc.) soient précisément contrôlées, de manière uniforme sur l'ensemble du territoire.

Cette expertise est d'ailleurs parfois sollicitée par les organismes eux-mêmes puisque, comme le leur permet la loi, certains d'entre eux demandent à la CNIL qu'elle effectue un contrôle du système qu'ils mettent en œuvre. Cette démarche de mise en conformité a été adoptée par des acteurs importants (SNCF, RATP, communes) et doit être encouragée.

Enfin, la CNIL est très fréquemment saisie par des salariés qui s'interrogent sur les conditions de mise en œuvre de dispositifs de vidéosurveillance par leur employeur (un peu plus de 300 plaintes). ■

QUELS CONSTATS ?

Tout d'abord, dans plus de la moitié des cas, les systèmes sont composés de plusieurs caméras et relèvent, pour partie, du code de la sécurité intérieure et, pour partie, de la loi «Informatique et Libertés». Si les obligations sont, dans le fond, globalement les mêmes, l'existence d'un double régime juridique est parfois source d'incompréhension pour les responsables concernés.

Par ailleurs, les contrôles effectués au cours de l'année 2013, ont permis de mettre en relief des irrégularités au regard des textes qui encadrent l'utilisation des dispositifs vidéo.

Une absence de formalités préalables

L'application de la loi « Informatique et Libertés » aux caméras filmant les lieux non ouverts au public est relativement ignorée des responsables de traitement, ce qui a conduit la CNIL à constater que près de la moitié des dispositifs n'ont pas fait l'objet de formalités préalables auprès d'elle.

En ce qui concerne les caméras filmant la voie publique ou les lieux ouverts au public, seuls 15% d'entre elles n'avaient pas été autorisés par le préfet territorialement compétent. Néanmoins, la CNIL a constaté à plusieurs reprises que certains des dispositifs n'ont pas fait l'objet d'une demande de renouvellement de leur autorisation préfectorale.

Une information des personnes à améliorer

On peut considérer l'information des personnes comme une des garanties essentielles apportées par la loi, notamment en ce qu'elle permet aux personnes filmées d'exercer, si elles le souhaitent, leur droit d'accès aux images qui les concernent. **Or, dans plus de 30% des cas, la CNIL a pu constater que cette information était soit inexistante soit insuffisante** (par exemple, en ce qu'elle n'indique pas les coordonnées de la personne à contacter pour exercer le droit d'accès).

Des durées de conservation à améliorer

Environ 15% des contrôles ont démontré une durée de conservation des images supérieure à celle autorisée par le préfet pour les dispositifs de vidéoprotection, ou admise par la CNIL pour la vidéosurveillance. Ces résultats sont essentiellement dus à une absence de paramétrage des dispositifs d'enregistrement.

Des mesures de sécurité insatisfaisantes

Dans plus de 30% des cas, les contrôleurs de la CNIL ont relevé des manquements au regard de l'obligation de sécuriser les dispositifs vidéo (accès aux images en temps réel ou accès aux enregistrements). Ces manquements peuvent consister en une mauvaise gestion des mots de passe permettant l'accès au dispositif de visualisation ou d'enregistrement mais peuvent aussi se traduire par un mauvais paramétrage du système qui rend parfois les caméras concernées accessibles depuis Internet.

Des dispositifs parfois trop intrusifs

Le contrôle, par la CNIL, de la proportionnalité d'un dispositif dépend du régime juridique dont il relève.

En ce qui concerne les dispositifs de vidéoprotection, la CNIL vérifie que les zones filmées sont uniquement celles autorisées par l'arrêté préfectoral. Elle porte une attention toute particulière aux dispositifs mis en œuvre par les collectivités locales afin que ceux-ci « ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées » (article L. 251-3 du code de la sécurité intérieure). Au cours de l'année 2013, **la CNIL a ainsi mis en demeure 7 communes** pour ne pas avoir respecté cette disposition essentielle au regard de la protection de la vie privée des personnes vivant sur le territoire communal.

En ce qui concerne les dispositifs de vidéosurveillance, la CNIL exerce un contrôle plus poussé du dispositif qui doit répondre aux exigences de proportionnalité posées par la loi du 6 janvier 1978 modifiée. Ainsi, la CNIL a précisé, notamment dans des fiches pratiques diffusées sur son site Internet, les conditions de mise en œuvre de ces dispositifs afin que ceux-ci ne portent pas atteinte à la vie privée des personnes filmées (les salariés ne doivent pas être filmés de manière permanente, interdiction de filmer l'entrée des habitations…).

Quelles suites ?

D'une manière générale, les organismes souhaitent se conformer aux préconisations qui sont adressées par la CNIL. En effet, les manquements relevés résultent le plus souvent d'une mauvaise connaissance du cadre légal plutôt que de la volonté de mettre en place un dispositif portant atteinte aux droits et libertés des personnes.

Ainsi, l'envoi d'un courrier d'observation est généralement suffisant pour obtenir une mise en conformité du dispositif contrôlé (94% des cas en 2013). Pour autant, en cas de manquement grave ou d'une absence de volonté de la part du responsable de se conformer à la loi, la CNIL peut prononcer une mise en demeure voire une sanction.

Ainsi, en 2013, la présidente de la CNIL a prononcé 8 mises en demeure portant sur les conditions de mise en œuvre de dispositifs de vidéoprotection.

Elle a également prononcé 8 mises en demeure concernant les conditions de mise en œuvre de dispositifs de vidéosurveillance. Les principaux manquements relevés sont relatifs à l'orientation ▸▸▸

> Les manquements relevés résultent le plus souvent d'une mauvaise connaissance du cadre légal.

des caméras, l'information des employés, la sécurité du système et la durée de conservation des images.

Enfin, la CNIL a développé des **outils d'information pédagogiques sur le sujet.** Elle a ainsi mis à disposition du public une série de fiches pratiques sur les conditions à respecter pour mettre en œuvre un dispositif de ce type. Ces fiches ont été téléchargées plusieurs dizaines de milliers de fois l'année dernière. De même, la CNIL a conclu une convention avec l'Association des maires de France, afin de faire connaître à l'ensemble des maires les bonnes pratiques en matière de vidéoprotection sur la voie publique.

Une nécessaire harmonisation des conditions de mise en œuvre des dispositifs de vidéoprotection

La mise en œuvre d'un dispositif de vidéoprotection est soumise à l'accord préalable du préfet territorialement compétent, après avis d'une commission départementale. À l'occasion des contrôles, la CNIL a constaté des divergences entre préfectures concernant les conditions de mise en œuvre des dispositifs de vidéoprotection.

Ainsi, certaines préfectures ont interdit des dispositifs de vidéoprotection dont la mise en œuvre prévoyait un traitement et une conservation des images dans un pays étranger, alors que d'autres préfectures l'ont admis.

La CNIL a également constaté la délivrance d'autorisation de mise en œuvre de dispositifs de vidéoprotection pour des finalités autres que celles prévues par la loi. Ainsi, une préfecture a autorisé un dispositif aux fins de « contrôle du personnel », finalité non prévue par le code de la sécurité intérieure.

Enfin, les contrôles ont permis de constater que certaines préfectures autorisaient la mise en œuvre de dispositifs dans des lieux de restauration, alors que d'autres refusaient, dans des situations similaires, en raison de l'absence de risques particuliers en matière de sécurité.

La CNIL a donc alerté le ministère de l'Intérieur sur la nécessité d'une application homogène des dispositions relatives à la vidéoprotection.

Évolution technique des dispositifs vidéo et conséquences juridiques

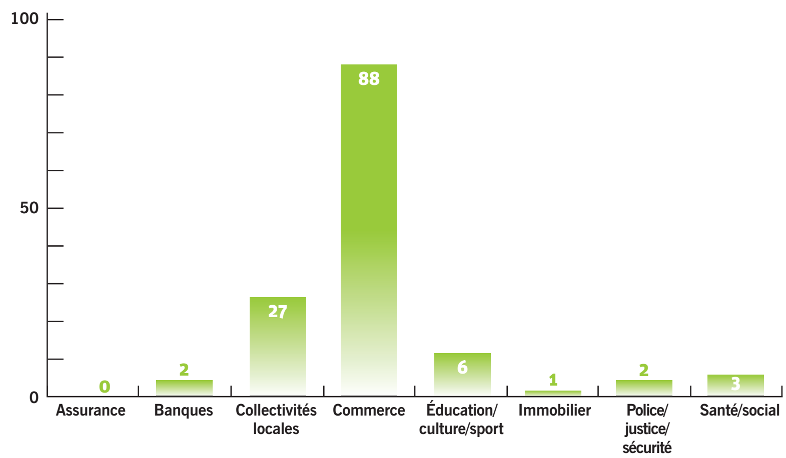
Au-delà de la volonté du législateur d'assurer par une autorité indépendante un contrôle uniforme des dispositifs de vidéoprotection sur l'ensemble du territoire, les contrôles effectués par la CNIL permettent également de constater les évolutions techniques de ces dispositifs qui, pour certaines d'entre elles, conduisent à réfléchir au cadre juridique applicable.

- En premier lieu, la CNIL a constaté que de nombreux dispositifs sont accessibles depuis des smartphones dont la sécurité de l'accès aux images et enregistrements n'est pas toujours assurée.
- En second lieu, de nombreux dispositifs vidéo sont aujourd'hui composés de caméras permettant un enregistrement du son. Or, cette possibilité n'est ni prévue, ni interdite par le code de la sécurité intérieure bien qu'elle pose des questions au regard de la protection de la vie privée des personnes situées dans leur champ de visualisation et donc, d'enregistrement sonore.
- En troisième lieu, la CNIL constate le développement de dispositifs d'enregistrement vidéo embarqués dans l'habitacle de véhicules susceptibles d'être occupés par le public (taxi, ambulances), dont on peut questionner le caractère ouvert au public, ou non.
- Enfin, d'une manière générale, la CNIL a relevé au cours de ces contrôles l'évolution générale des dispositifs de vidéoprotection et de vidéosurveillance, qui se caractérise aujourd'hui par le déploiement de caméras « dômes » dotées d'une très forte capacité de zoom.

Ces caméras, qui sont capables de filmer à 360° avec une redoutable capacité de précision, défient la notion juridique de « proportionnalité », centrale en matière de protection des données à caractère personnel. Si une solution peut être trouvée par la mise en place de caches physiques ou numériques destinés à restreindre les zones filmées, ces protections se révèlent généralement insuffisantes.

L'ensemble de ces questions a conduit la CNIL à saisir le ministère de l'Intérieur afin d'envisager les évolutions à apporter au cadre légal pour préserver l'équilibre entre la protection de la vie privée et la sécurité des biens et des personnes. ■

Nombre de contrôles vidéo par secteur d'activité



ANTICIPER ET INNOVER

Dans le cadre de son activité d'innovation et de prospective, la CNIL s'efforce de concilier deux objectifs : prendre en compte très en amont de nouveaux sujets, autour par exemple de tendances, de technologies ou d'usages émergents, et aborder des sujets d'étude et d'analyse par l'intermédiaire d'outils et de projets innovants. En 2013, cette double approche s'est incarnée dans plusieurs projets dont *Mobilitics* est l'exemple le plus avancé.

MOBILITICS, UNE EXPLORATION AU CŒUR DES SMARTPHONES

Créé en 2011, le laboratoire d'innovation de la CNIL est une structure souple destinée à porter des projets alliant usages émergents, nouvelles technologies, développements informatiques, innovation dans les outils et partenariats extérieurs. Le laboratoire répond certes en premier lieu à la volonté de la CNIL de disposer en son sein de moyens informatiques dédiés permettant de tester et d'expérimenter, dans des conditions réelles, des produits et applications innovants. Mais au-delà de ces tests au quotidien, le laboratoire a été conçu pour porter des projets d'analyse et d'expérimentation qui s'apparentent à des projets de « Recherche & Développement ». Un premier projet Intitulé *Mobilitics*, a été lancé début 2012.

Ce projet allie l'ensemble des caractéristiques déjà évoquées pour un projet de laboratoire :

- il est basé sur une analyse de l'émergence du marché des applications, sur la généralisation croissante de l'usage des smartphones et tablettes et sur l'hypothèse de l'expansion croissante des logiques de traçage au monde mobile (Voir chapitre I « Les données personnelles à l'heure du numérique ») ;
- il poursuit un objectif inédit : alors que de nombreuses études « *in vitro* » ont étudié le comportement des applications mobiles (comme par exemple le « *What they know mobile* » du Wall Street Journal), *Mobilitics* suit le comportement *in vivo* et dans la durée des applications mobiles ;
- *Mobilitics* a été conçu dans une logique collaborative en associant des agents de la CNIL volontaires aux travaux ;
- enfin, *Mobilitics* est un projet conçu en partenariat avec une équipe de recherche Inria (*Privatics*), dans le cadre de la convention signée en 2012 entre la CNIL et Inria.

Le projet *Mobilitics* a donc consisté à développer un outil logiciel capable de détecter et d'enregistrer les accès à des données personnelles par des applications ou programmes internes du téléphone (accès à la localisation, aux photos, au carnet d'adresses, à des identifiants du téléphone, etc.). La première version du logiciel concernait des smartphones fonctionnant sous le système d'exploitation mobile d'Apple (iOS). L'outil concernant le système d'exploitation Androïd de Google a été ensuite mis au point, et une deuxième phase d'expérimentation est en cours au premier trimestre 2014.

Après un an de développement et d'échanges réguliers entre les chercheurs et les équipes CNIL, la première phase d'expérimentation *Mobilitics* a eu lieu de novembre 2012 à février 2013.

Concrètement, la CNIL et Inria ont installé cet outil sur 6 iPhones appartenant au laboratoire de la CNIL. Pendant 3 mois, des agents de la CNIL volontaires ont utilisé ces smartphones comme s'ils leur appartenaient. Il s'agit donc d'une démarche expérimentale portant sur un nombre limité d'utilisateurs et d'applications, qui, dans ce contexte déterminé, permet d'étudier dans le temps l'évolution des accès aux données personnelles, sans prétention d'exhaustivité ou de représentativité de l'échantillon. Cette expérimentation a permis au laboratoire de la CNIL de collecter près de 9 Go de données dans une base de données de 7 millions d'événements à analyser. Les volontaires ont librement choisi les applications qu'ils souhaitaient utiliser, et à eux 6 ont donc testé 189 applications différentes. L'analyse des résultats se poursuit depuis le printemps 2013, avec des premiers résultats présentés à la presse le 9 avril 2013. Ces résultats permettent à la CNIL de confirmer certaines observations (par exemple autour de l'importance de la géolocalisation) mais également de détecter des sujets d'intérêts nouveaux.

> *Mobilitics*, c'est 9 Go de données à analyser dans une base de 7 millions d'événements.

La géolocalisation, reine des données

Près d'un tiers des applications utilisées par les volontaires ont accédé à un moment ou un autre à la localisation du smartphone. L'intensité de ces accès étonne : notre base de données contient des milliers d'accès à la géolocalisation, à tel point que cela correspondrait à plusieurs dizaines d'accès en moyenne par utilisateur et par jour pendant les 3 mois. Une telle intensité surprend, car si elle peut paraître logique pour certains usages, par exemple une application d'itinéraire routier va mettre à jour régulièrement la position sur le trajet, tel n'est pas le cas pour bon nombre d'applications. Ceci peut être dû soit à une absence de réflexion sur l'intérêt de collecter ou non une telle donnée lors de la conception de l'application, soit à la volonté du développeur de constituer, sous couvert d'une fonction accessoire, une base de données de géolocalisation des utilisateurs, base dont on connaît la valeur en termes de marketing et de publicité…

Le smartphone, « extension du domaine de la lutte » concernant la traçabilité

L'autre confirmation majeure des résultats de *Mobilitics* est l'omniprésence de stratégies de collecte d'identifiants ou de traces permettant de suivre, analyser, mesurer ou monétiser l'activité et les usages des utilisateurs. On connaît l'importance et l'omniprésence des cookies et autres traceurs dans la navigation Internet classique (mais l'enjeu actuel de croissance du marketing se trouve évidemment dans le mobile.

Un des enjeux majeur consiste à reproduire et étendre dans le monde fermé des applications mobiles les outils de traçage développés dans le navigateur web. *Mobilitics* montre que les développeurs et les parties tierces intéressées font preuve d'imagination en la matière, par exemple en détournant de leur finalité initiale des identifiants matériels de l'appareil (UDID, IMEI, adresses MAC, etc.). Ainsi dans notre étude, une application sur deux utilisée par nos volontaires a accédé à l'identifiant matériel unique UDID Apple du smartphone[1]. Nos résultats permettent également de constater que de nombreuses applications transmettent vers le propriétaire de l'application ou vers des tiers en partenariat avec lui cet identifiant « en clair ».

L'économie cachée des données personnelles sur smartphone : la partie immergée de l'iceberg

D'une manière générale, *Mobilitics* confirme une hypothèse de départ déjà très présente dans les travaux de la CNIL depuis le sondage « Smartphones et vie privée » réalisé par Médiamétrie en novembre 2011 et le plan d'action « smartphones » dont *Mobilitics* est un élément fondamental. En effet, au-delà de l'économie visible de l'écosystème du smartphone (forfaits, ventes de smartphones, ventes d'applications) prospère une véritable économie cachée des données personnelles du smartphone *Mobilitics* démontre la complexité de cet écosystème, qui réunit des acteurs aux modèles économiques, tailles et métiers très diversifiés, qui va du géant international avec une capitalisation boursière se comptant en centaines de milliards de dollars au petit développeur d'applications.

De plus, cet écosystème est progressivement envahi par des acteurs invisibles pour les utilisateurs qui fournissent par exemple des solutions techniques clé en main aux développeurs pour améliorer les applications, leur fournir des statistiques ou monétiser leur audience. Ces acteurs tiers peuvent être des acteurs classiques ou des nouveaux acteurs spécialisés dans le mobile, moins connus du grand public et des médias.

Les problématiques des cookies et autres traceurs se développent non seulement dans la navigation mobile mais également dans le monde des applications. Or les moyens d'information et de maîtrise par les utilisateurs, déjà limités dans le web « classique » sont quasi inexistants dans le monde « *in app* ». C'est dans ce contexte que le G29 (groupe des CNIL européennes) a publié un avis concernant les applications mobiles le 14 mars 2013, dans lequel il formule des recommandations à destination de ces grandes catégories d'acteurs. *Mobilitics* permet d'affiner ces recommandations en soulignant que les responsabilités sont partagées mais différenciées entre les différents acteurs de l'écosystème des smartphones, qui doivent respecter l'ensemble des règles applicables en matière de protection des données :

- les développeurs d'application doivent intégrer dès le départ les problématiques Informatique & Libertés dans une démarche de *privacy by design*. La CNIL souhaite développer l'accompagnement des acteurs à cette fin ;
- les magasins d'application doivent inventer des modes innovants d'information des utilisateurs et de recueil du consentement. La situation actuelle, binaire, du « à prendre ou à laisser » n'est pas satisfaisante ;
- les paramètres et réglages présents dans les systèmes d'exploitation pour smartphones sont insuffisants. Dans le cadre du projet *Mobilitics*, la CNIL et Inria ont développé, à titre expérimental, une démonstration des réglages qui pourraient être proposés par le fournisseur du système d'exploitation ;
- les acteurs tiers qui fournissent des services et des outils aux développeurs ne doivent collecter que les données nécessaires et ce, en toute transparence, vis-à-vis du développeur et par voie de conséquence vis-à-vis de l'utilisateur final.

Mobilitics, deuxième phase d'expérimentation

L'analyse de la base de données s'est poursuivie pendant toute l'année 2013 et cette première phase de *Mobilitics* a aussi servi de prototype au laboratoire. Dans l'optique de la deuxième phase d'expérimentation, la stratégie de construction de la base de données a été affinée afin de faciliter le travail d'analyse. La CNIL et Inria poursuivent leurs recherches dans le cadre du projet *Mobilitics*, notamment sur les autres fournisseurs de systèmes d'exploitation du marché, ce qui permettra de suivre dans le temps les progrès accomplis par l'ensemble des acteurs. Depuis le premier trimestre 2014, une nouvelle vague expérimentale est ainsi en cours sur des smartphones équipés du système d'exploitation Androïd. ■

[1] *Apple a d'ailleurs réagi en rendant impossible l'accès, par des applications, à cette information dans les versions ultérieures de son système d'exploitation mobile iOS.*

LES AUTRES PROJETS INNOVANTS

45 000 téléchargements de *Cookieviz* depuis décembre 2013.

CookieViz

Les cookies et autres traceurs constituaient un autre projet de recherche du laboratoire, comme évoqué dans le 33ème rapport d'activité de 2012. En 2013, ce travail s'est essentiellement concentré autour de deux axes :

• un travail interne autour des modèles économiques des entreprises fondés sur l'usage des traceurs. En 2012, un projet intitulé *CookieMiner* avait permis de dresser une première cartographie de la présence de cookies et autres traceurs dans le web en « .fr ». À partir de ces données, une analyse économétrique a conduit à identifier des grappes de modèles économiques différents. Ces travaux, encore exploratoires, ont permis à la CNIL d'affiner sa compréhension des différents pans de cette industrie foisonnante ;

• le développement de *CookieViz*. Cet outil, développé en interne, permet à l'internaute de voir en temps réel l'apparition des cookies et autres traceurs au fur et à mesure de sa navigation, avec une logique similaire et complémentaire de celle d'outils déjà existants tels que *Lightbeam* de la fondation Mozilla. Simultanément à la publication de la recommandation portant sur les cookies et autres traceurs (Voir partie I), *CookieViz* a ainsi été proposé en téléchargement gratuit. *CookieViz* constitue une première pour la CNIL puisqu'il s'agit du premier outil logiciel développé en interne et mis à disposition du public dans une première version « beta ». Il s'agit aussi du premier projet de logiciel libre de la CNIL car le code de *CookieViz* est ouvert et peut être librement réutilisé dans le cadre d'une licence GPLV3 et enrichi. *CookieViz* a été téléchargé plus de 45 000 fois depuis son lancement en décembre 2013.

Les échanges avec les start-ups et la participation au projet Mesinfos de la FING

La CNIL est partie prenante depuis le départ du projet *Mes Infos* du *think tank* la FING. Dans le cadre de ce projet, la CNIL fournit conseils et expertise à la FING, à ses partenaires et aux start-ups impliquées dans la plateforme et l'expérimentation qui a été lancée avec 300 participants volontaires au dernier trimestre 2013 et qui va se poursuivre pendant le premier semestre 2014. Cette participation s'inscrit dans un objectif global de suivi des initiatives pouvant se rattacher à la logique dite du VRM (*vendor relationship management*), qui veut promouvoir les outils intelligents contrôlés par l'utilisateur lui permettant d'équilibrer la relation avec des commerçants numériques.

Plus globalement, la CNIL a développé ses échanges avec l'écosystème du numérique, en particulier pour identifier et conseiller de jeunes entreprises innovantes qui mettent la protection de la vie privée et des données personnelles au cœur de leur modèle économique. Pour cela, plusieurs interventions ont été organisées dans des lieux incubant ou réunissant des start-ups : intervention au *OuiShare Festival*, intervention devant les start-ups sélectionnées pour la saison 5 de l'accélérateur de l'association parisienne Silicon Sentier, « Le Camping », co-organisation avec le W3C d'un événement sur le marketing mobile au NUMA, nouveau lieu réunissant les activités de Silicon Sentier depuis novembre 2013.

Le soutien et les conseils aux projets de recherche en sécurité, innovation numérique et *big data*

Enfin, la CNIL a poursuivi son travail avec la communauté universitaire et de la recherche. Outre la participation à des comités de pilotage de l'Agence Nationale de la Recherche, un certain nombre d'équipes de recherche ont sollicité des conseils et un accompagnement dans le déroulement de leurs projets.

Ainsi, la CNIL a eu des échanges avec une équipe de chercheurs Algopol (http://algopol.fr/) qui s'intéressent aux interactions entre individus sur des réseaux sociaux et appliquent à cette recherche des méthodologies d'extraction d'analyse de données massives particulièrement personnelles. Les chercheurs, qui interviennent sur un domaine assez émergent, ont accepté de tester des formats innovants et inédits d'information des personnes et de recueil du consentement. Cette « recherche dans la recherche » a d'ailleurs poussé ces chercheurs à rendre publique leur réflexion sur le statut particulier des chercheurs en sciences sociales dans le numérique par rapport à cette question de l'éthique du rapport à la donnée (Voir sur *Internet Actu* l'article de Irène Bastard, Dominique Cardon, Guilhem Fouetillou, Christophe Prieur et Stéphane Raux : « Travail et travailleurs de la donnée », 13 décembre 2013, http://www.Internetactu.net/2013/12/13/travail-et-travailleurs-de-la-donnee/).

Dans un domaine différent, mais pour des raisons identiques, la CNIL a développé une démarche d'accompagnement de projets centrés sur le « *big data* » à l'exemple du projet « Investissement d'avenir » X-data centré sur des problématiques de croisement de données. Dans le cadre de ce projet, un travail sur les méthodologies d'anonymisation et d'analyse des risques de désanonymisation sera mené par un laboratoire Inria, *Privatics*. ■

PARTICIPER À LA RÉGULATION INTERNATIONALE

Compte tenu de l'augmentation des échanges transfrontières de données, la protection des données s'inscrit aujourd'hui dans une logique mondiale. C'est pourquoi la coopération entre autorités de protection apparaît désormais stratégique et nécessaire. Consciente de cette dimension, la CNIL s'investit toujours plus dans les forums internationaux où les différentes visions de la régulation internationale se confrontent.

INSTANCES DE REGULATION INTERNATIONALE ET CODES DE BONNE CONDUITE

Le G29 (groupe des 28 « CNIL » européennes)

Marquée par une actualité particulièrement chargée au niveau européen (révélations d'Edward Snowden, nouvelle politique de confidentialité de Google…), le G29 a vu ses travaux se développer au cours de l'année 2013.

Cette activité a été particulièrement intense pour **le sous-groupe « Frontières, voyages et activités répressives » (désigné par son acronyme anglais, BTLE).**

Dans le prolongement des révélations d'Edward Snowden sur le programme de surveillance PRISM, une « task force » Surveillance a été créée au sein du sous-groupe afin de formuler des observations et des propositions visant à renforcer l'encadrement des échanges de données vers les États-Unis.

Le sous-groupe a, par ailleurs, élaboré un avis relatif au système de « frontières intelligentes », envisagé par la Commission Européenne et visant à lutter contre le terrorisme, la criminalité et l'immigration illégale. Le sous groupe a notamment exprimé ses inquiétudes sur la mise en place d'un système visant à répertorier les entrées et sorties du territoire européen par les nationaux d'États tiers au regard des principes européens régissant la protection des données personnelles.

D'autre part, il a poursuivi son travail d'analyse sur le projet de dispositif d'inspection-filtrage initié par l'association internationale des transporteurs aériens (IATA), dont l'objet est d'instituer différentes files de contrôle des passagers aériens en fonction des risques qu'ils représentent.

Il a également travaillé sur le système recueillant des renseignements précis sur les passagers (système API). Enfin, il a poursuivi son suivi des accords PNR (*Passenger Name Record*) organisant la transmission des données de passagers européens voyageant vers des pays tiers, et en particulier vers les États-Unis.

Enfin, le sous-groupe s'est également saisi du projet de protocole additionnel à la Convention de Budapest qui prévoit l'accès des autorités judiciaires d'États tiers aux données stockées par les États de l'Union Européenne.

Le sous-groupe « Futur de la vie privée », dont l'objet est de réfléchir à la règlementation de demain, a quant lui formulé des propositions sur de nombreux sujets tels que la compétence des autorités de protection des données, l'application de l'exception relative aux activités personnelles ou domestiques, le profilage et le recours par la Commission européenne à des actes d'exécution venant préciser les modalités d'application de la règlementation européenne. Par ailleurs, suite au vote de la Commission LIBE sur le projet de reforme, le G29 s'est également attaché à appeler l'attention des institutions européennes sur la nécessité de voir le projet rapidement adopté.

De son côté, **le sous-groupe « Technologie »** a poursuivi ses travaux en 2013. Ont ainsi été adoptés par le G29, plusieurs documents proposant un modèle d'étude d'impact relatif au déploiement des compteurs électriques intelligents, un avis sur les applications mobiles et un avis sur les cookies.

En outre, la « task force » mise en place en 2012 et composée de plusieurs autorités de protection des données (la France, l'Angleterre, l'Espagne, l'Italie, l'Allemagne et les Pays-Bas) a permis de déclencher une action répressive coordonnée à l'encontre de Google.

INFOS +

Le G29

En 2013, c'est 41 documents adoptés, 8 groupes de travail, 5 plénières regroupant les 28 autorités de protection des données de l'Union Européenne.

DERNIÈRE MINUTE

Isabelle Falque-Pierrotin a été élue présidente du G29 pour 2 ans le 27 février 2014.

Le sous groupe « Transfert » a élaboré un document explicatif concernant le modèle de règles d'entreprise contraignantes pour les sous-traitants. Par ailleurs, les discussions avec le groupe de travail « *Vie privée* » de l'APEC ont permis la poursuite d'une expérience unique sur le développement d'un outil commun de transferts : relier les « *Binding Corporate Rules* » européennes et les *Cross-Border Privacy Rules* (« CBPR ») existant dans la zone Asie–Pacifique.

Le sous-groupe « Questions financières » a particulièrement travaillé sur le projet de directive européenne anti-blanchiment en sensibilisant les membres de la Commission LIBE du Parlement Européen sur ses faiblesses.

S'agissant du **sous groupe « E-gouvernement »**, l'année 2013 a été marquée par une analyse approfondie sur la problématique de l'*open data* suite à l'adoption le 26 juin 2013, de la directive concernant la réutilisation des informations du secteur public.

Enfin le **sous-groupe « Key Provisions »** dont la mission est d'analyser les dispositions « clés » de la directive 95/46 a élaboré un avis sur l'exigence de finalité d'un traitement de données. ■

AMÉLIORATION ET CRÉATION D'OUTILS DE FLUX TRANSFRONTIÈRES

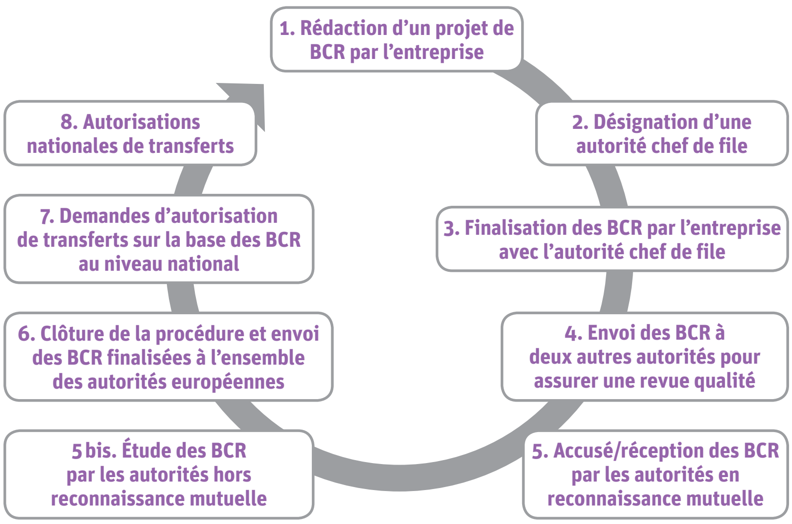
Les « BCR » : un sujet majeur pour les CNIL européennes

Les règles contraignantes d'entreprises (RCE, également dénommées « BCR » pour « binding corporate rules », constituent des **programmes de conformité** permettant de décliner les principes de protection des données personnelles sous forme de règles internes à un groupe d'entreprises. Ils représentent donc un réel outil de co-régulation.

Ainsi, la procédure d'approbation des BCR, fondée sur une coopération renforcée entre autorités par l'intermédiaire d'une autorité chef de file en charge de l'instruction de dossiers pour le compte des autres, a servi de base de réflexion aux autorités de protection des données et aux institutions communautaires, pour la préfiguration du système de gouvernance européen dans le cadre du projet de règlement.

Par ailleurs, les CNIL européennes se sont également attachées à améliorer leurs actions de coopération en matière de BCR, par l'intermédiaire du G29 (groupe des 28 « CNIL » européennes), notamment en réalisant un audit sur le délai moyen d'approbation d'un BCR, en développant des mécanismes d'accélération de la procédure par des autorisations implicites des autorités de protection des données et en instaurant une procédure de suivi des BCR en cours d'instruction afin d'éviter l'éventuel engorgement de certaines autorités.

Les grandes étapes des BCR



FOCUS

Quels délais pour les BCR ?

Un audit réalisé par le G29 s'est intéressé aux délais moyens d'instruction et de validation des BCR.

• **L'autorité chef de file met en moyenne 5 mois** pour gérer un dossier BCR : révision des différentes versions de BCR (3 en moyenne) et coordination de la coopération avec les autres autorités européennes de protection des données ;

• **Les procédures de reconnaissance mutuelle** (comprenant la révision des BCR par deux autorités secondaires) **et de coopération** avec les autres autorités **durent 3 mois environ** ;

• **Le groupe candidat à la validation de ses BCR par les autorités met environ 7 mois ½** pour prendre en compte les commentaires reçus par l'autorité chef de file et les autorités secondaires (et potentiellement les autorités qui ne font pas partie de la procédure de reconnaissance mutuelle) et pour soumettre des versions de BCR modifiées.

> Les BCR sont des outils de pilotage de conformité à l'échelle mondiale permettant de diffuser une véritable culture de la protection des données personnelles au sein de l'entreprise.

FOCUS

Liste des entreprises ayant officiellement adopté des BCR

(31 décembre 2013)

ABN AMRO, Accenture, American Express, ArcelorMittal, Atmel, AXA, AXA Private Equity, BP, Bristol Myers Squibb, CareFusion, Cargill, Citigroup, CMA-CGM, D.E. Master Blenders 1753 (Sarah Lee), Deutsche Post DHL, DSM, eBay, Ernst & Young, First Data, General Electric, GlaxoSmithKline, Hermès, Hewlett Packard, HR Access, Hyatt, IMS Health, ING Bank, International SOS, Intel, JP Morgan Chase & Co., Linklaters, LVMH, Michelin, Motorola Mobility, Motorola Solutions, Novartis, Novo Nordisk, OVH, Philips Electronics, Safran, Sanofi Aventis, Schlumberger, Schneider Electric, Shell, Société Générale, Spencer Stuart.

INFOS +

Transferts internationaux de données : le G29 et l'APEC proposent aux multinationales un outil pratique

Le système européen des BCR et celui des CBPR (*Cross-Border Privacy rules*) sont basés sur des approches comparables. Dans les deux cas il s'agit pour des entreprises de développer des codes de conduite pour les transferts internationaux qui sont revus a priori par des autorités de protection des données européennes (pour les BCR) ou par des tiers agréés (pour les CBPR).
Le G29 a étudié les CBPR afin d'identifier leurs similarités et leurs différences avec les BCR. Sur la base de cette comparaison, le G29 et les Etats membres de l'APEC ont élaboré un référentiel sur les exigences relatives à la protection des données personnelles et à la vie privée issues des BCR et des CBPR (WP212). Cet outil est destiné à aider les multinationales qui opèrent à la fois en Europe et dans la zone Asie-Pacifique puisqu'il identifie dans un document unique les éléments requis dans les systèmes BCR et CBPR.
Cet outil pratique liste, pour chaque principe et exigence, les éléments qui sont requis dans les deux systèmes, ainsi que les éléments additionnels spécifiques à chaque système. Dans tous les cas, ces éléments additionnels doivent être pris en compte par les entreprises multinationales souhaitant obtenir l'approbation de leurs BCR par les autorités de protection des données européennes d'une part, et la certification de leurs CBPR par un tiers certificateur agréé par l'APEC d'autre part.

Le réseau francophone des autorités de protection des données promeut les règles contraignantes d'entreprise (RCE)

Sous l'impulsion de la CNIL et des autorités belges et marocaines, l'Association francophone des autorités de protection des données personnelles (AFAPDP) a adopté en 2013 une « Résolution relative à la procédure d'encadrement des transferts de données personnelles dans l'espace francophone au moyen de règles contraignantes d'entreprise (RCE) », faisant suite à une résolution précédemment adoptée à Mexico le 31 octobre 2011.

Elle répond à la demande des autorités francophones de pouvoir disposer d'un outil commun pour encadrer et faciliter les transferts de données de l'espace francophone.

L'idée est de reprendre comme socle de base les principes adoptés par le G29 dans ses documents de travail établissant un cadre pour la structure des règles contraignantes d'entreprise (ou « RCE »). Cette solution offre plusieurs avantages : elle permet de garantir un niveau élevé de protection des données tout en s'appuyant sur un instrument juridique déjà connu et utilisé par les entreprises.

En termes de procédures, l'autorité en charge de RCE agirait comme un point de contact auprès des entreprises pour la vérification de la conformité au référentiel commun de l'outil développé par l'entreprise et comme coordinatrice auprès des autres autorités pour recueillir leurs commentaires sur cet outil. Les autorisations sur les transferts et/ou sur l'outil lui-même seraient délivrées par les autorités concernées, et non pas par l'autorité point de contact, conformément à leurs compétences nationales en matière de transferts. ■

> Cette démarche partenariale entre pays de l'espace francophone consiste à développer des outils de coopération avec différentes zones géographiques dans le monde.

LA COOPÉRATION INTERNATIONALE, UN ENJEU MAJEUR

Outre le cadre du G29, plusieurs forums internationaux sont consacrés à la question de la coopération en matière de protection des données.

Collaborer à la révision des textes régionaux fondamentaux

Les processus de révision des lignes directrices de l'OCDE et de la Convention n°108 du Conseil de l'Europe participent *de facto* à la mise en cohérence des textes internationaux en matière de protection des données et de vie privée. Dans ce contexte, il est fondamental que le niveau de protection élevé dont bénéficient certains des États-membres de l'Union européenne soit préservé.

L'OCDE adopte des nouvelles lignes directrices en matière de vie privée

L'OCDE est la seule institution internationale permettant un dialogue en matière de protection des données entre les pays de l'Union européenne, du Conseil de l'Europe et de la zone APEC (en particulier les États-Unis, le Canada et le Japon). La CNIL participe à ces réflexions en tant que représentant de la conférence internationale des commissaires à la protection des données (la Conférence internationale).

La nouvelle version des lignes directrices adoptée par l'OCDE le 11 juillet 2013 prévoit notamment une nouvelle section dédiée au renforcement de la responsabilisation des entreprises (« *accountability* »). En pratique, cela se traduit notamment par une obligation de mettre en œuvre des programmes de gestion de conformité interne en matière de vie privée et de notifier d'éventuelles failles de sécurité aux autorités compétentes et aux personnes concernées, par les responsables de traitement. Une préconisation est faite aux États participants de mettre en place et d'assurer le fonctionnement d'autorités chargées de protéger la vie privée.

Une clause générale précisant que les lignes directrices constituent des standards de niveau minimal qui peuvent être complétés de mesures supplémentaires permet aux pays de l'Union européenne de préserver le niveau élevé en matière de protection des données personnelles qui est le leur (notamment en matière de transferts de données et de durée de conservation).

Ces évolutions correspondent également à la volonté de rechercher les voies d'une meilleure interopérabilité entre les différents systèmes de protection des données personnelles.

Poursuite des travaux de révision de la Convention 108 du Conseil de l'Europe

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (dite « convention 108 ») du Conseil de l'Europe et son protocole additionnel, ratifiée par 44 pays, pose un certain nombre de principes contraignants en matière de protection des données, aujourd'hui universellement reconnus.

Les travaux de modernisation de la Convention, décidés depuis 2010, se poursuivent afin de l'adapter aux évolutions technologiques actuelles, avec un souci d'assurer une cohérence avec les textes adoptés par l'OCDE ainsi qu'avec le projet de Règlement européen.

Les propositions d'évolution du texte renforcent les droits des personnes de manière significative. Elles prévoient par exemple de faciliter l'exercice du droit de s'opposer au traitement de ses données, ou bien encore d'inclure les données génétiques et biométriques dans la catégorie des données sensibles.

Le projet de modernisation est désormais examiné par un comité intergouvernemental *ad hoc* pour la révision de la Convention 108 (dit « CAHDATA »), composé de représentants des gouvernements des États. La première réunion de ce comité s'est déroulée à Strasbourg du 12 au 14 novembre 2013. Les deux prochaines réunions du CAHDATA rendant possible une éventuelle adoption définitive de la Convention révisée devraient avoir lieu en 2014.

▸▸▸

La CNIL participe à ces travaux en tant que représentant de la conférence internationale des commissaires à la protection des données.

Le développement des forums de coopération internationale

La Conférence internationale tient une place particulière puisqu'elle regroupe le plus grand nombre d'autorités de protection de données indépendantes de par le monde. L'objectif de la Conférence est de favoriser les échanges entre les différents acteurs de la protection de la vie privée et de renforcer la coopération grâce à l'élaboration de règles communes. À ce titre, la Conférence Internationale dispose d'un groupe de travail sur la question des enquêtes et contrôles transfrontières. Ce groupe a pour objectif de rédiger un document cadre pour organiser la coopération dans ce domaine.

Certains forums optent pour une approche plus spécifique que celle de la Conférence internationale, ainsi que pour des critères d'adhésion plus larges. Tel est le cas du *Global Privacy Enforcement Network* (GPEN) qui, en cohérence avec les objectifs et le champ d'application de la Recommandation de 2007 de l'OCDE, se concentre sur les aspects pratiques de la coopération en matière d'enquêtes et de contrôles transfrontières et dont les membres ne sont pas nécessairement des autorités de protection indépendantes. La coopération au sein du GPEN a notamment permis d'organiser l'*Internet Sweep Day*, initiative proposant de scanner certains sites Internet afin de vérifier leur conformité par rapport aux principes de la protection des données. (Voir contrôler dans la partie II du rapport).

Aujourd'hui, face à l'émergence de problématiques de plus en plus complexes et de dimension transeuropéenne, se pose la question de l'opportunité d'élargir la coopération afin que celle-ci ne se limite pas uniquement aux contrôles mais s'ouvre également à d'autres domaines (tels que le partage de bonnes pratiques sur « l'*accountability* »). Plus généralement, trois défis majeurs semblent se présenter : d'abord celui du choix du forum le plus adapté pour accueillir et encadrer la coopération internationale, ensuite celui de la place des autorités européennes de protection des données et enfin, celui de l'étendue de la coopération. Pour la CNIL, la coopération doit s'entendre de manière large et ne pas se limiter à des questions spécifiques telles que les contrôles transfrontières. C'est pourquoi la Conférence internationale apparaît comme un forum idéal puisque regroupant de très nombreuses autorités et abordant tous types de problématiques. Enfin, il est aujourd'hui nécessaire que la voix des autorités européennes se fasse entendre de manière coordonnée, notamment au travers du groupe de travail de l'article 29.

> Il est primordial que les autorités européennes de protection des données coordonnent leurs positions afin que la voix européenne se fasse clairement entendre.

FOCUS

La 35ème Conférence internationale s'est déroulée du 23 au 26 septembre 2013 à Varsovie. 80 intervenants issus de plus de 40 pays ont débattu sur des sujets aussi variés que le profilage, l'accès des autorités publiques aux données, le *big data* ou encore la cyber sécurité.
La CNIL a notamment fait adopter une résolution portant sur le thème de l'éducation numérique.
En outre, à la suite de l'adoption d'une résolution sur l'évolution de la direction stratégique, la Conférence internationale réfléchit actuellement sur le rôle qu'elle souhaite tenir à l'avenir et sur les moyens à mettre en œuvre pour atteindre ses objectifs.

ISO : la CNIL acteur de la co-régulation

La CNIL est devenue un acteur de la co-régulation en normalisation internationale, vis-à-vis des membres de l'Association française de normalisation (AFNOR), du G29 et des participants aux réunions de l'Organisation internationale de normalisation (ISO). Elle assure également la liaison officielle entre le G29 et le groupe de travail de l'ISO en charge de la protection de la vie privée et a renforcé sa légitimité en sécurité de l'information en jouant le rôle d'éditeur de la norme centrale dans ce domaine, l'ISO/IEC 27001:2013.

La vision du G29 a ainsi été intégrée dans l'ISO/IEC 29100:2011 (*Privacy framework*), qui définit la terminologie et les principes de la protection de la vie privée. Cette norme a un rôle crucial dans le paysage normatif. Son intérêt reconnu par tous les pays participant à l'ISO a même valu qu'elle soit disponible gratuitement (http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html). La CNIL a également permis la création de plusieurs projets de normes relatives à la gestion des risques sur la vie privée (*Privacy Impact Assessments* – PIA), aux bonnes pratiques de protection de la vie privée et aux systèmes de management. Elle travaille aussi sur les projets de normes relatives au *cloud computing* et à la maturité dans le domaine de la protection de la vie privée. ■

3.
LES SUJETS DE RÉFLEXION EN 2014

Open data : un plan d'action pour accompagner la gouvernance des données publiques

Chantier bien-être et santé numérique

Mort numérique ou éternité virtuelle : que deviennent les données après la mort ?

OPEN DATA : UN PLAN D'ACTION POUR ACCOMPAGNER LA GOUVERNANCE DES DONNÉES PUBLIQUES

Les démarches dites d'*open data* sont de plus en plus nombreuses en France au niveau national comme au niveau local, à l'instar des pratiques constatées dans de nombreux autres pays. L'*open data* se définit par un certain nombre de principes et de valeurs autour de la mise à disposition, le plus souvent libre et gratuite, de données détenues par des acteurs publics. Cette mise à disposition vise à faciliter les réutilisations, commerciales ou non, de ces données. Les données personnelles sont une frontière naturelle affirmée avec force par les militants ou promoteurs de l'*open data*, souvent très conscients de l'importance de la préservation de la vie privée. Mais au-delà de cette affirmation de principe, déterminer si l'ouverture de données détenues par un acteur public peut induire un risque de réidentification ou de divulgation d'informations concernant des personnes n'est pas toujours chose aisée. La CNIL souhaite aider ceux qui sont en première ligne dans cette rénovation de la gouvernance des données publiques, et a pour cela mis en œuvre une stratégie en deux temps.

2013, ANNÉE D'ÉCHANGES ET DE CONCERTATION AVEC LES ACTEURS DE L'*OPEN DATA*

Consciente des bénéfices démocratiques et économiques susceptibles d'être engendrés par l'*open data*, la CNIL a souhaité avoir des échanges nombreux et ouverts avec les acteurs plongés au quotidien dans des projets ou démarches d'*open data* afin de comprendre leurs interrogations et d'évaluer l'importance des questions de données personnelles dans ces initiatives. Cette concertation s'est traduite par des rencontres et des échanges informels, puis par une journée de travail et de retours d'expériences organisée le 9 juillet 2013 avec les acteurs et experts du sujet. Il s'agissait de clarifier les termes du débat et de rechercher des solutions opérationnelles pour accompagner le développement de l'*open data* tout en garantissant le respect dû à la vie privée de chacun. Cette journée a été organisée dans les locaux de la CNIL avec le soutien de la mission Etalab, service du Premier ministre chargé de l'ouverture des données publiques et du développement de la plateforme data.gouv.fr. Elle a réuni une centaine de participants : représentants de collectivités territoriales et de ministères, réutilisateurs de données publiques, associations citoyennes, chercheurs, agents d'autorités publiques de régulation (CADA) ou de promotion de l'*open data*, et des agents de la CNIL.

Cette journée « openCNIL » a été ouverte le matin autour de deux tables rondes, après des propos introductifs de la Présidente de la CNIL et du directeur d'Etalab, Henri VERDIER (par ailleurs, membre du Comité de la prospective de la CNIL) et un rappel du cadre législatif en vigueur par le Président de la CADA, Serge DAËL.

L'après-midi était organisé autour de 4 ateliers : « Comment anonymiser ? », « Quels droits des personnes dans l'*open data* ? », « Comment faciliter l'accès des chercheurs aux données publiques ? « l'*open data* et au-delà… ».

Un compte-rendu complet du séminaire est disponible sur le site cnil.fr mais les discussions ont en particulier mis en exergue quelques éléments :

• Les données personnelles semblent très peu présentes dans les jeux de données mis à disposition aujourd'hui dans le cadre de l'*open data*.

• Les acteurs et experts de l'*open data* éprouvent cependant de réelles difficultés pour apprécier, au cas par cas, si les données dont la mise à disposition et la réutilisation sont prévues peuvent, ou non, être attachées à des personnes physiques identifiables. Les producteurs comme les réutilisateurs expriment un besoin d'informations et de conseils pratiques de la part de la CNIL.

• Dans le doute, certaines administrations sont très prudentes en matière de mise à disposition de données.

• Peu d'outils ou de méthodes sont mis à disposition des producteurs de données pour assurer l'anonymisation des données. Une demande de solutions techniques comme de recommandations d'usage s'est exprimée sur ce point.

• Enfin, la question de l'articulation entre le principe de finalité et la libre réutilisation appelle une clarification, les acteurs rencontrant parfois des difficultés pour appliquer la loi « Informatique et Libertés ». ■

UN PLAN D'ACTION POUR 2014 AUTOUR DE 5 AXES

Pour faire suite à ces constats, 5 axes de travail ont été dégagés et servent de cadre au travail de 2014 :

1. Dresser un état des lieux des pratiques des acteurs de l'*open data* et de la gouvernance des données publiques à travers un questionnaire en ligne, qui a été ouvert pendant tout le mois de janvier 2014 et qui a permis à près de 400 personnes intéressées (acteurs impliqués dans la mise en œuvre d'une plateforme ou d'une politique d'*open data*, producteurs ou gestionnaires d'informations publiques susceptibles d'être ouvertes, réutilisateurs à divers titres ainsi que les Correspondants Informatiques et Libertés) de faire part de leur retour d'expériences à la CNIL. Les résultats de cette enquête seront rendus publics.

2. Évaluer le cadre juridique actuel, en liaison étroite avec d'autres institutions publiques, en particulier la CADA et Etalab, le cas échéant, d'identifier les clarifications et simplifications nécessaires.

3. Proposer des outils opérationnels aux acteurs. Il s'agit de concevoir et de diffuser des conseils pratiques, illustrations à l'appui, notamment sur des concepts clés de la loi Informatiques & Libertés, comme la notion de données personnelles.

4. Explorer de nouvelles solutions techniques. La CNIL poursuit les investigations sur les solutions d'anonymisation disponibles pour les tester et envisager leur amélioration, et ce, en partenariat avec des chercheurs (en particulier ceux d'Inria) et en collaboration avec certains acteurs industriels travaillant sur ces sujets. Elle s'intéresse également aux initiatives étrangères prises en ce domaine et notamment aux travaux conduits par l'ukanon, consortium réunissant l'ICO, l'équivalent britannique de la CNIL, l'*open data Institute* et des universités…

5. Développer l'*open data* à la CNIL. La CNIL souhaite s'engager dans une politique d'ouverture de ses propres données. Elle a en conséquence engagé un travail de recensement des jeux de données susceptibles d'être mis à disposition sur la plateforme *data.gouv.fr* ■

INFOS +

Deux missions d'information

Le Sénat a créé fin 2013 deux missions d'information sur des sujets touchant aux questions mêlant gouvernance des informations publiques et respect de la protection des données personnelles. La première est une mission commune d'information sur l'accès aux documents administratifs et aux données publiques. Présidée par M. Jean-Jacques Hyest, cette mission « réfléchira aux modalités d'amélioration du dialogue entre les administrations et le public grâce à la simplification et à l'accélération des démarches administratives, au renforcement de la transparence de l'action publique par la facilitation de l'accès aux documents administratifs et la généralisation de la diffusion des données publiques (*open data*) ». Parallèlement, la Commission des lois du Sénat a confié à Gaëtan Gorce (par ailleurs membre de la CNIL) et François Pillet une mission d'information sur « l'*open data* et la protection de la vie privée » afin d'examiner l'articulation « entre législation sur l'accès et la réutilisation des informations du secteur public, d'une part, et, protection des données personnelles, d'autre part ». Ces deux missions devraient remettre leurs conclusions au cours du premier semestre 2014.

DERNIÈRE MINUTE

Les résultats de la consultation « *open data* et données personnelles »

Le questionnaire et les personnes ayant répondu

Pour compléter et élargir les débats de la journée « OpenCNIL » de juillet 2013, la CNIL a mené, au début de l'année 2014, une consultation publique: auprès des acteurs impliqués dans la mise en œuvre d'une plateforme ou d'une politique d'*open data* ; des producteurs ou gestionnaires d'informations publiques susceptibles d'être ouvertes ; des réutilisateurs à divers titres ; ainsi qu'auprès des référents ou Correspondants Informatique et Libertés (CIL). Au total, 391 personnes ou organismes ont répondu au questionnaire : 199 CILs et référents Informatique et Libertés, 98 réutilisateurs, 45 gestionnaires de données publiques et 49 responsables *open data*. Si ces chiffres sont assez importants eu égard à la nature de la consultation, cette consultation ne peut, pour autant, être représentative statistiquement de l'ensemble des publics concernés.

Les principaux enseignements de la consultation

Dans leur majorité, les acteurs de l'écosystème de l'*open data* ont déjà été confrontés à la question des données personnelles.

55 % des répondants « responsables *open data* » et « gestionnaires de données publiques » se sont déjà demandés si certains jeux de données dont l'ouverture était envisagée, pouvaient contenir des données personnelles.

44 % des réutilisateurs répondants se sont également posé cette question. Quant aux CIL et référents, seuls 15 % disent ne jamais avoir été consultés concernant ces questions d'*open data*, la moitié d'entre eux ayant été consultés par des « responsables *open data* » et/ou des « gestionnaires de données publiques », et entre 20 et 25 % l'ayant été par des réutilisateurs. Enfin, 1/3 des CIL ou référents Informatique et Libertés répondants ont déjà eu l'occasion de soulever un risque de diffusion de données à caractère personnel lorsqu'ils étaient consultés dans le cadre d'un projet d'*open data*.

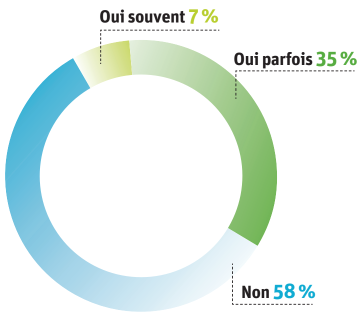
Lorsque cette question se pose, les CILs et la CNIL constituent des interlocuteurs privilégiés.

Pour tous les publics, le CIL ou référent Informatique & Libertés et le référent pour l'accès aux documents administratifs semblent des recours assez naturels lorsqu'ils existent et sont connus. La CNIL est également citée dans entre 20 et 30 % des réponses. En dehors de ces acteurs, les personnes ou entités consultées sont plus diverses : les pilotes et responsables *open data* ainsi que les réutilisateurs font ainsi appel à des réseaux informels d'experts et autres acteurs du domaine.

Le risque de présence de données personnelles est souvent pris en compte, sans pour autant bloquer la diffusion de données si des solutions simples peuvent être trouvées.

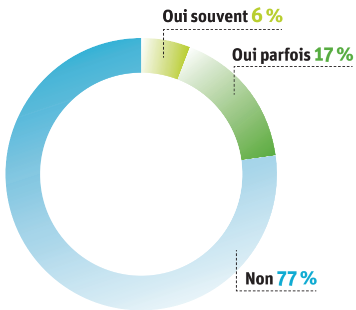
Près de 50% des gestionnaires de données publiques répondants ont indiqué avoir déjà fait part de leur opposition à l'ouverture de certaines données au motif d'un risque d'identification de personnes physiques.

Avez-vous déjà fait part de votre opposition à l'ouverture de certaines informations/données détenues ou produites par votre organisme au motif d'un risque d'identification des personnes concernées par les données ? (en valeur absolue)



Un peu moins de 25% des réutilisateurs répondants ont également indiqué avoir déjà essuyé des refus d'ouverture d'informations détenues par un organisme au motif d'un risque d'identification des personnes (exemples : données concernant des professions libérales et artisans, décisions de justice, données géolocalisées, données INSEE, données de santé, données relatives aux marchés publics, liste des bans de mariage, noms d'élus, ...).

Avez-vous déjà, suite à une demande précise, essuyé des refus d'ouverture d'informations détenues par un organisme au motif d'un risque d'identification des personnes concernées par les données ?



Lorsque les données contiennent ou semblent contenir des données personnelles, l'ouverture des données n'est pas nécessairement bloquée pour autant. Les CIL interrogés recommandent alors l'anonymisation des données (47 cas) ou le recueil du consentement (35 cas), et rarement l'abandon du projet d'ouverture (seulement 6 cas évoqués, en particulier pour des listes incluant des coordonnées de personnes).

Des solutions pratiques (anonymisation ou recueil du consentement) encore vagues

Peu de répondants ont su se positionner face aux questions concernant les techniques d'anonymisation ou de recueil du consentement. Souvent, les méthodes d'anonymisation évoquées sont sommaires (retrait des identifiants directs comme les noms et prénoms).

CHANTIER BIEN-ÊTRE ET SANTÉ NUMÉRIQUE

Début 2013 la CNIL a ouvert un chantier « bien-être et santé numérique ». L'objectif est de mesurer les impacts sur la vie privée de nouvelles pratiques numériques de santé, en lien avec le développement des capteurs connectés et des applications mobiles. Parfois décrit sous le vocable de *quantified self*, ce mouvement résulte d'une volonté d'accéder à une meilleure connaissance de soi en recourant à des mesures portant sur différentes activités liées au mode de vie et en les retranscrivant en chiffres.

Que ce soit au travers d'une application mobile de santé ou d'une balance connectée, ces pratiques se fondent sur des modes de capture de données de plus en plus automatisés et induisent la circulation de grandes masses de données personnelles aussi bien à l'initiative du partage par les individus eux-mêmes, qu'en raison des modèles d'affaires des acteurs économiques de ce marché.

Pour la CNIL, et dans le prolongement des travaux conduits dans le cadre du chantier vie privée 2020, il est naturel d'analyser plus en profondeur l'impact de ces pratiques sur les données personnelles de santé.

2013 a ainsi été l'occasion pour la CNIL d'engager plusieurs séries de travaux :

- entretiens avec des experts du sujet (chercheurs, institutionnels, médecins, acteurs économiques) ;
- état des lieux à l'international sur les régulations à l'œuvre relatives aux applications mobiles et capteurs connectés ;
- étude sur le marché et le modèle économique des acteurs ;
- lancement des tests de matériel dans le cadre du laboratoire.

2014 devrait permettre de livrer les premières conclusions sur les modalités de régulation envisagées pour accompagner le développement de ce marché tout en préservant la vie privée des utilisateurs. ■

> En 2017, 1 utilisateur de smartphone sur 2 aura installé au moins une application dédiée au bien-être ou à la santé.
>
> Source : Mobile Health Market Report 2013-2017 par Research2Guidance, Mars 2013

> 75 milliards d'objets connectés à l'horizon 2020.
>
> Source : Morgan Stanley, 2013

DES DONNÉES LIÉES AU CORPS, AU CŒUR DU MODÈLE ÉCONOMIQUE DES NOUVEAUX ENTRANTS

Qu'il s'agisse du nombre de pas réalisés dans la journée, de la qualité du sommeil ou de l'enregistrement d'activités sportives, ce mouvement est particulièrement intéressant à étudier dans la mesure où il concerne des données produites par les individus qui touchent à leur intimité et pourtant le plus souvent destinées à être partagées.

Ces pratiques semblent illustrer un nouveau rapport au corps, aux données et préfigurent sans doute des usages à venir en lien avec le développement des objets connectés. Les capteurs utilisés dans une logique de *quantified self* peuvent en effet être appréhendés comme la première vague de l'Internet des objets. Ces capteurs présentent la double particularité ▸▸▸

Un marché mondial estimé à 26 milliards de dollars à l'horizon 2017.

Source : Mobile Health Market Report 2013-2017 par Research2Guidance, Mars 2013

d'être portés par et « sur » les individus, et de produire des données d'un nouveau genre, formant une empreinte du corps, se situant ainsi à la frontière du bien-être et de la santé au sens médical.

La démocratisation de l'usage des capteurs ou d'applications dédiés en dehors des pionniers du « soi quantifié » repose sur 3 facteurs essentiels :

- le développement du *cloud computing* ;
- la baisse du coût des capteurs ;
- la progression de l'équipement en smartphone qui devient à la fois la télécommande des objets connectés et joue un rôle de hub pour la consultation des données. ■

QUEL CADRE DE RÉGULATION FACE À CES NOUVEAUX ENJEUX ?

Les enjeux en termes de protection des données sont différents selon que les initiatives proviennent des acteurs « traditionnels » du monde de la santé (professionnels, autorités de santé, laboratoires) ou des individus eux-mêmes.

Dans le premier cas, le déploiement de solutions ou de dispositifs nouveaux est encadré et a vocation à s'insérer par exemple dans les procédures d'agréments existantes (matériels médicaux, hébergeurs de données de santé, etc.). Les domaines de vigilance concernent alors généralement la sécurité et l'effectivité des droits des patients.

Dans le deuxième cas de figure, plusieurs séries de questions se posent :

- **Le statut des données** : une caractéristique essentielle des pratiques de quantification est qu'elles produisent des données qui se situent sur une frontière floue entre le bien-être et la santé. Or, les données de santé sont considérées comme sensibles et à ce titre font l'objet d'une réglementation renforcée (article 8 de la loi Informatique et Libertés). Qu'en est-il des données de bien-être ? En étant finalement plus ou moins directement reliées au corps, ces données sont aussi susceptibles de révéler la vie intime, y compris pour les moins sensibles d'entre elles *a priori*. Elles peuvent par exemple renseigner sur les heures de lever et de coucher (suivi de sommeil), sur les lieux fréquentés (géolocalisation des activités sportives), ou bien même estimer un risque cardio-vasculaire (données liées au poids).
- **La centralisation de ces données** : où sont-elles hébergées ? Comment sont-elles sécurisées ? Sont-elles cédées ? À quelles fins peuvent-elles être réutilisées ? Ces questions sont d'autant plus prégnantes que les utilisateurs peuvent avoir l'impression d'établir un rapport direct avec leurs données puisqu'ils en sont à l'origine. Or, la relation entre les utilisateurs et leurs données se fait par l'intermédiaire de l'entreprise qui produit le capteur ou édite l'application. Les données transitent d'abord par ses serveurs avant d'être visualisables et exploitables par l'utilisateur.
- **Vers un caractère normatif de la pratique de l'auto-mesure** : Le *quantified self* pourrait-il demain s'imposer à chacun comme certaines pratiques d'assureurs américains semblent le présager ? À l'avenir, pourrait-il devenir suspect de ne pas s'auto-mesurer ? ■

INFOS +

Le smartphone : un stéthoscope 2.0 ?

Selon l'étude *Research2guidance Mobile Health Market Report 2013-2017*, le nombre d'applications mobiles de santé disponibles dans les différents magasins est passé de 17 000 en 2010 à 97 000 en 2012. Le marché potentiel de la m-santé pourrait passer de 1 milliard d'utilisateurs en 2012 à 3,4 milliards en 2017. Concrètement, cela signifie qu'à cet horizon 1 possesseur de smartphone sur 2 devrait avoir installé au moins une application dédiée au bien-être ou à la santé. Les revenus issus du marché des applications santé devraient ainsi atteindre le chiffre de 26 milliards de $ avec un doublement du marché entre 2016 et 2017, avec un part non négligeable – environ 15 % – relative aux applications à destination des professionnels de santé.
À l'origine du développement du marché, les auteurs de l'étude soulignent le rôle clé des médecins dans la prescription d'applications ainsi qu'une structuration de l'offre avec l'émergence de magasins d'applications mobiles spécialisés dans le référencement d'applications de bien-être et de santé.

MORT NUMÉRIQUE OU ÉTERNITÉ VIRTUELLE : QUE DEVIENNENT LES DONNÉES APRÈS LA MORT ?

De nombreux internautes s'interrogent sur le devenir des données concernant leurs proches ou eux-mêmes après la mort. C'est dans ce contexte qu'a émergé le concept de « mort numérique », potentiellement porteur d'interrogations juridiques mais également sociétales. Sensible à la dimension humaine de cette thématique et soucieuse d'assurer une protection effective de l'identité individuelle, la CNIL ouvre le débat des enjeux de la mort numérique.

SUR LES RÉSEAUX SOCIAUX : À TERME PLUS DE MORTS QUE DE VIVANTS ?

Le développement de nouveaux modes d'exposition de soi en ligne a conduit à faire vivre son identité après la mort de multiples façons : il peut s'agir d'entretenir le souvenir d'un défunt, de créer un avatar qui dialoguera avec les vivants ou de laisser des messages ainsi que des biens dématérialisés (fleurs ou bougies) à ses héritiers ou ses proches. Ainsi, de nombreux sites proposent de faire vivre la personne après la mort, de rendre visible sa dernière « demeure » sur la toile, de proposer une tombe virtuelle, d'organiser un testament numérique ou enfin, de gérer ses identités numériques *post-mortem*.

Certaines collectivités locales proposent également des services de ce type (cimetières 2.0, bornes interactives dans les cimetières, gestions des données des personnes décédées, organisation de la réutilisation des archives de l'état-civil, etc.). Dès lors, comment concilier le droit à l'oubli numérique et les possibilités d'atteindre l'éternité numérique offertes par la vie en ligne ?

D'ici quelques années, une majorité des personnes décédées se sera dotée d'une identité numérique *post-mortem*. En effet, à défaut d'effacement programmé par la personne concernée, le profil d'un défunt continue d'exister, d'être visible sur la toile et d'être référencé par les moteurs de recherches.

LA MORT NUMÉRIQUE SOUS L'ANGLE « INFORMATIQUE ET LIBERTÉS »

Que les données concernent des personnes vivantes ou des personnes décédées, la CNIL, interlocuteur naturel des internautes en matière de protection des données personnelles, veille à ce que l'informatique ne porte atteinte, ni à l'identité du défunt, ni à la vie privée de ses héritiers.

Sur le plan de la loi Informatique et Libertés, la question de la mort numérique invite à s'interroger sur la prise en compte par les réseaux de la mort d'une personne, mais également sur le respect de ses droits ainsi que sur leur application effective par ses héritiers. Les droits d'accès, de modification, et de suppression prévus par la loi sont des droits personnels qui s'éteignent à la mort de la personne concernée.

La loi ne prévoit pas la transmission des droits du défunt aux héritiers : un héritier ne peut donc, sur le fondement de la loi Informatique et Libertés, avoir accès aux données d'un défunt. La loi autorise toutefois les héritiers à entreprendre des démarches pour mettre à jour les informations concernant le défunt (enregistrement du décès par exemple).

Pourtant, les familles des personnes disparues qui s'adressent à la CNIL veulent pouvoir accéder aux données concernant le défunt, ou exigent au contraire leur suppression. Dans ce contexte souvent douloureux, la Commission fait face à des problématiques aussi bien techniques que juridiques. Chargée de veiller au respect des durées de conservation des données conformément à la finalité poursuivie, elle s'intéresse à l'effacement, la suppression, le déréférencement ou la désindexation des données des personnes décédées.

Toutefois, la prise en compte de l'intérêt des héritiers n'est pas évidente en l'absence d'expression de la volonté du défunt. Afin de pallier cette carence, les grands acteurs de l'Internet, tels Google et Facebook proposent désormais des fonctionnalités permettant de paramétrer « la mort numérique ». ■

LES ENJEUX DE LA RÉGULATION DE LA MORT NUMÉRIQUE

L'encadrement juridique de la mort numérique ne devrait pas reposer sur les seules conditions générales d'utilisation des sites, d'autant plus que de nombreuses questions n'ont parfois pas de réponses. Dans quelles conditions les héritiers peuvent-ils récupérer les données du défunt ? Si rien n'est prévu dans les conditions générales d'utilisation des sites, quels sont les héritiers qui pourront demander la mise à jour ou la suppression des données ? Comment résoudre les conflits entre des héritiers qui n'ont pas toujours la même perception de la volonté *post-mortem* du défunt (si un héritier souhaite accéder aux données alors qu'un autre souhaite les supprimer) ?

S'agissant de la conservation et l'accessibilité des données, la Commission a été invitée à plusieurs reprises à se prononcer sur le cadre juridique de la conservation et l'archivage des données des personnes décédées et sur leur accessibilité et leur réutilisation [1].

Cependant la régulation de la mort numérique ne se limite pas à la seule protection des données personnelles des défunts ou de la vie privée de leurs ayants-droits. Le droit des contrats ainsi que le droit des successions devront sans doute évoluer pour répondre à ces nouveaux besoins exprimés par les utilisateurs et anticiper la problématique de la mort en ligne.

À la veille de l'adoption d'un règlement européen consacrant de nouveaux droits (le droit à l'oubli ou le droit à la portabilité des données), il semble nécessaire d'introduire dans les débats, la question de la prise en compte de la mort par les réseaux sociaux et ses conséquences pour les personnes. La CNIL n'ayant pas vocation à arbitrer l'équilibre qui doit être trouvé entre les besoins de suppression de toutes traces de l'identité après la mort, et la volonté d'atteindre l'immortalité numérique en continuant à faire vivre l'identité au-delà de la mort. Cependant, il apparaît essentiel que les autorités de protection des données, en concertation avec les pouvoirs publics, les professionnels de l'Internet, les acteurs de la société civile et les citoyens, ouvrent la discussion sur ce sujet qui tend à devenir une problématique incontournable de « l'âge numérique ». ■

[1] *CNIL, rapport annuel d'activité 2012*

4. BILAN FINANCIER ET ORGANISATIONNEL

LES MEMBRES DE LA CNIL

LE BUREAU

Présidente

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

Vice-président déléguée

Marie-France MAZARS, Doyen de la Cour de cassation honoraire
Secteurs : Ressources Humaines, travail et biométrie
Marie-France Mazars est membre et vice-présidente, déléguée de la CNIL depuis février 2014.

Vice-président

Éric PERES, membre du Conseil économique, social et environnemental
Secteurs : industrie, transports, énergie, défense
Éric Peres est membre de la CNIL depuis décembre 2010, puis vice-président depuis février 2014.

LES MEMBRES (COMMISSAIRES)

Jean-François CARREZ, président de la chambre honoraire à la Cour des comptes
Secteurs : police, immigration, coopération internationale
Jean-François Carrez est membre de la CNIL depuis janvier 2009. Il a été élu Président de la formation restreinte.

Dominique CASTERA, membre du Conseil économique, social et environnemental
Secteurs : Libertés individuelles, vie associative, vote électronique, élections
Dominique Castera est membre de la CNIL depuis octobre 2010.

Nicolas COLIN, inspecteur des finances, cofondateur et associé de la société de capital-risque *TheFamily*
Secteurs : santé (assurance maladie/recherche/e-santé)
Nicolas Colin est membre de la CNIL depuis février 2014.

Claude DOMEIZEL, sénateur des Alpes-de-Haute-Provence
Secteurs : éducation, enseignement supérieur
Claude Domeizel est membre de la CNIL depuis décembre 2008. Il est membre élu de la formation restreinte.

Laurence DUMONT, députée du Calvados
Secteurs : social et logement
Laurence Dumont est membre de la CNIL depuis octobre 2012.

Joëlle FARCHY, professeure de sciences de l'information et de la communication à l'Université Paris I et chercheure au Centre d'économie de la Sorbonne
Secteurs : affaires culturelles, sportives, jeux, tourisme
Joëlle Farchy est membre de la CNIL depuis février 2014.

Gaëtan GORCE, sénateur de la Nièvre
Secteurs : justice, eurojust
Gaëtan Gorce est membre de la CNIL depuis décembre 2011.

Sébastien HUYGHE, député du Nord
Secteurs : collectivités locales, vidéoprotection, téléservices
Sébastien Huyghe est membre de la CNIL depuis juillet 2007. Il est membre élu de la formation restreinte.

Philippe LEMOINE, président-directeur général de LaSer, Président du Forum d'Action Modernités et Président de la Fondation Internet nouvelle génération
Secteurs : recherche, statistiques, archives et données publiques
Philippe Lemoine est membre de la CNIL depuis février 2014.

Alexandre LINDEN, Conseiller honoraire à la Cour de cassation
Secteurs : santé (assurance maladie/recherche/e-santé)
Alexandre Linden est membre de la CNIL depuis février 2014. Il est vice-président de la formation restreinte.

Marie-Hélène MITJAVILE, conseiller d'État
Secteur : international
Marie-Hélène Mitjavile est membre de la CNIL depuis février 2009. Elle est membre élue de la formation restreinte.

François PELLEGRINI, professeur des universités à l'université de Bordeaux
Secteurs : distribution, commerce-marketing, lutte contre la fraude et impayés, international
François Pellegrini est membre de la CNIL depuis février 2014.

Maurice RONAI, chercheur à l'École des Hautes Études en Sciences Sociales (EHESS)
Secteurs : NTIC, communications électroniques, innovations technologiques
Maurice Ronai est membre de la CNIL depuis février 2014. Il est membre élu de la formation restreinte.

Jean-Luc VIVET, conseiller Maître à la Cour des comptes
Secteurs : banque, crédit, assurance et fiscalité
Jean-Luc Vivet est membre de la CNIL depuis février 2014.

Commissaires du gouvernement

Jean-Alexandre SILVY
Catherine POZZO DI BORGO, adjoint

LES RESSOURCES HUMAINES

LE PERSONNEL

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

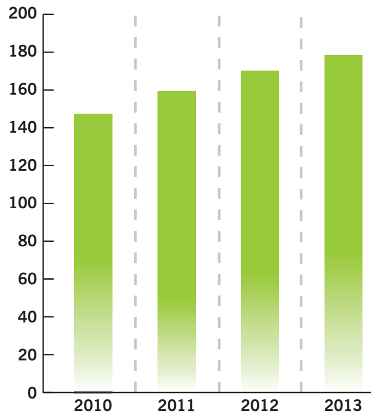
Ainsi, en 2013, elle a été dotée de 7 postes supplémentaires, passant ainsi de 171 postes à 178, soit une augmentation de 4 % de ses effectifs.

Ces nouveaux emplois ont permis :

- de consolider les équipes dédiées aux activités « traditionnelles » de la CNIL (examen de formalités préalables obligatoires, instructions de plaintes, sanctions, contrôles) afin d'améliorer constamment la qualité du service rendu aux usagers,
- de renforcer les moyens alloués à l'expertise informatique en raison des dernières missions confiées par le législateur (contrôle de la vidéoprotection - loi n°2011-267 du 14 mars 2011 dite LOPPSI 2 et enregistrement des notifications des failles de sécurité -, loi n°2011-302 du 22 mars 2011), ainsi qu'à la direction de l'innovation et de la prospective.

Dans cette perspective d'évolution croissante de l'activité de la CNIL, les moyens en personnel vont continuer à progresser, à raison de 7 créations de postes par an durant le triennal budgétaire 2013-2015.

Nombre de postes entre 2010 et 2013



LE BILAN FINANCIER

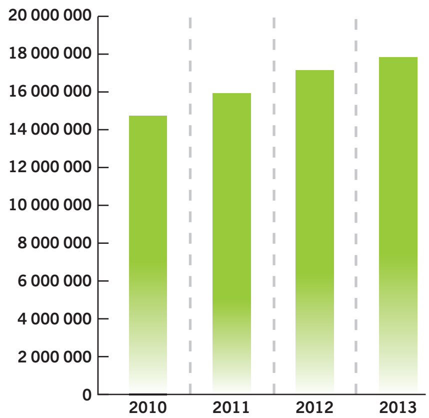
En 2013, les crédits totaux octroyés à la CNIL (16 926 309 €) ont continué d'apparaître dans une dynamique de croissance (+2,4%). Pourtant, cette année a été marquée par un tournant en termes de dotations budgétaires au regard de la diminution du budget de fonctionnement alloué (-3,7 %).

En effet, si les crédits consacrés au personnel (11,66 millions d'euros) ont cru de 5,5 % en vue de financer les 7 postes supplémentaires alloués, les crédits alloués au fonctionnement (5,2 millions d'euros) ont, quant à eux, nécessité une maîtrise accrue visant à absorber la baisse des dotations et le coût de fonctionnement induit par ces postes supplémentaires aux fins de mener à bien les projets métiers priorisés.

Dans ce cadre, un travail de recherches et de réalisations d'économies dans les postes de fonctionnement a été effectué.

Par ailleurs, la CNIL a poursuivi son recours à des dispositifs d'achats mutualisés, notamment les marchés passés par le Service d'Achats de l'État en vue de réaliser des économies structurelles sur les dépenses de fonctionnement.

Budget total LFI en € entre 2010 et 2013



ORGANIGRAMME DES DIRECTIONS ET SERVICES

- **Isabelle Falque-Pierrotin** – Présidente
  - **Édouard Geffray** – Secrétaire général
    - Qualité performance et risques
    - Service des affaires européennes et internationales
    - Conseil juridique et Relations institutionnelles
    - Service de la communication externe et interne
    - **Direction de la Conformité (DC)**
      - Service du secteur régalien et des collectivités locales
        - Service de la santé
          - Pôle en charge de la gestion des formalités préalables
      - Service du secteur économique
        - Service des questions sociales & RH
          - Service des correspondants Informatique et Libertés
            - Pôle BCR
              - Pôle labels
    - **Direction de la protection des droits et des sanctions (DPDS)**
      - Service des plaintes
        - Service des contrôles
          - Service des sanctions
            - Service droit d'accès indirect
    - **Direction des technologies et de l'innovation (DTI)**
      - Service de l'expertise technologique
        - Service de l'informatique interne
          - Pôle innovation, études et prospective
    - **Direction des relations avec les publics et la recherche (DRPR)**
      - Service de l'information et de la documentation
        - Service des relations avec les publics
          - Pôle des publications scientifiques et partenariats avec le monde de la recherche
            - Pôle éducation au numérique
    - **Direction administrative et financière (DAF)**
      - Service des ressources humaines
        - Service des finances et des marchés publics
          - Service des moyens généraux

ANNEXES

Liste des organismes
contrôlés en 2013

Lexique

LISTE DES ORGANISMES CONTRÔLÉS EN 2013

ASSOCIATION

ASSOCIATION HÔPITAL FOCH

ASSURANCE

INTER MUTUELLES ASSISTANCE

MACIF

BANQUE

BGD

BNP PARIBAS PERSONAL FINANCE

CAISSE RÉGIONALE DU CRÉDIT AGRICOLE MUTUEL ALPES PROVENCE

CRÉDIT AGRICOLE SA

BIOMÉTRIE

ACTION TRAVAIL SERVICES

A DOC

A DOMI PLUS

AEROSHUTTLE

APDC NHBM

ATAO AUDIO SYSTEM

BRIGADE DES SAPEURS POMPIERS DE PARIS

CARAT FRANCE

COLLÈGE CLAUDE DEBUSSY

COLLÈGE CONDORCET

COLLÈGE JEAN DE VERRAZANE

COLLÈGE LAVOISIER

COLLÈGE PAUL GAUGUIN

COLLÈGE VOLTAIRE

EREA ALEXANDRE DUMAS

ÉTABLISSEMENT PUBLIC MUSÉE QUAI BRANLY

FECIT - HÔTEL NAPOLÉON

GIE GIEPROD

GSD GESTION

GURDEBEKE SA

IT'GYM

LYCÉE ALAIN COLAS

LYCÉE GERARD DE NERVAL

LYCÉE MAURICE RAVEL

LYCÉE PIERRE BEREGOVOY

LYCÉE PROFESSIONNEL CHENNEVIERE MALEZIEUX

LYCÉE PROFESSIONNEL ÉTIENNE DOLET

LYCÉE RECAMIER

MAIRIE D'ASNIÈRES

MAISON DE RETRAITE SAINT-GEORGES

MUTUELLE UMC

OGEC DU SACRÉ CŒUR

PERL

PMGS

PRIMARK FRANCE SAS

RDI

SMILAIR

SOTREMA

TYLER INSURANCE

COLLECTIVITÉS LOCALES

ASSOCIATION PUTEAUX EN MOUVEMENT (AUDITION)

CENTRE COMMUNAL D'ACTION SOCIALE DE TROYES

COMMUNE D'AMIENS

COMMUNE DE BEAUVAIS (CENTRE CULTUREL FRANCOIS MITTERRAND)

COMMUNE DE BLANQUEFORT (MÉDIATHÈQUE ASSIA DJEBAR)

COMMUNE DE CARRIERES-SOUS-POISSY

COMMUNE DE GARGES-LES-GONESSE

COMMUNE DE NANTERRE

COMMUNE DE PARIS

COMMUNE DE PERSAN

COMMUNE DE PUTEAUX

COMMUNE DE ROUBAIX

COMMUNE DE SAINT-GRATIEN

COMMUNE DE TROYES

COMMUNE DE VALENCIENNES

COMMUNE DU CROTOY

CONSEIL GÉNÉRAL DE L'ESSONNE

CONSEIL GÉNÉRAL DU VAL DE MARNE

COMMERCE

AMBASSADRICES PARISIENNES

ARCELORMITTAL MÉDITERRANÉE

BASE & CO

BOUYGUES TÉLÉCOM

BRICO DÉPOT

BVA

CAJIS FRANCE (AUDITION)

CAPDECISION

CASINO D'URIAGE

CENTRE EXPRESS LIMOUSIN

CGM HÔTELLERIE

CHARMILLES IMMOBILIER

CITADINES

CMS (ESPACE-INFORMATIQUE)

COGNAC DISTRIBUTION

CORA

COSEM (COORDINATION DES ŒUVRES SOCIALES ET MÉDICALES)

CSA

DES RELAIS D'ALSACE - TAVERNE KARLSBRAU

DREAMLEAD INTERACTIVE (AUDITION)

ÉLECTRICITÉ DE FRANCE

ELITE DIFFUSION

ENDEMOL FRANCE

ÉTABLISSEMENTS DARTY ET FILS

EUROSTAR INTERNATIONAL

FEDERAL EXPRESS INTERNATIONAL FRANCE (FEDEX)

FONEX (AUDITION)
FREE
GFK ISL CUSTOM RESEARCH FRANCE
GIBERT JEUNE GROUPE SA
GIBERT JOSEPH
GIFI MAG
GOOGLE.INC
GROUPE CIRCET
H & M HENNES & MAURITZ
HERTZ CLAIM MANAGEMENT
HERTZ FRANCE SAS
HYPERCOSMOS
IFOP
IPSOS FRANCE
JDC AQUITAINE
JIVE SQUAD
J.P.B
LABORATOIRE GLAXOSMITHKLINE
LE BOURGOGNE
LE GRAU DU ROI LOISIRS (CASINO FLAMINGO)
LE MEILLEUR DES MONDES (PARIS-CY)
LIGUE DE TENNIS DES HAUTS-DE-SEINE
MAN DIESEL & TURBO FRANCE
MCDONALD'S PARIS NORD
MEDIAMETRIE
MEDIASTAY
MEUBLES IKEA FRANCE
MGI-TWC SAS
NMP FRANCE (HÔTEL MERCURE PARIS ARC DE TRIOMPHE ETOILE)
OPINION WAY
P2H INVESTISSEMENT
PAYPAL FRANCE SAS
PHŒNIX TRANSPORT
PIXMANIA
PROGRESS
PUBLICATIONS AGORA FRANCE
REGIME COACH
RESTO IN
SCI BEAUGRENELLE
SEPHORA
SOCIETE JOUL
SOCIETE VIGICORP
SOCLIDIS
SODICO EXPANSION
SPORTSDIRECT.COM FRANCE
STARBUCKS COFFEE FRANCE
SUPPLY CHAIN FRANCE
TAYLOR NELSON SOFRES
TOFIPAR (MC DONALD'S)
TOYOTA FRANCE
U.G.C.
UBISOFT
WW E-SERVICES FRANCE
YOUGOV FRANCE
Z9 EUROPE (AUDITION)

CULTURE

BIBLIOTHÈQUE NATIONALE DE FRANCE
CENTRE GEORGES POMPIDOU
COMMUNE D'AIX EN PROVENCE (CITÉ DU LIVRE-BIBLIOTHÈQUE MEJANES)
COMMUNE DE BAGNEUX (MÉDIATHÈQUE LOUIS ARAGON)
COMMUNE DE JOINVILLE LE PONT (ESPACE MULTIMÉDIA)
COMMUNE DE PARIS (MÉDIATHÈQUE MARGUERITE YOURCENAR)
COMMUNE DE NANTERRE (MÉDIATHÈQUE PIERRE ET MARIE CURIE)
COMMUNE DE TOURS (MÉDIATHÈQUE FRANCOIS MITTERRAND)

ÉDUCATION

AUTO-ECOLE FEU VERT
COLLEGE FRANÇOISE GIROUD
UNIVERSITÉ RENÉ DESCARTES PARIS V (BIBLIOTHEQUE UNIVERSITAIRE) À MALAKOFF

IMMOBILIER

ASSOCIATION URBAINE LIBRE DU PARC (AFUL)
CHAMPS ÉLYSÉES PRESTATIONS
EIFFAGE IMMOBILIER ATLANTIQUE
FP IMMOBILIER
GREEN POINT
QUEVILLY HABITAT STE ANONYME D'HABITATIONS À LOYER MODÉRÉ
SOCIÉTÉ ANONYME D'ÉCONOMIE MIXTE DE CONSTUCTION IMMOBILIÈRE DE BÈGLES

MINISTÈRES

OFFICE NATIONAL DES ANCIENS COMBATTANTS À LILLE

PARTI POLITIQUE

FÉDÉRATION DÉPARTEMENTALE DU RHÔNE DE L'UNION POUR UN MOUVEMENT POPULAIRE (U.M.P) À LYON
FÉDÉRATION DE PARIS DE L'UNION POUR UN MOUVEMENT POPULAIRE (U.M.P) (PRESTATAIRE EXTELIA) À SOPHIA-ANTIPOLIS
UNION POUR UN MOUVEMENT POPULAIRE (CIRCONSCRIPTION DE SAÔNE ET LOIRE) À MACON
UNION DES DEMOCRATES ET INDÉPENDANTS À PARIS

POLICE - JUSTICE

AGENCE FRANCAISE DE SÉCURISATION DES RÉSEAUX ROUTIERS
MINISTÈRE DE L'INTÉRIEUR (DIRECTION INTERRÉGIONALE POLICE JUDICIAIRE DE LYON) - SERVICE DES COURSES ET JEUX ANTENNE DE GRENOBLE
MINISTÈRE DE L'INTERIEUR (FPR) - SERVICE TECHNIQUE DE RECHERCHES JUDICIAIRES ET DE DOCUMENTATION DE LA DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE - ROSNY SOUS BOIS
MINISTÈRE DE L'INTÉRIEUR (STIC) - SERVICE TECHNIQUE DE RECHERCHES JUDICIAIRES ET DE DOCUMENTATION DE LA GENDARMERIE NATIONALE - ROSNY SOUS BOIS
MINISTÈRE DE L'INTÉRIEUR (STIC) – DIRECTION INTERRÉGIONALE DE POLICE JUDICIAIRE DE LILLE
MINISTÈRE DE L'INTERIEUR (STIC) - DIRECTION RÉGIONALE DE LA POLICE JUDICIAIRE DE PARIS

MINISTÈRE DE LA JUSTICE (DIRECTION INTERRÉGIONALE DES SERVICES PENITENTIAIRES D'ÎLE DE FRANCE) - FRESNES

MINISTÈRE DE LA JUSTICE (DIRECTION INTERRÉGIONALE DES SERVICES PÉNITENTIAIRES EST-STRASBOURG) - METZ

MINISTÈRE DES AFFAIRES ÉTRANGÈRES (AMBASSADE DE FRANCE - UKRAINE - KIEV

PRÉFECTURE DE POLICE DE PARIS

SANTÉ ET SOCIAL

AIR FRANCE

ALTAO

AMEDIM

AP-HP HOPITAL COCHIN

ATMAN FORMATION

ATMAN TRAINING CENTER

CAF DU NORD

CAISSE NATIONALE D'ALLOCATIONS FAMILIALES DE PARIS

CEGEDIM STATEGIC DATA FRANCE

CENTRE COMMUNAL D'ACTION SOCIALE D'AMIENS

CENTRE COMMUNAL D'ACTION SOCIALE D'ARLES

CENTRE COMMUNAL D'ACTION SOCIALE DE BOULOGNE BILLANCOURT

CENTRE COMMUNAL D'ACTION SOCIALE DE BOULOGNE SUR MER

CENTRE COMMUNAL D'ACTION SOCIALE D'ORANGE

CENTRE COMMUNAL D'ACTION SOCIALE DE NANTES

CENTRE COMMUNAL D'ACTION SOCIALE DE NICE

CENTRE COMMUNAL D'ACTION SOCIALE DE SAINT-BRIEUC

CENTRE COMMUNAL D'ACTION SOCIALE DE SAINT-DENIS

CENTRE COMMUNAL D'ACTION SOCIALE DE TOULOUSE

CENTRE D'OSTÉOPATHIE ATMAN

CENTRE HOSPITALIER D'ARMENTIERES

CENTRE HOSPITALIER DE BOURG-EN-BRESSE

CENTRE HOSPITALIER DE ROUBAIX

CENTRE HOSPITALIER DE SAINT-MALO

CENTRE HOSPITALIER DU ROUVRAY

CENTRE HOSPITALIER INTERCOMMUNAL EURE-SEINE – SITE D'EVREUX ET DE VERNON

CENTRE HOSPITALIER MARC JACQUET

CENTRE HOSPITALIER UNIVERSITAIRE CAEN (CECOS)

CENTRE HOSPITALIER UNIVERSITAIRE DE NANCY

CENTRE HOSPITALIER UNIVERSITAIRE DIJON (CECOS)

CENTRE HOSPITALIER UNIVERSITAIRE REIMS (CECOS)

CENTRE HOSPITALIER UNIVERSITAIRE RENNES (CECOS)

CLINIQUE ARAGO

COMMUNE D'ARLES

COMMUNE DE BOULOGNE BILLANCOURT

COMMUNE DE BOULOGNE SUR MER

COMMUNE DE NANTES

COMMUNE DE NICE

COMMUNE D'ORANGE

COMMUNE DE SAINT-BRIEUC

COMMUNE DE SAINT-DENIS

COMMUNE DE TOULOUSE

CONSEIL GÉNÉRAL DU VAUCLUSE

CORSACOD (AUDITION)

COSEM COORDINATION ŒUVRES SOCIALES ET MEDICALES

DL SANTE

DS ANALYSIX

EVOLAB (AUDITION AUPRÈS DU PRESTATAIRE DL SANTÉ)

GIE HUMANIS ASSURANCE DE PERSONNES

GROUPE HOSPITALIER JEAN-VERDIER

HÔPITAL PRIVÉ GÉRIATRIQUE DES MAGNOLIAS

HOPITAL TENON

HOSPICES CIVILS DE LYON

IMPLICIT

INTUITIVE (AUDITION)

JMT CONSEILS (AUDITION M. TORA JEAN-MARC)

KRAWCZYK PASCAL

LABORATOIRE DE CONTACTOLOGIE APPLIQUÉE

MEDLINK (AUDITION)

MUTUALE, LA MUTUELLE FAMILIALE

MUTUELLE FAMILIALE DU LOIR ET CHER

MYLAN S.A.S.

PLANSANTE

PÔLE DE SANTÉ DU PLATEAU

PÔLE EMPLOI - NOISY LE GRAND + PARIS + BAGNOLET

SAHONA CONSEIL

SÉCURITÉ

COMMISSARIAT À L'ÉNERGIE ATOMIQUE - GIF SUR YVETTE

COMMISSARIAT À L'ÉNERGIE ATOMIQUE (STE VOXALY ET BUREAU ESPACE SECRÉTARIAT TÉLÉMATIQUE) - SAINT-HERBLAIN

COMMISSARIAT À L'ÉNERGIE ATOMIQUE (ITS INTEGRA) - NANTERRE

SUPPLY CHAIN FRANCE

SPORT

CONSORTIUM STADE DE FRANCE

TRANSPORT

AIR CARAIBES

GO VOYAGES

LASTMINUTE

LOC CAR DREAM

OPODO

SOCIÉTÉ DES AUTOROUTES PARIS-RHIN-RHONE

VOYAGES-SNCF.COM

LISTE DES ORGANISMES CONTRÔLÉS EN 2013 DISPOSITIFS DE VIDÉOPROTECTION/VIDÉOSURVEILLANCE

BANQUE

CRÉDIT AGRICOLE
SOCIÉTÉ GÉNÉRALE

COLLECTIVITÉS LOCALES

COMMUNAUTÉ URBAINE DE STRASBOURG
COMMUNE D'ANET
COMMUNE D'ORANGE
COMMUNE DE BOIS COLOMBES
COMMUNE DE BORDEAUX
COMMUNE DE CANNES
COMMUNE DE CHALON-EN-CHAMPAGNE
COMMUNE DE CHARENTON-LE-PONT
COMMUNE DE CHARLEVILLE-MEZIERES
COMMUNE DE CLUSES
COMMUNE DE COLOMBES
COMMUNE DE COMPANS
COMMUNE DE COURBEVOIE
COMMUNE DE LEVALLOIS-PERRET
COMMUNE DE LIBOURNE
COMMUNE DE MELUN
COMMUNE DE NEMOURS
COMMUNE DE NOISY-LE-SEC
COMMUNE DE NOYELLE-GODAULT
COMMUNE DE PANTIN
COMMUNE DE RETHEL
COMMUNE DE SAINT-HERBLAIN
COMMUNE DE SARTROUVILLE
COMMUNE DE SURESNNES
COMMUNE DE VENISSIEUX
COMMUNE DE YERRES

COMMERCE

ANTONELLE
APPLE RETAIL
AROMES RESTAURATION GERLAND – CLASS'CROUTE
BARBA MARÉE
BENETTON
BIJOUTERIE FLINOIS
BRIENNE AUTO
CARREFOUR HYPERMARCHÉ
CASINO DE LUC-SUR-MER
CENTRE COMMERCIAL AUCHAN
CENTRE COMMERCIAL LA PART DIEU
COMPAGNIE PARISIENNE DE RESTAURATION VILLA MONTMARTRE
CORA
DAMART
DECATHLON BESANCON
DECATHLON SAINT-HERBLAIN
DECAVISION
DISTRITOUL
EARL BALTARD
E-NETWORK
ETB ALARME
EUROBRILLANCE
EUROCOM SYSTEM
FONTAN SAS
FOOT LOCKER
GALERIES LAFAYETTE
GARAGE BUZEAU
GINEYS SAS
GRANDE PHARMACIE DE PARIS
HÔTEL B&B
HÔTEL DABICAM
HÔTEL ENTRE TERRE ET MER
HÔTEL FRANCOIS 1ER COGNAC CENTRE
HÔTEL MERCURE
HÔTEL PLAZZA ATHENEE
HÔTEL VANEAU SAINT-GERMAIN
HÔTEXCO SA
HYPERMARCHÉ CORA
ICE WATCH STORE
IN CHOISY – CFI
INSTITUT FLEUR DE LYS
INTS FRANCE DESIGUAL
IZAC
JUCEL INTERMARCHE
KARDA ETAM
KREMLIN DISTRIBUTION CENTRE LECLERC
LA POSTE
LE BOWLING COMTOIS

LE COIN DES MARQUES
LES DÉLICES DE CHARONNE
LORMA
M'SPORT
MAGASIN CERISE ET POTIRON (ECULLY + LYON)
MAGASIN FRAIS ET COMPAGNIE
MAGASIN INTERMARCHÉ THYEZ
MAP (UGO BACCI)
MARIONNAUD
MATSOBE
MERCEDES BENZ
MUJI TO GO
NESPRESSO France
NTT CAUMARTIN
Ô DÉLICES DE MARIUS
PHARMACIE DE LA GARE
PHARMACIE DES PORTES DU SUD
PHARMACIE DU MARCHÉ VERNON
PROMOCASH
PROVIDIS LOGISTIQUE
RELAIS FNAC
RÉSEAU CLUB BOUYGUES TELECOM
RESIDATHENES
RODMAX TUTTI PIZZA
SANSONID
SARL DELICE
SCADI
SHAYEIM & MARLOW
SIMPLY MARKET
SOCIÉTÉ DE SERVICES BAGAGES AÉROPORTUAIRES
SOCIÉTÉ DES TRANSPORTS DU BASSIN CHELLOIS
SOCIÉTÉ DU 16 RUE CAMBACERES
SYNDICAT MIXTE DE LA BASE DE LOISIRS DE TRAPPES
TABAC PRESSE DES TOULEUSES
VIOLETTE OPTIC

CULTURE

ÉTABLISSSEMENT DU CHÂTEAU DU MUSÉE DU DOMAINE NATIONAL DE VERSAILLES
MUSÉE DES AUGUSTIN
MUSÉE RODIN
MUSÉUM D'HISTOIRE NATURELLE PARIS
ZOO FAUVERIE DU MONT-FARON

ÉDUCATION

LYCÉE PROFESSIONNEL CONDE

IMMOBILIER

LEPINAY MALET

POLICE - JUSTICE

ICTS MARSEILLE-PROVENCE
SURVISION

SANTÉ/SOCIAL

CLINIQUE VICTOR PAUCHET
GROUPE HOSPITALIER MUTUALISTE DE GRENOBLE
SECURITAS DIRECT

SPORT

ESPACE SPORTIF PAILLERON

TRANSPORT

GARE D'IVRY-SUR-SEINE
GARE DE NANTES
GARE DE PERPIGNAN
VEOLIA TRANSPORTS
VEOLIA TRANSPORTS NEMOURS

LEXIQUE

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

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

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

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

Biométrie
La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales…).
Bring your own device (BYOD)
Pratique qui consiste à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel

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

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

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

Correspondant Informatique et Libertés
Créé en 2004, le correspondant Informatique et Libertés (CIL) est chargé d'assurer de manière indépendante le respect des obligations prévues par la loi du 6 janvier 1978 ; en contrepartie de sa désignation, les traitements de données personnelles les plus courants sont exonérés de déclarations auprès de la CNIL.

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

Donnée sensible
Information concernant l'origine raciale ou ethnique, les opinions politiques,

philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

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

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

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

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

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

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

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

G29
L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationale. Cette organisation réunissant l'ensemble des CNIL européennes a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ.

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

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

PNR (« Passenger Name Record »).
Il s'agit des informations collectées auprès des passagers aériens au stade de la réservation commerciale. Elles permettent d'identifier, entre autres : l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que des préférences alimentaires spécifiques (végétarien, asiatique, cascher, etc.) ou des services liés à l'état de santé du passager. Des informations du type « tarif pèlerin » « missionnaire » « clergé » telles qu'elles figurent dans les champs « libres » des rubriques « remarques générales ». Ces données étant susceptibles de faire apparaître indirectement une origine raciale ou ethnique supposée , des convictions religieuses ou philosophiques, ou l'état de santé des personnes sont considérées par la directive européenne comme des données sensibles, à exclure ou à protéger.

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

RFID (Radio Frequency Identification)

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

Séance plénière

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

SIS (Système d'information Schengen

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

Smart Grids

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

Traitement de données

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

Traitement des Antécédents Judiciaires (TAJ)

Le Traitement des Antécédents Judiciaires (TAJ), successeur depuis le 1er janvier 2014 des fichiers STIC (Système de Traitement des Infractions Constatées) et JUDEX (Système Judiciaire de Documentation et d'Exploitation) regroupe, sur la base des procédures établies par les services de police et unités de gendarmerie, les informations concernant les personnes mises en cause ou victimes d'infractions pénales.

Transfert de données

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

Vidéoprotection

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

Vidéosurveillance

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

Violation de données à caractère personnel

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

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

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

Diffusion
Direction de l'information légale et administrative

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

ISBN : 978-2-11-009785-9
DF : 5HC37800
Prix : 15 €

9 782110 097859

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

Commission Nationale de l'Informatique et des Libertés