rapport d'activité 2014

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 **2014**

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

LES CHIFFRES CLÉS DE 2014

CONSEILLER ET RÉGLEMENTER

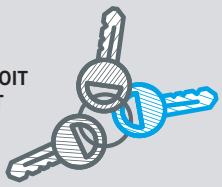
2277
DÉCISIONS ET DÉLIBÉRATIONS

dont **390** autorisations
dont **100** avis
15 autorisations uniques
3 normes simplifiées

PROTÉGER

5825
PLAINTES

dont **39%**
concernent internet



5246
DEMANDES DE DROIT D'ACCÈS INDIRECT (+22%)

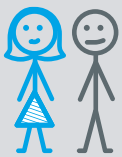
(FICHIERS DE POLICE, DE GENDARMERIE, DE RENSEIGNEMENT, FICOBA, ETC.)

6656
VÉRIFICATIONS RÉALISÉES

MOYENS DE LA CNIL

185
POSTES

38,5
ÂGE MOYEN



63%
DE FEMMES

37%
D'HOMMES

ACCOMPAGNER LA CONFORMITÉ

92663
DOSSIERS DE FORMALITÉS REÇUS

11892
DÉCLARATIONS POUR LES SYSTÈMES DE VIDÉOSURVEILLANCE

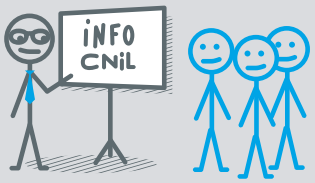
6123
DÉCLARATIONS POUR DES DISPOSITIFS DE GÉOLOCALISATION

401
AUTORISATIONS EN MATIÈRE DE BIOMÉTRIE

3 PACKS DE CONFORMITÉ

14441
ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT SOIT 4000 CIL

34
ATELIERS D'INFORMATION
QUI ONT ACCUEILLI 1000 PARTICIPANTS



44
LABELS DÉLIVRÉS
(dont 10 en 2014)

2 NOUVEAUX RÉFÉRENTIELS ADOPTÉS

34
NOTIFICATIONS DE VIOLATIONS DE DONNEES PERSONNELLES

INFORMER

37120
COURRIERS REÇUS

130
INTERVENTIONS

133213
APPELS TÉLÉPHONIQUES

CONTRÔLER ET SANCTIONNER

421
CONTRÔLES

dont **88** contrôles vidéo
58 contrôles en ligne

62
MISES EN DEMEURE

18
SANCTIONS

dont **8** sanctions financières
7 avertissements
3 relaxes

SOMMAIRE

AVANT-PROPOS DE LA PRÉSIDENTE

LES VALEURS HUMANISTES, UNE BOUSSOLE POUR CONSTRUIRE LE NUMÉRIQUE

L'année 2014 s'est caractérisée par une intensification du débat public et de nombreuses interventions d'experts sur la question des données personnelles. Celle-ci est désormais centrale tant auprès des acteurs publics que privés. Toutes les institutions se mobilisent pour essayer de comprendre et, le cas échéant, de réguler le phénomène, alors que le grand public hésite entre la fascination et l'alarme.

Au plan national, on peut citer notamment le rapport du Conseil d'État sur le numérique ou la consultation du CNNum sur le projet de loi numérique envisagé par Axelle Lemaire.

Dans les deux cas, la CNIL a largement contribué à ces travaux et elle a salué le fait que ces réflexions transversales qu'elle a tant appelées de ses vœux dépassent le cercle des autorités de protection des données et mettent en discussion une certaine vision, politique, économique et sociétale de nos sociétés.

> “Opposer innovation et protection des données est une posture fausse et stérile.”

Au plan international, les discussions ont été également très vives, autour notamment du droit à l'oubli.

La décision de la Cour de justice de l'Union Européenne en matière de droit au déréférencement de mai 2014 qui confirme l'application du droit européen aux moteurs de recherche, a en effet polarisé l'intérêt de tous et elle apparait comme une avancée majeure et irréversible pour les citoyens européens. Donner aux internautes la possibilité de demander aux moteurs de recherche, sous certaines conditions, de rendre moins visibles des contenus affectant leur vie privée est un moyen de rééquilibrer leurs relations avec les grands acteurs de l'internet et de renforcer la maîtrise de leur identité numérique.

Beaucoup d'encre a alors coulé, beaucoup d'idées fausses ont circulé pour discréditer ce droit au déréférencement, dénoncer un « vide juridique », voire un impérialisme européen. Face à cette agitation, et dès l'annonce de l'arrêt de la CJUE, le G29 s'est mis en ordre de marche pour en assurer une application uniforme et lisible à travers toute l'Europe. Cette coopération a abouti, six mois plus tard, à l'adoption d'un mode d'emploi opérationnel qui permet, au travers d'une liste de critères communs, d'objectiver l'instruction des plaintes reçues par les autorités de protection et de guider la décision des moteurs de recherche. De façon générale d'ailleurs, l'année passée a permis au G29 de rentrer dans une phase plus opérationnelle de son histoire.

Sur le sujet du droit au déréférencement comme sur l'action répressive à l'encontre de Google et le pack de conformité qui lui a été proposé, le G29 a su démontrer sa capacité à **coordonner un réseau d'autorités encore assez hétérogènes et à afficher un front uni** sur des questions complexes. Cette évolution du G29 vers un réseau à la fois plus opérationnel et aussi plus stratégique est un des axes que j'ai souhaité inscrire au titre des priorités de la nouvelle présidence.

Isabelle Falque-Pierrotin,
Présidente de la CNIL

Le débat international s'est aussi beaucoup nourri de la perspective du règlement européen et de ses conséquences pour les grands acteurs internationaux.
S'est en effet mis en place au cours de l'année un discours très offensif à l'encontre des principes européens, au service d'une stratégie de conquête d'un modèle concurrent. Les principes européens sont présentés par certains comme inadaptés aux nouvelles réalités numériques, incapables de répondre aux enjeux du Big data ou de l'internet des objets.
Face à ces nouveaux défis, le régulateur doit savoir se renouveler tout en maintenant le cap fixé par des valeurs fondatrices encore robustes.
« *Privacy is dead !* » entendait-on par exemple à Davos en janvier dernier. **Non, la vie privée n'est pas morte mais elle évolue incontestablement vers une dimension plus individuelle**. Aujourd'hui, les données personnelles sont la particule élémentaire du monde numérique. Elles sortent du strict champ de la vie privée et participent à la construction d'une vie publique revendiquée par les individus eux-mêmes. Ces derniers font d'ailleurs la distinction entre ce qui relève de l'intime et qu'ils souhaitent préserver et ce qui peut contribuer à leur vie publique. Ils paramètrent leur vie privée pour obtenir une exposition sur-mesure, « à façon ». Aujourd'hui, plus que de protection, c'est de maîtrise que les individus sont demandeurs. Le projet de règlement va d'ailleurs dans ce sens en renforçant les droits et en proposant par exemple un droit à la portabilité des données. Cette approche plus individuelle de la vie privée ne doit pas pour autant conduire à faire peser tout le poids de la régulation sur l'individu. Poussée à l'extrême, une telle démarche pourrait conduire à la privatisation des données, au risque d'oublier que la protection des données est un droit fondamental, donc inaliénable même par l'individu lui-même. **L'enjeu pour le régulateur consiste dès lors à intégrer ces tensions nouvelles entre l'individuel et le collectif**. Pour ce faire, il doit proposer des outils juridiques et pratiques qui aboutissent à plus de transparence de la part des acteurs économiques et plus de maîtrise pour les individus.
"*Big data is beautiful !*". Autre formule que l'on a beaucoup entendue ces derniers temps et qui n'est pas sans lien avec la précédente. L'antienne ressassée à l'envi nous explique que la révolution du big data, ô combien prometteuse dans un contexte économique difficile, est un phénomène orthogonal à la loi informatique et libertés. Pire encore, celle-ci entraverait l'expansion de cet eldorado alors que **tout devrait s'incliner inéluctablement devant la puissance de l'algorithme**. Mieux vaudrait donc laisser les seules entreprises décider de croiser et brasser toutes les données qu'elles souhaitent en pariant sur les bénéfices obtenus par ce traitement de masse.
Je pense, pour ma part, que **la réalité est sans doute plus modeste et parfaitement intégrable à une démarche informatique et libertés**. Les principes de la loi sont suffisamment robustes et plastiques pour ingérer le changement d'échelle induit par le big data. Assurément, la procédure et les outils doivent s'adapter en allégeant le contrôle *a priori* (finalité de la collecte) et en développant des outils de conformité adaptés aux usages sectoriels. La CNIL y travaille à travers notamment ses packs de conformité. Les techniques d'anonymisation sur lesquelles s'est penché le G29 dans son avis d'avril 2014 peuvent également ouvrir des voies opérationnelles de traitement des données dans le cadre du big data.
Opposer innovation et protection des données comme certains voudraient nous y conduire est donc une posture fausse et stérile. Non seulement ces principes ne s'opposent pas, mais au contraire ils enclenchent un cercle vertueux, un cercle de confiance, clé de voûte d'un numérique durable. Et les principes de protection de données peuvent aider l'Europe à être à la pointe du Big data. ▸▸▸

Il faut d'autant plus écarter cette inutile opposition qu'une nouvelle tension s'exerce de plus en plus sur la protection de la vie privée et des libertés individuelles, celle liée à l'impératif de sécurité.
Depuis les révélations d'Edouard Snowden et à nouveau, avec les attaques terroristes perpétrées en janvier en France, **l'équilibre entre libertés et sécurité est en effet débattu dans tous les pays**.
Snowden a levé le voile sur la surveillance massive et généralisée de l'ensemble de la population par des acteurs privés, pour le compte d'acteurs publics. Snowden questionne toutes les démocraties et les réponses que celles-ci élaborent face à une menace terroriste croissante.
Pour trouver de réelles voies d'action pour faire face à la situation actuelle, il faut, me semble-t-il sortir d'une opposition binaire entre sécurité et liberté. **Le respect des libertés fondamentales n'est pas contradictoire avec l'impératif de sécurité : c'est le garde-fou de nos démocraties**, les deux doivent aller de pair. Dès lors, pour être acceptable d'un point de vue juridique, éthique et social, la recherche de nouveaux outils de sécurité doit nécessairement s'accompagner d'un renforcement des garanties. C'est précisément le rôle de la CNIL de contrôler cet équilibre fragile et de prévenir les dérives éventuelles, au plan national comme sur les dossiers européens.
Mais, tout dispositif doit être analysé non à l'aune de ses intentions mais à celle des usages effectifs que permettent les textes et qui ne peuvent conduire, sauf à sortir de l'Etat de droit, à une surveillance massive et indiscriminée des personnes.
C'est autour de ces convictions que le G29 a adopté une déclaration commune présentée le 8 décembre 2014 à Paris, à l'occasion d'une conférence internationale à l'UNESCO. Cette déclaration pose le principe d'un nécessaire équilibre entre protection des données personnelles, innovation et surveillance, et elle pointe la nécessité de mettre en œuvre des dispositifs ciblés et non massifs en matière de surveillance.

L'année 2014 a donc, vous le voyez, été riche en évènements, rebondissements et débats. La CNIL face à cela avance, construit sa route, sans a priori, ni exclusion.

L'année 2015 s'annonce déjà et notre priorité consiste avant tout à **adopter au plus vite le projet de règlement européen sur les données personnelles**. Il semble qu'après une période d'accalmie due au renouvellement des institutions européennes, le calendrier s'accélère à nouveau et l'on parle maintenant d'une adoption en 2015. Une telle étape est indispensable pour crédibiliser l'unité et l'identité de l'Europe ; aussi pour créer un espace européen de la donnée attendu de tous.

> “Le respect des libertés fondamentales n'est pas contradictoire avec l'impératif de sécurité : c'est le garde-fou de nos démocraties.”

Sur un plan plus opérationnel, nous allons continuer à **accompagner la transition numérique des acteurs en développant des outils de conformité plus souples et plus sectoriels**. Nous souhaitons également favoriser **la responsabilité des individus face à tous ces changements**. Le numérique est construit autour de l'utilisateur et de ses usages. Ses données sont au cœur de la dynamique. Il doit donc être respecté dans sa capacité de choix et d'arbitrage et ne pas devenir un simple objet du numérique. Un travail doit donc être mené sur la manière de l'armer, afin qu'il garde la maîtrise d'un environnement en changement permanent.

Nos démocraties connaissent une période extrêmement complexe pour nos libertés. Mais dans la tempête, nous avons une boussole : celle de l'Etat de droit, d'un Etat qui protège les individus, et qui place la personne au cœur de son projet. C'est ce modèle équilibré qu'il nous faut défendre fermement tout en le renouvelant pour en faire un cadre éthique et juridique durable, propice à l'innovation et respectueux du droit des personnes.

> Le processus de mise en conformité dynamique implique de recourir à des nouveaux outils qui responsabilisent les organismes. ”

MOT DU SECRÉTAIRE GÉNÉRAL

LA CNIL AU SERVICE DE SES PUBLICS

Édouard Geffray,
Secrétaire général

Alors que, depuis plusieurs années, l'activité de la CNIL connaît une forte croissance, les services de l'institution ont été réorganisés en 2014 avec pour objectifs de mieux répondre aux attentes des différents publics, d'anticiper sur le règlement européen et de mettre en œuvre des outils et méthodes de régulation innovants.

S'agissant de la hausse de l'activité de la CNIL, elle est naturellement liée à l'importance des traitements de données dans l'univers numérique, aussi bien du point de vue des entreprises (2 277 délibérations ont été adoptées) que des particuliers. Le droit au déréférencement, consacré en mai 2014 par la Cour de justice de l'Union européenne, s'est ainsi traduit, en France, par plusieurs dizaines de milliers de demandes adressées aux moteurs de recherche, et près de 200 plaintes d'ores et déjà adressées à la CNIL. Plus généralement, la CNIL a enregistré plus de 5 800 plaintes et 5 246 demandes d'exercice du droit d'accès indirect aux fichiers sensibles (sécurité publique ou fiscaux, soit + 22 % en un an, après + 17 % en 2013 et + 40 % en 2012). L'activité répressive de la CNIL s'en est fortement ressentie, avec 62 mises en demeure et 18 sanctions prononcées.

Au-delà des chiffres, la croissance et l'évolution de la CNIL témoignent surtout de la diffusion rapide d'une culture de la conformité à la loi « informatique et libertés ». La question n'est plus, pour un organisme public ou privé, de savoir s'il a fait la bonne démarche auprès de la CNIL. La question est de savoir s'il assure une protection optimale des données personnelles de ses clients ou usagers en permanence. Or, ce processus de mise en conformité dynamique implique de recourir à des nouveaux outils, qui responsabilisent les entités concernées tout en leur donnant les « clés » de compréhension de cette culture. Cette évolution est d'autant plus nécessaire qu'elle est consacrée par le futur règlement européen, qui place l'accompagnement de la conformité au cœur des démarches des CNIL, au détriment des formalités administratives.

Concrètement, cela se traduit par le succès de l'ensemble des outils de la conformité. Les « correspondants informatique et libertés » sont désormais présents dans 14 400 organismes (contre 13 000 en 2013 et 10 700 en 2012). Les labels, qui permettent à une entreprise de faire valoir le respect d'exigences élevées en matière de ▸▸▸

protection des données, connaissent un succès croissant, avec 44 labels délivrés et deux nouveaux référentiels adoptés. Le dernier référentiel, adopté début 2015, porte ainsi sur la gouvernance de la protection des données personnelles, permettant ainsi à une entreprise de faire de cet aspect un élément fondamental de la relation de confiance avec ses clients ou ses fournisseurs. En aval, les contrôles menés par la CNIL, suivis le cas échéant d'une mise en demeure par la Présidente, se traduisent dans l'immense majorité des cas par la mise en conformité de l'organisme, sans qu'il soit besoin d'enclencher la procédure de sanction. Enfin, la conformité suppose une juste compréhension des nouvelles technologies et des innovations. L'activité d'études et prospective de la CNIL, portée par un pôle dédié, et plus généralement l'ensemble de ses capacités d'expertise technologique, permettent de répondre à ces besoins, en lien étroit avec les professionnels concernés et les chercheurs.

Les « packs de conformité » constituent la clef de voûte de l'ensemble de ce dispositif : nouvel outil mis en œuvre en 2013, ils visent à donner à l'ensemble des professionnels d'un secteur les clés de compréhension et d'application de la loi « informatique et libertés ». Ils regroupent ainsi des bonnes pratiques et des outils de simplifications, les seconds étant les corollaires du respect des premiers.

La conformité implique en effet d'orienter l'activité de la CNIL comme les efforts des responsables des traitements de données vers le respect des obligations substantielles. La CNIL diffuse donc les bonnes pratiques et construit des cadres de régulation sécurisants pour pouvoir, corrélativement, simplifier massivement les formalités administratives. C'est ainsi que plus de la moitié des déclarations reçues par la CNIL consistent désormais en des « engagements de conformité » à un cadre de référence prédéfini. De la même manière, en 2014 la CNIL a adopté 15 « autorisations uniques » représentant à terme plusieurs centaines d'engagements de conformité, qui seront autant de formalités administratives en moins pour les entreprises, au profit d'un cadre protecteur et unifié.

Mais la conformité implique aussi une diffusion large de l'information, à la fois aux personnes concernées et aux entités qui traitent leurs données. Les demandes de conseils ne cessent d'augmenter (133 000 appels en 2014 contre 124 000 en 2013), et la CNIL va donc lancer, au printemps 2015, un nouveau service de réponse en ligne. Cet outil permettra ainsi à tout à chacun de trouver une réponse à plusieurs centaines de questions fréquemment posées, et, le cas échéant, d'entrer ensuite en contact avec la CNIL pour des questions plus ciblées. Le site internet de la CNIL sera par ailleurs refondu au cours de l'année, afin de privilégier une approche par type de public et, ainsi de constituer un service public numérique de référence. À cet égard, la forte implication de la CNIL sur les réseaux sociaux (38 000 followers sur Twitter, soit la 18ème institution publique) contribue également à une large diffusion des conseils et informations.

La protection des données est donc au cœur des enjeux contemporains : droit fondamental reconnu à toute personne, protégé et garanti par la CNIL, elle constitue également une condition de développement de l'innovation et des services numériques. Il s'agit de construire aujourd'hui un cadre éthique, juridique et technologique de confiance. Ceci passe par un cadre réglementaire adapté – c'est le sens du règlement européen qui sera adopté cette année et des travaux du Législateur – mais aussi par une régulation pragmatique, concertée, et tournée vers les différents publics concernés (pouvoirs publics, entreprises, citoyens). Tel est le sens de l'action, dévouée et fidèle aux principes et valeurs fondamentaux de notre État de droit, des 189 agents qui travaillent au service de la Commission. ■

> “La protection des données constitue une condition de développement de l'innovation et des services numériques.”

1. ANALYSES JURIDIQUES

DROIT AU DÉRÉFÉRENCEMENT : UNE AVANCÉE IRRÉVERSIBLE

Le 13 mai 2014, la Cour de Justice de l'Union européenne a rendu un important arrêt dans une affaire "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (C-131/12).

De nombreux commentateurs de cet arrêt ont communément souligné son caractère inédit, le présentant comme consacrant un « droit à l'oubli ». Telle n'est pourtant pas la réalité du droit consacré par la Cour : il s'agit en réalité, pour les personnes, de la possibilité d'obtenir des moteurs de recherche le déréférencement de certaines de leurs données, dans certaines conditions. Ce droit au déréférencement ne constitue pas davantage une révolution juridique : il est la déclinaison, pour le cas particulier des moteurs de recherche, des droits d'accès, d'effacement et d'opposition, que consacre la loi « Informatique et Libertés » en France depuis 1978, et la directive 95/46/CE dans l'ensemble de l'Union européenne depuis 1995.

Pour autant, l'arrêt comporte des éléments d'importance fondamentale pour le droit européen en matière de protection des personnes au regard du traitement de leurs données à caractère personnel.

> La Cour a renforcé de manière significative les droits des personnes vis-à-vis des moteurs de recherche.

LE POINT DE DÉPART : L'AFFAIRE « COSTEJA »

En 2010, M. Costeja, citoyen espagnol, a adressé une plainte à l'autorité de protection des données espagnole à l'encontre d'un éditeur de site de presse en ligne intitulé « La Vanguardia », d'une part, et des sociétés Google Spain and Google Inc., d'autre part. M. Costeja considérait que l'accessibilité, via les résultats obtenus en saisissant ses nom et prénom dans le moteur de recherche, à une notice légale publiée sur ce site relative à la saisie et mise aux enchères de son bien immobilier pour défaut de paiement portait atteinte à son droit à la protection des données. Il considérait en effet que les informations disponibles sur Internet le concernant n'étaient plus pertinentes, la procédure le concernant ayant été clôturée depuis plusieurs années. Il demandait par conséquent à l'autorité qu'il soit enjoint au journal en ligne d'effacer ou de modifier les pages en question afin que ses données n'y apparaissent plus, et à Google Spain ou Google Inc. que les données personnelles le concernant n'apparaissent plus dans les résultats de recherche.

L'autorité espagnole a rejeté la première réclamation de M. Costeja visant le site, estimant que la publication des informations en cause sur ce site était justifiée dès lors qu'elle avait eu lieu sur ordre du ministère du Travail et des Affaires sociales et visait précisément à conférer une publicité maximale à la vente publique afin de réunir le plus grand nombre d'enchérisseurs. En revanche, elle a accueilli la réclamation dirigée contre Google Spain et Google Inc, considérant que les exploitants de moteurs de recherche sont soumis à la législation espagnole en matière de protection des données. Ils sont par conséquent tenus de répondre favorablement aux demandes d'effacement et d'opposition émanant de personnes physiques quant aux données les concernant, dès lors que celles-ci sont légitimes. C'est alors que les sociétés Google Inc. et Spain ont interjeté appel de cette décision devant la juridiction espagnole compétente.

De la réponse relative aux obligations qui incombent aux moteurs de recherche en matière de protection des données personnelles dépendait l'interprétation de plusieurs dispositions de la directive européenne 95/46/CE. Saisie du litige opposant Google à M. Costeja et à l'autorité espagnole, la juridiction espagnole a donc décidé de poser à la Cour de Justice de l'Union européenne trois questions précises quant à l'interprétation de ce texte. La Cour, saisie de ce renvoi préjudiciel, a renforcé de manière significative les droits des personnes vis-à-vis des moteurs de recherche. ■

LES PRINCIPAUX ENSEIGNEMENTS DE L'ARRÊT « GOOGLE SPAIN » DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

Applicabilité de la directive 95/46/CE aux moteurs de recherche

Le premier apport majeur de l'arrêt de la Cour, consiste à **qualifier les activités des moteurs de recherche de « traitements de données à caractère personnel »** au sens de l'article 2(b) de la directive 95/46/CE. Ces activités consistent en effet « *à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné* ». Ces informations publiées portent, entre autres, sur des données personnelles. L'exploitant de ce moteur de recherche doit être considéré comme le «responsable» dudit traitement, au sens de l'article 2(d) de la même directive.

En retenant cette qualification, la Cour a écarté l'argument des moteurs selon lesquels ceux-ci, n'étant pas à l'origine des données accessibles à travers leurs services, ne sauraient voir peser sur eux aucune responsabilité au sens de ce texte – argument que le G29 contestait depuis plusieurs années déjà.

Applicabilité du droit européen à la société Google Spain, bien que le serveur à partir duquel sont traitées les données du plaignant se trouve aux États-Unis

Le second apport de l'arrêt consiste à **retenir la pleine application des règles européennes de protection des données aux moteurs de recherche**, au motif que ceux-ci sont établis sur le territoire européen du fait du modèle économique de leurs activités.

En effet, ceux-ci doivent être considérés comme étant « établis » sur le territoire européen au sens de l'article 4(1)(a) de la directive 95/46/CE. Le raisonnement de la Cour est le suivant : un traitement de données à caractère personnel est bel et bien effectué « *dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre* », au sens de cette disposition, dès lors que le moteur de recherche crée dans un État membre une succursale ou une filiale destinée, en l'espèce, à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre. L'existence de cet établissement a pour conséquence de le soumettre au droit européen.

Possibilité pour toute personne physique de demander que ses données ne soient plus accessibles via un moteur de recherche sur le fondement du droit européen

Tirant les conséquences logiques de l'application des dispositions de la directive 95/46/CE aux moteurs de recherche, la Cour estime que ceux-ci sont tenus de respecter les droits d'accès et d'opposition que prévoient ses articles 12 et 14.

Dans cette configuration, l'exercice de ces droits par les personnes se traduit par **la possibilité d'obtenir d'un moteur de recherche la suppression d'un ou plusieurs résultats de la liste de résultats associés à leurs données personnelles** (en pratique, leurs nom et prénom).

Ces moteurs doivent supprimer de la liste de résultats des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, dès lors que les conditions d'exercice de ces droits sont réunies. Ce droit peut être exercé de manière autonome, c'est-à-dire que son exercice peut être justifié même si ces données personnelles ne sont pas effacées préalablement ou simultanément de ces pages web – y compris, le cas échéant, alors même que leur publication en elle-même sur lesdites pages est licite. En effet, s'il est fait droit à la demande, l'information figurant sur le site source ne disparaît pas, mais crée une impossibilité de retrouver ledit site à partir d'une recherche comprenant le nom et le prénom de la personne par exemple.

Dès lors qu'il consiste en une application du droit commun aux moteurs de recherche, **le droit au déréférencement apparaît alors comme le prolongement logique de ces deux consécrations jurisprudentielles, et non comme la nouveauté juridique si souvent annoncée**.

L'application pratique de cet arrêt, en revanche, pose des questions nouvelles et d'une ampleur inédite pour les acteurs impliqués - au premier rang desquels figurent les moteurs de recherche qui ont vu affluer des dizaines de milliers de demandes depuis l'arrêt de la Cour.

Ces questions se sont également posées aux autorités de protection des données européennes, qui sont saisies des décisions de refus que les moteurs opposent aux personnes ayant exercé leurs droits directement auprès d'eux. Dans un souci d'une mise en œuvre cohérente du droit consacré par la Cour, les autorités européennes réunies au sein du G29 ont adopté des lignes directrices communes pour aborder ces questions de manière concertée. ■

LA MISE EN ŒUVRE DU DROIT AU DÉRÉFÉRENCEMENT : LES LIGNES DIRECTRICES DU G29

Le 26 novembre 2014, Le G29 a adopté deux documents pour permettre la mise en œuvre du droit au déréférencement : d'une part, une interprétation commune de l'arrêt, d'autre part, des critères communs pour l'instruction des plaintes qui leurs sont adressées à la suite d'un refus de déréférencement.

Depuis cette date, la CNIL utilise ces outils pour examiner les plaintes qui lui sont soumises par les internautes et confirmer, ou non, les décisions de refus déréférencement que ceux-ci ont essuyées de la part des moteurs de recherche. A cet égard, plusieurs éléments sont importants à souligner.

Qui peut faire valoir son droit au déréférencement ?

Comme l'a rappelé la Cour, la protection des personnes au regard du traitement de leurs données à caractère personnel est un droit fondamental consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. À ce titre, « toute personne physique » a droit à la protection de ses données et peut, sous certaines conditions, obtenir le déréférencement d'une information, par exemple quand elle est périmée ou inexacte.

Pour autant, en pratique, les autorités de protection européennes sont amenées à instruire les demandes des personnes ayant un lien clair et certain avec l'Union européenne, qu'elles soient citoyennes ou résidentes d'un pays membre de l'Union. Ainsi, s'agissant de la CNIL, tout ressortissant français ou personne résidant en France peut la saisir à la suite d'un refus de déréférencement.

À cela s'ajoute que, comme c'est le cas pour la plupart des droits dont disposent les personnes au titre de la loi du 6 janvier 1978, une demande de déréférencement est un droit que seule la personne concernée peut exercer, un tiers ne pouvant le faire à sa place.

Comment concilier droit au déréférencement et droit à l'information ?

La question de la conciliation entre droit au déréférencement, liberté d'expression et droit du public à avoir accès à l'information a été posée de manière récurrente par les commentateurs de la décision de la Cour de justice.

Or, **l'application du droit au déréférencement n'est pas absolue mais doit être conciliée avec ces autres libertés fondamentales**. Ainsi, le droit au déréférencement est entouré de garde-fous qui assurent sa mise en œuvre équilibrée et respectueuse de ces autres droits et libertés, également garantis par la Charte européenne des droits fondamentaux.

En premier lieu, **le déréférencement ne conduit pas à la suppression d'un contenu d'internet**. Il empêche uniquement que, sur la base de la saisie d'un nom, certaines informations apparaissent dans la liste des résultats d'un moteur de recherche. Le contenu déréférencé reste ainsi disponible sur le site source et peut être retrouvé par des requêtes effectuées sur la base d'autres mots clés figurant eux aussi dans le contenu en ligne.

> Le droit au déréférencement est entouré de garde-fous qui assurent sa mise en œuvre équilibrée et respectueuse des autres droits et libertés.

Déréférencement et demande de suppression du contenu sont en effet deux procédures indépendantes, qui n'ont pas le même objet. Une personne peut ainsi présenter sa demande de déréférencement indépendamment de toute demande d'effacement de l'information auprès de l'éditeur du site ou de l'hébergeur. À l'inverse, la circonstance qu'une personne ait obtenu le déréférencement d'une URL sur un moteur de recherche n'exonère pas l'éditeur du site de sa responsabilité en cas de demande d'effacement qui lui serait directement formulée.

En deuxième lieu, **la décision de déréférencement n'est pas automatique** : toute demande doit faire l'objet d'*une appréciation au cas par cas*, et peut être rejetée lorsque, compte tenu par exemple du rôle public de la personne concernée, le droit à l'information du public prévaut.

C'est pourquoi l'articulation entre le droit au déréférencement et le droit du public à avoir accès à l'information est un point essentiel d'attention des autorités de protection dans le cadre de l'instruction des demandes de déréférencement. Pour ce faire, elles appliquent un contrôle de proportionnalité tel qu'elles en opèrent quotidiennement dans le cadre de leurs activités (par exemple pour déterminer si les données collectées en vue de la création d'un fichier sont proportionnées au regard de la finalité poursuivie).

S'agissant des éléments à prendre en considération pour opérer cette « balance d'intérêts », l'arrêt de la CJUE indique uniquement que la prépondérance de principe du droit au déréférencement sur le droit du public à l'information peut être remise en question pour des raisons particulières, telles que, par exemple, « *le rôle joué par la personne concernée dans la vie publique* ».

Sur la base des indications données par la Cour, les autorités de protection ont constitué un faisceau d'indices à appliquer au cas par cas pour se prononcer sur les plaintes leur parvenant en cas de refus de déréférencement. C'est à cet usage qu'ont été destinés les **critères communs adoptés par le G29** le 26 novembre 2014.

INFOS +

Les critères communs adoptés par le G29

Les critères retenus consistent en une série de questions qui, combinées entre elles, permettent de déterminer si l'information figurant dans le moteur de recherche doit ou non être déréférencée. Ces critères portent tant sur la personne qui exerce son droit au déréférencement que sur le contenu incriminé lui-même, ou sur le contexte de sa mise en ligne.

Ces critères s'articulent autour de 3 séries de questions :

▸ En ce qui concerne ***la personne dont émane la demande de déréférencement***, les autorités doivent tout d'abord vérifier qu'il s'agit d'une personne physique puisque cela conditionne la recevabilité de sa démarche. Elles doivent ensuite déterminer s'il s'agit d'une personne jouant un rôle dans la vie publique. Ce critère figurant explicitement dans l'arrêt de la Cour, il est crucial dans l'orientation de la décision. **Plus la personne est active et impliquée dans la vie publique, moins le déréférencement est susceptible d'être acquis**. Enfin, **est pris en considération le fait que le demandeur soit ou non mineur au moment de la mise en ligne du contenu**, puisqu'il appartient aux autorités de prendre en compte « l'intérêt supérieur de l'enfant » consacré par l'article 24 de la Charte des droits fondamentaux, qui milite plutôt en faveur d'un déréférencement.

▸ ***Les critères portant sur le contenu*** mis en ligne visent à déterminer si l'information est exacte, pertinente ou au contraire excessive. Il est ainsi examiné si elle est en lien avec l'activité professionnelle de la personne ou sa vie intime. Le référencement d'une information apparaît naturellement plus pertinent lorsque celle-ci relève de la sphère professionnelle, même s'il convient de prendre en considération le métier exercé par la personne concernée et l'intérêt du public à avoir accès à cette information. De même, la nature injurieuse de l'information est prise en compte. Sans préjudice de la qualification pénale qui pourrait être retenue par un juge, les autorités apprécient ici le caractère excessif de l'information comme elles le font pour n'importe quel traitement. Par ailleurs, le fait qu'il s'agit ou non d'une information sensible, c'est-à-dire renvoyant par exemple à la santé ou aux orientations sexuelles d'une personne, est pris en compte. Ce type d'informations a évidemment un impact plus important sur la vie privée des personnes que d'autres données plus ordinaires. Enfin, même s'il n'y a pas d'obligation pour les personnes de le démontrer, l'existence d'un préjudice ou d'un risque lié à la diffusion des informations visées par la demande constitue un facteur en faveur du déréférencement.

▸ La troisième série de ***questions relatives au contexte de mis en ligne*** vise notamment à déterminer si la personne ne pouvait ignorer la diffusion des informations ou si, au contraire, cela s'est fait à son insu, ce qui est de nature à faire pencher la balance en faveur d'un déréférencement. Le vecteur de mise en ligne est également un élément essentiel de l'appréciation qui sera portée sur la demande. Ainsi, **le fait que la diffusion d'une information s'effectue par un organe de presse pèse dans l'évaluation qui sera faite d'une demande de déréférencement**. Toutefois, cela ne saurait conduire de manière systématique à refuser un déréférencement. Ce critère doit être combiné avec d'autres, par exemple celui de la durée de la diffusion ou du préjudice pour la personne concernée. C'est la même démarche qui sera adoptée concernant les données mises en ligne pour répondre à une obligation légale et qui, en première analyse, n'ont pas vocation à être déréférencées sauf, par exemple, si la durée de diffusion est dépassée ou l'information périmée.

Outre le fait que ces critères doivent permettre d'assurer le caractère objectif des décisions prises sur les refus de déréférencement et ainsi renforcer leur sécurité juridique, ils sont aussi les garants d'une harmonisation des pratiques entre les autorités de protection des données à l'échelle européenne. Néanmoins, ces exigences doivent aussi être conciliées avec la nécessaire prise en compte des spécificités nationales, qu'elles soient culturelles ou légales, et le caractère évolutif des critères soumis à la prise en compte de l'expérience acquise au fil de l'instruction au cas par cas ou des décisions de justice prises en matière de déréférencement.

Quelle portée du déréférencement sur Internet ?

S'agissant de la portée territoriale du droit au déréférencement, les autorités réunies au sein du G29 considèrent que pour donner plein effet à l'arrêt de la Cour de justice, les décisions de déréférencement doivent être mises en œuvre de manière à garantir effectivement la protection des droits fondamentaux des personnes et à ne pas permettre leur contournement.

À cet égard, limiter le déréférencement aux extensions européennes des moteurs de recherche en considérant que les utilisateurs effectuent généralement des requêtes à partir des extensions nationales du moteur ne garantit pas l'application de ce droit de manière satisfaisante. Cela signifie donc, en pratique, que **le déréférencement doit être effectif sur toutes les extensions d'un nom de domaine, européennes, ou non, y compris (mais non seulement) l'extension.com**.

Par ailleurs, le droit au déréférencement n'est qu'une déclinaison au cas particulier des moteurs de recherche du droit d'opposition consacré en France depuis l'entrée en vigueur de la loi du 6 janvier 1978. À ce titre, le traitement mis en œuvre dans le cadre du moteur de recherche n'est qu'un seul et unique traitement décliné sous la forme d'extensions nationales (.fr, .uk, .ru, .ca…).

Il résulte de ces deux éléments que le droit d'opposition exercé par les personnes doit être effectif sur toutes les extensions, celles-ci n'étant que des chemins d'accès techniques « locaux » à un traitement unique.

Les enjeux liés à cette question peuvent aisément être illustrés par un cas concret dont la CNIL a été saisie. ▸▸▸

HISTOIRE VÉCUE

Un ressortissant français travaillant à l'international et d'origine extra-européenne a demandé le déréférencement de contenus diffamants et injurieux le concernant. Le moteur de recherche concerné a accepté leur déréférencement mais uniquement à partir de l'extension française. Pour autant, les proches de cette personne vivant encore dans son pays d'origine ainsi que ses relations professionnelles situées hors de France continuaient à accéder aux informations incriminées, sur la base de la saisie de son nom. C'est pourquoi la personne a décidé de saisir la CNIL pour obtenir un déréférencement global.

Dans le même temps, la CNIL a reçu **138 demandes en 2014**. Le nombre d'adresses URL concernées par ces demandes était de 702 (environ 5 URL par plainte). Ces demandes étaient au nombre de 211 en mars 2015.

Dans 92 % des cas, Google motive son refus par le fait que l'information mise en ligne est en lien avec l'activité professionnelle de la personne ou qu'elle reste pertinente au regard de l'actualité ou de la finalité du traitement, sans plus de précision. Ces motifs peuvent être combinés avec d'autres, tels que le fait que l'information a été mise en ligne par le gouvernement ou la personne à l'origine de la demande de déréférencement ou le fait que la personne joue un rôle dans la vie publique.

À l'issue de la phase de concertation européenne, la CNIL a procédé à l'instruction des refus opposés par Google et a adressé en décembre 2014 ses premières demandes de déréférencement sur les dossiers pour lesquels elle a estimé que le moteur de recherche avait commis une erreur d'appréciation.

Dans le même temps, elle a continué à participer aux travaux du groupe de travail européen sur cette question afin de maintenir un fort niveau de coopération entre les autorités. Ces échanges sur des cas concrets de refus de déréférencement sont le moyen d'assurer une cohérence dans les décisions prises.

Au vu de ce qui précède, il est prévisible que le traitement de ce dossier du droit au déréférencement se prolongera sur l'année 2015. ■

▸▸▸ Cet exemple révèle que le déréférencement partiel des informations conduit à l'absence de prise en compte effective des droits des personnes et, possiblement, à la persistance d'un préjudice tant dans leur vie personnelle que professionnelle. La CNIL et ses homologues européens seront donc amenés à envisager les suites qu'elles souhaiteront donner aux éventuels refus persistants de moteurs de recherche qui considèrent qu'une application du droit au déréférencement sur l'ensemble des extensions, y compris non-européennes, constituerait une application extraterritoriale injustifiée du droit européen.

Les principes et outils à l'épreuve du quotidien

Au cours de l'année 2014, Google a reçu environ **170 000 demandes de déréférencement**, dont à peu près 40 000 provenaient de France, soit un peu moins de 25 % du total des saisines. À cela s'ajoute le fait que, bien souvent, une demande de déréférencement porte sur plusieurs adresses URL renvoyant à un contenu sur internet. C'est ainsi que depuis mai 2014, date de l'arrêt de la Cour, le moteur de recherche a dû se prononcer sur le déréférencement de plus de 800 000 URL qui correspondant à moins de 300 000 demandes (mars 2015). Globalement, dans la moitié des cas, les demandes de déréférencement ont été acceptées par Google.

... HISTOIRES VÉCUES

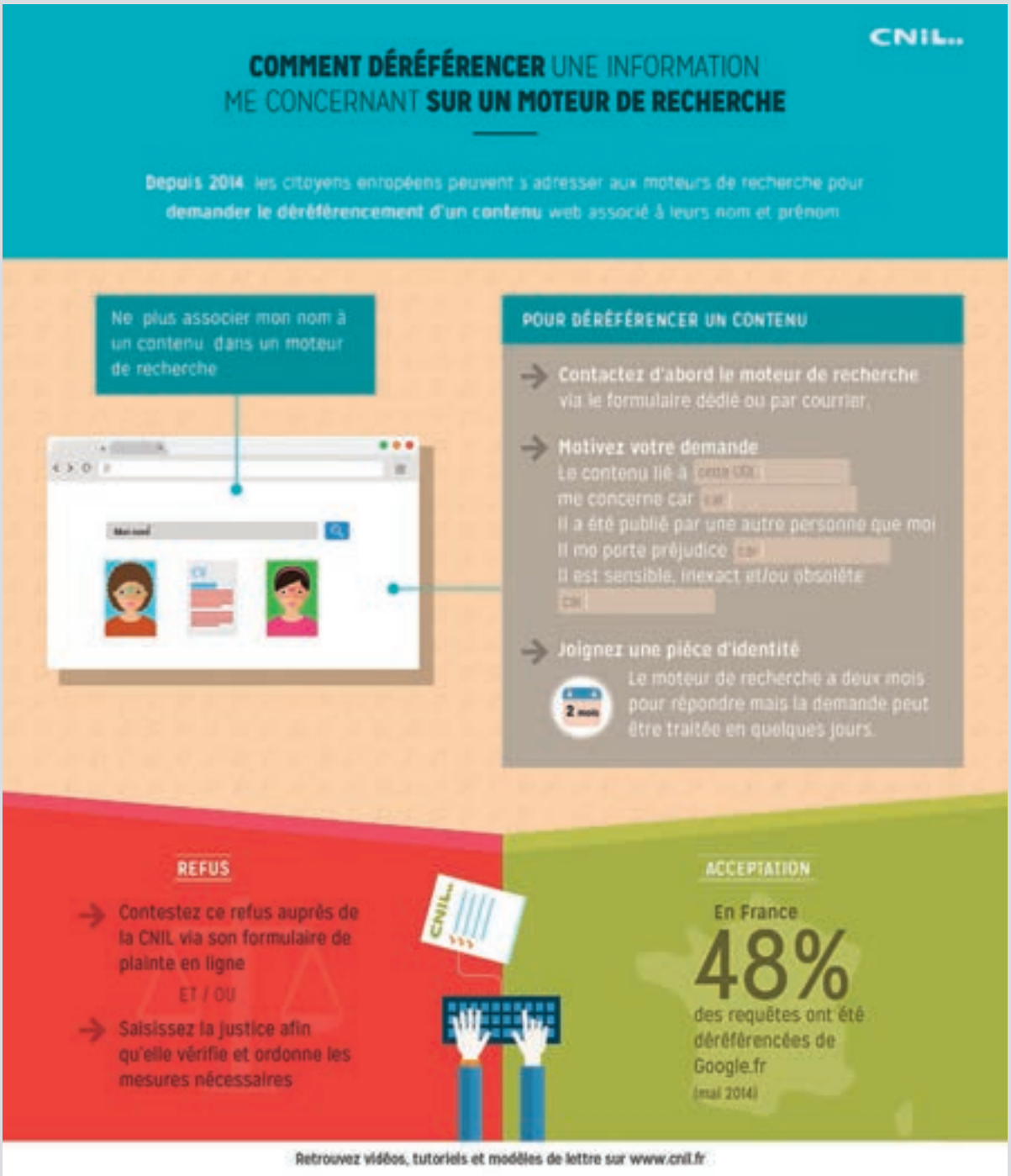
▸ Un homme demande le déréférencement d'un article publié dans un quotidien régional au sujet d'une garde à vue, non suivie d'une condamnation, datant de 1998. Google a accepté de déréférencer.

▸ Une femme constate qu'un blog diffuse des données la concernant. Elle n'arrive pas à obtenir la suppression des données en contactant son auteur, car celui-ci ne dispose plus de l'accès au blog. Google refuse dans un premier temps le déréférencement au motif de l'intérêt du public concernant son aptitude professionnelle. La CNIL est intervenue afin d'appuyer sa demande auprès de Google qui a finalement procédé au déréférencement du lien concerné.

▸ Une internaute constate en tapant ses nom et prénom sur un moteur de recherche qu'il renvoie vers des URL de sites pornographiques. Sa demande de déréférencement lui a été refusée dans un premier temps puis acceptée dans un second temps après l'intervention de la CNIL.

▸ Un homme souhaite obtenir le déréférencement d'un arrêt publié sur un site anglo-saxon de manière nominative alors que l'arrêt est anonymisé sur le site français à l'origine de la publication. Google a accepté le déréférencement.

▸ Condamné pénalement en première instance, Monsieur X. a été relaxé en appel en 2006. À la suite de l'institution, au mois de mai 2014, d'un droit au déréférencement, il demande au moteur de recherche de déréférencer un lien apparaissant dans les résultats d'une recherche faite sur son identité et renvoyant à un article relatif à cette affaire. Le moteur de recherche refuse au nom de l'intérêt du public à avoir « connaissance de cette information pertinente eu égard aux fins du traitement de données ». Monsieur X. a donc saisi la CNIL de ce refus, qui a considéré que cette information n'avait pas été mise à jour à la suite de sa relaxe et lui causait donc un préjudice tant personnel que professionnel. À la suite de l'intervention de la CNIL, le moteur de recherche a déréférencé le lien hypertexte concerné dans les déclinaisons européennes du moteur de recherche.


CNIL.
COMMENT DÉRÉFÉRENCER UNE INFORMATION ME CONCERNANT SUR UN MOTEUR DE RECHERCHE
Depuis 2014, les citoyens européens peuvent s'adresser aux moteurs de recherche pour demander le déréférencement d'un contenu web associé à leurs nom et prénom
Ne plus associer mon nom à un contenu dans un moteur de recherche
POUR DÉRÉFÉRENCER UN CONTENU
Contactez d'abord le moteur de recherche via le formulaire dédié ou par courrier.
Motivez votre demande
Le contenu lié à
me concerne car
Il a été publié par une autre personne que moi
Il me porte préjudice
Il est sensible, inexact et/ou obsolète
Joignez une pièce d'identité
2 mois
Le moteur de recherche a deux mois pour répondre mais la demande peut être traitée en quelques jours.
REFUS
Contestez ce refus auprès de la CNIL via son formulaire de plainte en ligne
ET / OU
Saisissez la justice afin qu'elle vérifie et ordonne les mesures nécessaires
ACCEPTATION
En France
48%
des requêtes ont été déréférencées de Google.fr
(mai 2014)
Retrouvez vidéos, tutoriels et modèles de lettre sur www.cnil.fr

COOKIES : DE LA RECOMMANDATION AUX CONTRÔLES

Les cookies et autres traceurs sont des techniques permettant de suivre les personnes utilisant des services de communication électroniques (navigation sur des sites internet, boîtes mail, applications mobiles, etc.) afin d'analyser leurs déplacements, navigation sur le web, habitudes de consommation, etc.

Ces techniques consistent à lire ou à inscrire des données sur un appareil (ordinateurs, smartphones, tablettes numériques et consoles de jeux vidéos connectées à Internet) pour suivre l'activité de son utilisateur. Elles peuvent prendre des formes variées (cookie http, cookies « flash », pixels invisibles, calcul d'empreinte du terminal ou utilisation d'identifiant généré par un logiciel ou présent dans le terminal) et répondre à différents objectifs.

Les cookies peuvent être déposés et exploités par de nombreux acteurs (éditeur de sites, régies publicitaire, annonceurs, réseaux sociaux, etc.) pour répondre à des objectifs très variés.

4 grandes familles de cookies peuvent être distinguées :

- Les cookies liés aux opérations relatives à la **publicité ciblée** (cookie permettant de savoir quelles pages/courriers électroniques ont été consultés, combien de temps, de quel site le visiteur provient, ses données sociodémographiques, etc.);
- Les cookies de **mesure d'audience** permettant d'évaluer sous forme statistique la fréquentation d'un site, les pages les plus visitées, la provenance des internautes concernés, etc., et valoriser ainsi l'audience d'un site ;
- Les cookies traceurs de **réseaux sociaux** générés par les « boutons de partage de réseaux sociaux » ;
- Les cookies **« techniques »** bénéficiant d'exemptions, ayant pour finalité exclusive de permettre ou faciliter la communication par voie électronique, ou strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur (cookies de panier d'achat pour un site de e-commerce ou des cookies pour s'authentifier sur un service en ligne, traceurs de session créés par un lecteur multimédia, traceurs persistants de personnalisation de l'interface utilisateur). ■

INFOS +

Cookies

À ce jour, le traceur le plus courant est le cookie. Il s'agit d'un fichier contenant a minima un identifiant (numéro unique permettant d'individualiser l'utilisateur de l'appareil) et le nom du serveur qui l'a envoyé. Ce fichier est déposé lorsque l'internaute effectue une requête vers le serveur web du site internet qui l'intéresse pour afficher son contenu. Ce serveur transmet alors du code à exécuter contenant non seulement les éléments de la page à afficher, mais aussi d'autres contenus tels que des images et cookies, ainsi que des instructions de dépôt ou de mise à jour de cookies. C'est ainsi que les cookies sont générés puis envoyés par le serveur du service visité, lors de la première visite et à chaque visite ultérieure.

L'ÉVOLUTION DU CADRE JURIDIQUE

La modification du régime applicable aux traceurs résulte de la réforme d'un corpus de règles européennes désignées sous le nom de « Paquet Télécom », à l'occasion de laquelle la directive dite « vie privée dans le secteur des communications électroniques » (2002/58/CE) a été modifiée (par la directive 2009/136/CE).

Cette directive a été transposée en droit français dans une ordonnance publiée le 24 août 2011 (dite ordonnance « Paquet télécom ») qui modifie notamment l'article 32-II de la loi du 6 janvier 1978.

À RETENIR

L'accord libre spécifique et éclairé prévu par l'article 32-II implique donc :
• une absence de dépôt de cookies ou autres traceurs lors de l'arrivée sur le site et tant que la personne n'a pas exprimé de choix ;
• la mise à disposition d'outil d'opposition complet, efficaces, aisément utilisables.
Une fois le consentement recueilli pour le dépôt d'un cookie répondant à une finalité donnée, le premier niveau d'information (bandeau) peut disparaître. En revanche, l'information des personnes via la rubrique dédiée (2ème niveau), doit rester aisément accessible, notamment pour leur offrir la possibilité de s'opposer à tout moment au suivi. La durée du consentement dépend de celle du traceur concerné. La CNIL recommande une durée maximale de 13 mois à l'issue de laquelle le cookie doit être supprimé et le consentement renouvelé.

Sous l'empire de l'ancien article 32-II de la loi, seule était requise l'information sur la finalité du traitement et la manière de s'opposer aux traceurs (*opt-out*). Désormais, l'accord préalable et informé de l'internaute est de rigueur avant tout accès ou inscription de données sur son terminal (*opt-in*).

C'est sur la base de cette évolution de la législation que la CNIL a publié en 2012 un premier jeu de fiches pratiques à destination des professionnels de l'internet pour faciliter leur mise en conformité avec la nouvelle réglementation.

À cette occasion la CNIL a fait part de son positionnement vis-à-vis de certains cookies de mesure d'audience regardés comme pouvant, sous conditions, bénéficier du régime des cookies techniques.

Pour faciliter la mise en œuvre de la nouvelle législation face à la persistance de difficultés pratiques, la CNIL a décidé la création d'un groupe de concertation avec les principales organisations professionnelles intéressées. Ce groupe rassemblait donc les éditeurs de site internet, les régies publicitaires et les annonceurs.

Durant l'année 2013 le groupe de travail s'est réuni périodiquement pour débattre et élaborer des solutions opérationnelles au bénéfice des professionnels en fonction des besoins exprimés.

Le 5 décembre 2013, la CNIL à publié une recommandation relative aux Cookies et aux autres traceurs. Cette recommandation a été accompagnée par la publication de nombreux développements explicatifs, fiches pratiques et outils de conformité. ■

LA RECOMMANDATION EN PRATIQUE

L'article 32-II de la loi du 6 janvier 1978 dispose désormais que « tout abonné ou utilisateur d'un service de communications électroniques doit être **informé de manière claire et complète**, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

- de la **finalité de toute action** tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
- des **moyens dont il dispose pour s'y opposer**.
- Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice **ait exprimé, après avoir reçu cette information, son accord** qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont **pas applicables si l'accès** aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit **a pour finalité exclusive de permettre ou faciliter la communication** par voie électronique ;
- **soit est strictement nécessaire à la fourniture d'un service de communication** en ligne à la demande expresse de l'utilisateur ».

La recommandation publiée par la CNIL le 5 décembre 2013 explicite la portée et les conséquences pratiques de cette nouvelle disposition, que ce soit en termes de technologies concernées, de modalités de recueil du consentement éclairé des personnes ou d'exercice de leur droit d'opposition. ▸▸▸

▸▸▸ Portée de l'article 32-II

De manière générale, l'article 32-II ne s'applique pas qu'aux cookies déposés depuis des sites internet mais à toute technologie permettant de tracer un utilisateur de service de communications électroniques en accédant à des informations contenues dans son appareil ou en inscrivant des informations dans ledit appareil, quelle que soit la nature de ce dernier (smartphone, téléphone mobile, tablette, ordinateur portable ou fixe, etc.) et que ce traçage s'opère dans le monde virtuel (internet) ou physique (déplacement des personnes).

Seuls les traceurs nécessaires à la fourniture du service demandé ou à la transmission de la communication initiée par l'internaute sont totalement exemptés. Certains cookies de mesure d'audience bénéficient par ailleurs d'un régime allégé.

Par ailleurs, les mécanismes de traçage sont exploités par de nombreux acteurs, à différents niveaux, que ce soit au stade de leur installation, de la collecte d'information, de l'enrichissement de ces informations, de leur analyse et transmission à d'autres acteurs, etc. Ces acteurs engagent leur responsabilité dès lors qu'ils exploitent les données collectées pour leur propre compte.

Par exemple, les éditeurs de site décident des traceurs déposés depuis leur site, facilitent leur dépôt et leur lecture par leurs partenaires, lesquels vont à leur tour décider de la manière d'exploiter ces cookies, etc. Sur la base de ce constat, la CNIL les considère comme co-responsables.

Par ailleurs, il est important de noter que, même si la directive et la loi visent indistinctement l'ensemble des informations lues ou inscrites sur le terminal d'un utilisateur, les données collectées par l'intermédiaire des traceurs ont un caractère personnel. En effet, les traceurs ont pour premier objet de singulariser la personne. Les informations collectées par leur biais sont forcément reliées à cette dernière et constituent en ce sens des données à caractère personnel dont le traitement requiert le respect de la loi « Informatique et Libertés » dans son ensemble, notamment en termes d'information des personnes sur les destinataires de leurs données et d'encadrement de ces transmissions, y compris lorsqu'elles impliquent des acteurs établis dans des pays n'offrant pas un niveau de protection adéquat.

FOCUS

Les cookies de mesures d'audience exemptés du recueil du consentement

La CNIL, suivant en ce sens un avis du groupe de l'article 29 (réunissant les autorités de protection des données européennes), a aménagé le régime des cookies de mesure d'audience.
Consciente de la nécessité pour les éditeurs de connaître l'audience de leur site internet ou de leur application, notamment afin d'organiser leur contenu ou de détecter des problèmes de navigation, la CNIL exempte du recueil du consentement (mais pas de l'information préalable et de la faculté de s'opposer *a posteriori*) les techniques réunissant les caractéristiques suivantes :
• leur finalité est limitée à la mesure d'audience du contenu visualisé afin de permettre une évaluation des contenus publiés et de l'ergonomie du site ou de l'application ;
• l'utilisation du cookie déposé est strictement cantonnée à la production de statistiques anonymes ;
• les données collectées ne sont pas recoupées avec d'autres traitements (fichiers clients ou statistiques de fréquentation d'autres sites par exemple) ;
• les cookies utilisés ont une portée limitée à un seul éditeur et ne permettent pas le suivi de la navigation de la personne utilisant différentes applications ou naviguant sur différents sites internet ;
• les adresses IP éventuellement collectées aux fins de géolocalisation ne permettent pas de situer la connexion de manière plus précise que la ville depuis laquelle elle est initiée (par le biais de la suppression des deux premiers octets si nécessaire) et sont supprimées une fois la géolocalisation opérée ;
• les cookies utilisés ainsi que les informations collectées par leur biais ne sont pas conservées au-delà de 13 mois.

Obligations découlant de l'article 32-II

Toute personne doit être informée de la finalité des traceurs et pouvoir les refuser ou les accepter (donc exprimer sans ambigüité son choix) avant leur installation. Elle doit également pouvoir revenir sur son accord à tout moment.

Par sa recommandation du 5 décembre 2013, la Commission a rappelé que le consentement doit avant tout « *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* ». Ces principes doivent éclairer les professionnels dans le choix de solutions conviviales et ergonomiques que la CNIL examinera *in concreto*.

En pratique, la CNIL propose une cinématique en deux étapes pour les éditeurs de site internet : la première étape consiste à informer directement et immédiatement l'internaute, lorsqu'il arrive sur le site, des modalités d'expression de son consentement et de la portée de ce dernier. Qu'il s'agisse du fait de cliquer sur une image ou de faire défiler intentionnellement la première page consultée, l'internaute doit avoir pleinement conscience des conséquences de son action pour que celle-ci traduise son accord au dépôt de cookies.

Cette première étape (en termes d'information immédiate de l'internaute) doit intégrer un renvoi vers une page correspondant à la seconde étape de la cinématique proposée par la CNIL, explicitant la finalité des traceurs et la manière de s'y opposer avant et après leur dépôt.

Aucun traceur ne doit être utilisé, sauf exception, tant que la personne n'a pas

exprimé son choix, que ce soit en réalisant l'action indiquée comme manifestant son accord (poursuite de la navigation, clic sur un lien, etc.) ou en refusant leur présence, par les moyens mis à sa disposition dans la seconde page d'information.

L'accord de l'internaute ne sera en tout état de cause valable que s'il dispose d'un moyen simple et intelligible de s'opposer à chaque famille de cookies, avant de poursuivre sa navigation. À défaut, l'accès au site (et la poursuite de la navigation) impliquerait une acceptation contrainte de traceurs notamment publicitaires. Or, l'accord exigé par l'article 32-II doit se traduire par une « *manifestation de volonté, libre, spécifique et informée* ». Le choix de l'internaute ne pourra pas être considéré comme libre s'il ne peut exprimer son refus sans encourir des conséquences négatives telles que l'impossibilité d'accéder au site.

L'accord exprimé par la personne poursuivant sa navigation (par exemple) ne sera donc pas valable :

- si les moyens mis à sa disposition pour refuser les traceurs et exprimer par ce biais son choix sont incomplets, inefficients ou inintelligibles,
- s'il est obligé d'accepter les cookies pour accéder au site.

L'ensemble de ces principes sont transposables aux applications sur smartphone, sur télévision intelligentes, liseuses, etc.

En pratique, il est donc essentiel de vérifier l'efficacité du dispositif proposé, qu'il s'agisse de gestion des tags via un outil maîtrisé par l'éditeur du site ou la régie ou encore de paramétrer un outil à la disposition de l'internaute. L'explication quant à la manière de procéder doit être claire et complète et un renvoi global vers les paramétrages du navigateur de l'internaute ne saurait nécessairement suffire. L'efficacité du dispositif suppose de vérifier que lesdits paramétrages permettent à l'internaute d'exprimer son choix de manière différenciée pour chaque grande famille de cookies, sans que cela ne soit préjudiciable pour son confort de navigation.

À titre d'exemple, le renvoi vers les paramétrages ne sera pas satisfaisant s'il concerne des cookies publicitaires internes au site (*cookies first*). En effet, de nombreux navigateurs n'offrent que deux options en termes d'opposition, en identifiant les cookies non pas par leur finalité mais en fonction de leur provenance (origine interne au site ou externe). Or les cookies internes peuvent répondre à différents besoins techniques conditionnant l'accès au site et le confort de navigation. Refuser les *cookies first* , sans distinction au vu de leur utilité, peut sérieusement nuire à la navigation de l'internaute et compromettre la fourniture du service demandé. L'acceptation de l'internaute dans un tel cas n'est pas libre.

De même, en l'état, les paramétrages du navigateur ne permettent que la gestion des « cookies http » et n'offrent aucune solution en ce qui concerne les « cookies flash », ou les techniques de *fingerprint* par exemple. ■

> Aucun traceur ne doit être utilisé, sauf exception, tant que la personne n'a pas exprimé son choix.

INFOS +

Illustration de la cinématique en 2 étapes sur un site marchand

1ère étape : affichage d'un bandeau d'information complet dès l'arrivée sur le site, indiquant « *En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour vous proposer des publicités adaptées à vos centres d'intérêts et réaliser des statistiques. Pour en savoir plus et paramétrer les cookies (lien hypertexte)*».
2ème étape : la rubrique accessible via le lien « *en savoir plus* » permet, de manière simple et intelligible, de refuser tout ou partie des Cookies nécessitant un recueil du consentement.

INFOS +

Fingerprinting

Le « fingerprinting » consiste à générer l'empreinte d'un terminal (ordinateur, smartphone, tablette) sur la base d'informations qui sont stockées à l'intérieur de ce terminal, telles que la version de certains logiciels ou les polices de caractères installées. Hormis la version du navigateur et du système d'exploitation, les autres informations doivent être explicitement demandées par le serveur qui, de ce fait, accède aux informations stockées dans le terminal.
À l'inverse du traçage par cookies, le fingerprinting ne nécessite pas de stocker des informations sur le terminal de l'utilisateur.
Les mêmes obligations doivent s'appliquer concernant le recueil du consentement En 2013, la recommandation de la CNIL indiquait qu'il était nécessaire d'obtenir le consentement de l'utilisateur avant de prendre l'empreinte de son navigateur, sauf si cette technique est nécessaire pour fournir un service demandé par l'utilisateur. La recommandation publiée par le G29 a confirmé cette interprétation de la directive européenne.

INFOS +

Do Not Track

Certains internautes souhaitent ne pas avoir à indiquer systématiquement, lors de la visite de chaque site, qu'ils refusent les cookies quand ils naviguent sur Internet, surtout s'ils effacent leur cookie après chaque visite. Pour leur permettre d'indiquer leur préférence directement dans leur navigateur et de ne pas avoir à se re-prononcer par la suite, un groupe de travail du W3C (consortium publiant les normes du web) a travaillé pendant plusieurs années sur le mécanisme DoNotTrack (DNT). Ce mécanisme, déjà présent dans de nombreux navigateurs, prend la forme d'une case à cocher dans votre navigateur et centralise les demandes de consentement.
Si l'adoption par les navigateurs fut rapide, très peu de sites respectent cette préférence quant les internautes l'ont renseignée, car le DNT n'a pas encore été complètement normalisé. En 2014, un consensus a été trouvé sur une normalisation technique, et une consultation publique a été ouverte sur ce projet de norme. Dans sa recommandation sur les cookies et autres traceurs, la CNIL a clairement indiqué que les sites devront prendre en compte les signaux DNT envoyés par les internautes. La normalisation définitive du mécanisme DNT devrait être effective dès 2015, pour que les sites l'adoptent rapidement.

ACCOMPAGNER LES INTERNAUTES

Les cookies et traceurs restent un concept obscur pour beaucoup d'internautes. Pour les aider à mieux appréhender les principes de fonctionnement et les enjeux du traçage sur internet, la CNIL met à disposition sur son site des outils, fiches et vidéo pédagogiques, depuis une adresse simple à retenir : « www.cnil.fr/cookies ».

Les conseils en question sont immédiatement applicables par l'internaute : ils apportent des solutions simples pour paramétrer son navigateur, ajouter des extensions au navigateur, maîtriser les cookies résultant de la présence de boutons sociaux ou bloquer le chargement de ressources provenant de sites tiers, lorsque l'internaute consulte un site internet.

Même si elles ne sauraient remplacer à long terme les mécanismes de demande de consentement et d'opposition au dépôt de cookie mis en place par les sites, les extensions de navigateurs permettent aux internautes de s'opposer au dépôt de certains cookies sur tous les sites. La CNIL a étudié le vaste panorama de solutions proposées, allant des outils bloquant tout type de contenu externe (outils pouvant être difficiles à paramétrer) aux outils bloquant toutes les publicités, en passant par les outils spécialisés dans le blocage de cookies tiers.

Par ailleurs elle suit le déploiement des technologies de traçage, telles que le *fingerprinting* (voir encadré), et tente de référencer des outils permettant de détecter ces nouvelles techniques.

La CNIL propose des outils pour les 4 navigateurs internet les plus utilisés. En fonction de son navigateur, l'internaute est redirigé vers la page dédiée afin de paramétrer son navigateur pour bloquer systématiquement les « cookies tiers » (cookies qui sont les plus utilisés pour des finalités de suivi de la navigation, notamment pour la publicité ciblée) et d'installer les outils qui le rendent plus difficile à tracer.

Pour les outils qui nécessitent un paramétrage particulier, comme la gestion des « cookies flash », leur paramétrage est également présenté. Depuis peu, une rubrique

dédiée pour les smartphones et autres terminaux mobiles est aussi proposée. Elle recense les principaux outils disponibles pour ces plateformes. La CNIL reste à l'écoute des internautes et étudie les différents outils que ceux-ci lui recommandent.

Enfin, la CNIL met à disposition depuis son site un outil – dénommé Cookieviz – permettant de visualiser en temps réel les cookies déposés lors de la navigation et de mesurer l'ampleur du traçage. En l'installant les internautes peuvent découvrir la face cachée de leur navigation, voir les destinataires des données captées lorsqu'ils visitent un site d'information, de commerce en ligne, un réseau social et identifier les croisements potentiels.

CookieViz a été téléchargée plus de 100 000 fois. C'est un outil open source dont le code de l'application est librement accessible et peut être modifié ou enrichi par toute personne qui souhaiterait contribuer. ■

ACCOMPAGNER LES PROFESSIONNELS

Les services de la CNIL répondent quotidiennement par téléphone et courrier, aux questions techniques comme juridiques des professionnels, relatives à l'application de l'article 32-II . À ces occasions sont rappelés l'applicabilité de la loi à de nombreuses techniques de traçage, le caractère préalable du consentement, les formes dans lesquelles celui-ci peut se manifester, la précision des informations à fournir aux internautes, etc.

Cette dimension de conseil et d'accompagnement de la mise en conformité des responsables de traitements est l'une des missions de la CNIL. Pour ce faire, elle s'appuie sur les besoins exprimés par les professionnels en tenant compte également des éventuelles difficultés rencontrées, pour apporter des solutions concrètes et les généraliser chaque fois que possible.

De même, les organismes professionnels avec lesquels la CNIL a engagé des échanges continus sur la question des traceurs depuis l'adoption de l'article 32-II, ont largement relayé auprès de leurs membres les principes issus de la recommandation. Cela s'est matérialisé par la publication de livre blanc et de « FAQ » (ou questions réponses) destinés à accompagner les professionnels dans leur démarche de mise en conformité.

Pour accompagner très pratiquement les éditeurs de sites, la CNIL propose des outils ne nécessitant pas de consentement ou, lorsque cela n'est pas possible, des scripts de demande de consentement.

Afin d'aider les nombreux utilisateurs de Google Analytics, la CNIL met à disposition sur son site un script de demande de consentement spécialement adapté à ce service de mesure de fréquentation proposé par Google. Un simple copier-coller permet aux éditeurs de sites de bloquer les cookies de Google Analytics si le consentement des internautes n'est pas obtenu, ou de les supprimer s'ils décident de s'y opposer. Ce script a évolué au cours de cette année pour prendre en compte les remarques de différents éditeurs de sites. Par ailleurs, des contributeurs volontaires ont amélioré cet outil via le répertoire collaboratif mis en place sur Github (gestionnaire de projets collaboratifs).

La CNIL recense par ailleurs les outils gratuits et open source qui permettent aux éditeurs de site de se mettre en conformité avec sa recommandation. Ainsi, les sites peuvent être mis en conformité à moindre frais, et de façon transparente, puisque les outils recommandés sont vérifiables.

La mise en conformité étant un processus dynamique et la technologie évoluant, les organismes professionnels et la CNIL poursuivent leur dialogue et leur coopération afin d'apporter des réponses adaptées aux questions nouvelles. ■

DE L'AUDIT AU CONTRÔLE

Le 11 juillet 2014, la CNIL a annoncé sur son site que des contrôles relatifs aux cookies et autres traceurs seraient opérés à partir du mois d'octobre.

Un recours à toute la palette des contrôles

Les contrôles effectués ont essentiellement concerné des sites Internet, mais des vérifications ont également été faites auprès des acteurs tiers intervenant dans les processus de tracking liés aux cookies (régies publicitaires notamment).

Les investigations ont principalement été réalisées dans le cadre des nouveaux pouvoirs de contrôle en ligne (voir en annexe).

Toutefois, la CNIL s'est également appuyée sur :

- des contrôles sur place, dans les locaux de la société ;
- des auditions sur convocation dans les locaux de la CNIL.

27
CONTRÔLES EN LIGNE

24
CONTRÔLES SUR PLACE

2
AUDITIONS

!

359 cookies déposés sur la page d'accueil d'un site de presse !

Extrait du procès-verbal de constatations : « Constatons 5 minutes après l'arrivée sur la page d'accueil précitée, sans avoir effectué de « clic » et en ayant fait défiler la page, le dépôt de plus de 150 cookies supplémentaires ; Constatons qu'à ce stade le nombre total de cookies s'élève alors à 359 (voir pièce n°3) »

▸▸▸ Les constatations effectuées lors des contrôles en ligne, sur place et dans le cadre des auditions ont été consignées dans un procès-verbal de contrôle comportant également les pièces annexées : copies d'écran du site Internet, copies des mentions légales et/ou conditions générales, enregistrement des cookies déposés sur le terminal aux différents stades de la navigation, code source de certaines pages Internet et capture des en-têtes HTTP. Enfin, dans certains cas, des demandes d'information ou de pièces complémentaires ont été adressées aux éditeurs de sites qui disposaient d'un délai limité pour y répondre.

Les préalables techniques à la vérification

La configuration de l'environnement nécessaire à la réalisation des constatations en ligne relative aux cookies et autres traceurs a été rigoureusement définie. En effet, les cookies et traceurs n'étant pas directement « visibles » par l'internaute, des outils ont été utilisés pour les détecter. De plus, certains éléments de configuration du terminal de navigation ont dû être pris en considération dans la mesure où ils peuvent générer ou, à l'inverse, bloquer des dépôts ou lectures de cookies, ou d'autres traceurs. Tel est par exemple le cas de certaines extensions ou de certains éléments de configuration présents sur le logiciel de navigation utilisé.

Points de vérification et manquements constatés

• Le type de traceurs utilisés

Le premier point analysé lors des contrôles a porté sur le type de traceurs utilisés par le site web : s'agit-il de cookies HTTP, de *local shared object* (« cookies flash »), de techniques de *finger printing*, etc. ? Actuellement, c'est le cookie http auquel il est le plus souvent recouru, mais les autres techniques précitées, qui relèvent aussi de l'article 32-II de la loi « Informatique et Libertés » et nécessite de recueillir le consentement des personnes selon leur finalité, ont également été observées. Ce dernier point est souvent mal connu, certains éditeurs ou régies publicitaires pensant que le recours à d'autres techniques de traçage leur permettrait de sortir du champ d'application de la loi.

• La finalité des cookies

Le second point de vérification a concerné **la finalité des cookies ou autres traceurs**, puisque c'est elle qui détermine si le consentement de l'internaute doit être recueilli. Les contrôles effectués montrent que le plus souvent, les sites Internet utilisent des cookies nécessitant un recueil du consentement tels que ceux liés à la publicité ciblée ou aux boutons de partage des réseaux sociaux. Ceux qui n'en utilisent pas sont les sites reposant sur un modèle économique payant pour l'internaute, qui s'appuient sur une solution de mesure d'audience respectant certaines conditions (information des personnes, faculté de s'opposer au traceur, finalité du traceur limitée à la mesure d'audience, géolocalisation réduite et durée de vie du traceur inférieure ou égale à 13 mois).

Parfois, des cookies n'ont pas ou plus de finalité ! Certains sites Internet ont en effet tellement de prestataires publicitaires qui agissent dans leurs pages qu'ils « oublient » d'arrêter le système de *tracking* de ces derniers quand les prestations se terminent. Techniquement, ce sont des morceaux de code source (appelés *tags*) qui continuent à s'exécuter dans la page Internet et à déclencher, sans finalité, des lectures et dépôts de cookies opérés par les serveurs informatiques d'une société tierce. Ce problème, assez répandu, est désigné sous le terme de « *tags obsolètes* ».

• Les modalités de recueil du consentement

Lorsque la finalité poursuivie par les cookies utilisés nécessite le consentement de l'internaute, ce qui est le cas le plus fréquent, la CNIL contrôle alors

> Les cookies sont presque toujours déposés dès l'arrivée sur la page d'accueil du site sans consentement de l'internaute.

les **modalités de son recueil**. Le consentement est-il recueilli de manière effective ? Quelle est la qualité, la visibilité et la simplicité de l'information relative aux cookies et autres traceurs ? Quelles sont les conséquences en cas de refus du consentement ? Le consentement peut-il être retiré à tout moment ?

Aujourd'hui, la majorité des sites à forte audience ont mis en place un bandeau d'information avec recueil de consentement en deux étapes. Le contenu du bandeau d'information est le plus souvent conforme aux préconisations de la recommandation relative aux « cookies et autres traceurs » de la CNIL (art.2). Cependant, les contrôles ont mis en évidence que les cookies sont presque toujours déposés dès l'arrivée sur la page d'accueil du site et en l'absence de toute action de l'internaute, c'est-à-dire sans attendre qu'il ait donné son consentement.

La manière dont l'internaute exprime son accord au dépôt et à la lecture de certains cookies a également été analysée : par un clic, en poursuivant sa navigation après lecture d'un 1er bandeau, en faisant défiler la page (scroll), etc.

Parfois, les modalités de recueil du consentement n'apparaissent pas valables en raison des conséquences négatives pour la personne en cas de refus. Ainsi, plusieurs sites contrôlés proposent à l'internaute le blocage de tous les cookies depuis son navigateur comme seul moyen d'opposition, sans possibilité de choix par finalité. Or, ces mêmes sites précisent dans leurs mentions d'information que ce blocage entraine l'impossibilité de créer un compte sur le site, de se connecter ou de réaliser un achat…

- **La durée de vie des cookies**

Les vérifications effectuées ont également porté sur la durée de vie des cookies. La recommandation de la Commission prévoit une durée maximale de 13 mois. Or, de nombreux cookies ont des durées de vie supérieure ou égale à 2 ans, et parfois même 10 ans.

- **Les défauts de sécurité**

Par ailleurs, ces contrôles ont mis en évidence qu'**un mauvais usage des cookies pouvait entraîner un défaut de sécurité**. En effet, si les cookies stockent souvent des données à caractère personnel indirectement identifiantes (numéro identifiant unique d'utilisateur par exemple) ou des données *a priori* difficilement intelligibles, ils sont parfois utilisés pour stocker des données directement identifiantes « en clair » : nom/prénom, email, login, etc. Ce cas a été rencontré deux fois sur des sites Internet à forte audience qui avaient pourtant fait l'effort de sécuriser leurs formulaires d'inscription par l'usage du protocole HTTPS. Or, le stockage des données saisies dans un cookie a pour effet de les transmettre « en clair » à chaque requête HTTP postérieure. La confidentialité de la transmission des données n'est donc pas assurée malgré l'usage d'un protocole sécurisé sur les pages hébergeant les formulaires.

Les suites

Sur la base des constatations effectuées dans le cadre des contrôles sur l'usage des cookies, la CNIL est susceptible d'adopter des mises en demeure, voire des sanctions à l'égard des organismes à l'encontre desquels des manquements à la loi ont été relevés. Ces procédures pourront, si les circonstances le justifient, être accompagnées de mesures de publicité. ■

INFOS +

Cookies Sweep day

La CNIL a participé au niveau européen à un « Cookies sweep day » visant à vérifier les modalités d'information et de recueil du consentement des internautes. Cette opération, s'inscrivant hors procédure formelle de contrôle, visait à établir un comparatif des pratiques à l'échelle européenne. Il a permis à la CNIL d'auditer 100 sites Internet du 15 au 19 septembre 2014.

DRONES ET VIE PRIVÉE : UN CADRE À INVENTER

Qu'il s'agisse d'utilisateurs individuels, d'entreprises ou des pouvoirs publics, les drones ont connu une croissance exponentielle au cours de ces derniers mois. Aujourd'hui, ces plateformes volantes équipées de nombreux capteurs sont utilisées ou envisagées pour des applications aussi diverses que les loisirs, les services (commerciaux ou non), la photographie, la logistique ou encore la surveillance d'infrastructures.
Depuis deux ans, la CNIL a initié une réflexion prospective[1] qui s'étend également aux niveaux européen et international.

DES MILLIERS DE DRONES « À TOUT FAIRE »

Encore récemment, les drones étaient perçus par le grand public soit comme des armes de guerre, soit, à l'opposé, comme des jouets. Dans le premier cas, ils sont associés à des capacités de portée, d'intrusion, de frappe et de furtivité tellement élevées qu'elles semblent presque irréelles[2] ; dans le second, à l'inverse, l'usage est à ce point limité qu'il s'apparente plutôt à celui d'un inoffensif jeu radiocommandé.

Le développement fulgurant de l'usage des drones civils dans la sphère de l'entreprise et des pouvoirs publics, ainsi que l'exceptionnelle dilatation des usages de loisirs ont considérablement changé la donne. L'un des signes les plus tangibles est la multiplication des sollicitations adressées à la CNIL, qu'il s'agisse d'entreprises qui souhaitent les utiliser, de particuliers qui s'en inquiètent, ou encore des médias qui s'interrogent sur l'étendue des usages et des risques éventuellement associés.

Les usages par les pouvoirs publics : de nouveaux dispositifs de surveillance ou de gestion de crise

Les premiers utilisateurs historiques des drones étaient les États eux-mêmes. L'origine militaire des drones ne pouvait qu'impliquer une dualité d'usage plus ou moins rapide selon les moyens et les besoins des pouvoirs publics.

Des besoins de sécurité publique, de maintien de l'ordre, de surveillance des frontières mais également de sécurité civile, de secours aux personnes ou de gestion de crise peuvent être remplis par des drones. Cependant, dans la majorité des cas, les drones ne font que compléter une panoplie existante, pour remplacer par exemple des hélicoptères.

Les usages par les professionnels et les entreprises, dans tous les secteurs et pour des usages très variés

Les usages par les professionnels sont également en pleine expansion, à la fois en nombre d'opérateurs, types d'appareils et cas d'usages.

La réglementation française concernant ces activités[3] permet à la Direction générale de l'aviation civile (DGAC) de disposer de chiffres concernant les opérateurs professionnels de drones, ceux-ci étant invités à se déclarer auprès d'elle. Au 31 décembre 2014, 1256 opérateurs professionnels étaient déjà déclarés[4]. Certains opérateurs disposant de plusieurs appareils, ce sont plusieurs milliers d'appareils professionnels qui sont venus parcourir le ciel français en quelques années. En outre, le nombre d'opérateurs et d'appareils en activité va probablement continuer à croitre de manière importante.

Les professionnels proposent leurs services à des particuliers ou, le plus souvent d'ailleurs à d'autres professionnels : aider un agriculteur à comprendre les caractéristiques de sa parcelle, permettre à un exploitant de grands ouvrages d'arts (comme un barrage) d'accomplir une mission d'inspection à moindre coût, fournir une nouvelle capacité de surveillance à l'exploitant de grands réseaux (lignes à haute tension, rails de chemin de fer), etc.

L'imagination des opérateurs semble pour le moment sans limite. Si globalement les drones sont privilégiés pour des missions dangereuses ou monotones, les nouveaux appareils pouvant porter des charges utiles plus importantes ouvrent

1 / Voir la lettre Innovation et Prospective n°6 : Drones, innovations, vie privée et libertés individuelles*, décembre 2013. http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/LettreIP6.pdf - 2 / CHAMAYOU, Grégoire.* Théorie du drone*. Paris : La Fabrique, 2013, 363 p - 3 / Les arrêtés du 11 avril 2012 relatifs à « la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent » et à « l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord » sont en cours de mise à jour par la DGAC et leurs successeurs sont attendus pour 2015. - 4 / Site officiel de la DGAC, consulté en janvier 2015 : http://www.developpement-durable.gouv.fr/Exploitants-Effectuer-des*

1256 opérateurs professionnels de drones en France au 31 décembre 2014 selon la DGAC.

la voie à des centaines de nouvelles applications. Ainsi, même si les missions de surveillance ou de sécurité sont un usage naturel des drones eu égard à leurs qualités (discrétion, accès à des zones difficiles d'accès, captation à partir d'un point culminant), on ne peut résumer les drones à de simples « caméras de vidéosurveillance volante ».

Les usages par les particuliers de drones de loisirs : vers une responsabilisation accrue des utilisateurs

De même que le marché professionnel s'est constitué en quelques mois, les drones de loisirs ne sont plus dorénavant réservés à des amateurs éclairés d'aéromodélisme, mais sont devenus des objets de grande consommation et un loisir attractif pour le grand public. Deux tendances convergentes ont permis ce saut.

Premièrement, le développement de très nombreux drones-jouets peu coûteux s'est appuyé sur l'omniprésence des smartphones, ceux-ci devenant des outils de pilotage et de contrôle du drone. Selon les informations rendues publiques par la société Parrot, celle-ci aurait vendu 700 000 drones grand public en 2014[5]. Mais, Parrot n'est pas seul sur ce marché : au 5 janvier 2015, 73 constructeurs français de drones étaient déclarés auprès de la DGAC[6]. Une récente étude de l'institut Xerfi[7] estime également que le chiffre d'affaires des constructeurs et ▸▸▸

INFOS +

« DIYdrones » : des plateformes d'innovation à la portée de tous

Dès la lettre *Innovation et Prospective* de décembre 2013, la CNIL attirait l'attention de tous sur l'aspect « bricolable » des drones. Les composants mécaniques ou électroniques utiles aux drones sont dorénavant très faciles à trouver et peu coûteux. On trouve sur le marché des moteurs, des hélices, des structures pour des prix modiques et l'explosion du marché des objets connectés fait que la partie computationnelle des drones est également de moins en moins coûteuse : une carte de calcul, quelques capteurs (accéléromètres, gyroscopes) présents également dans les smartphones, de la communication radio… et voilà un « *DIYDrone* », un drone fait maison !
Le réservoir de personnes potentiellement capables de produire des drones ou d'inventer des usages augmente donc considérablement. On voit fleurir les hackathons consacrés aux drones et des lieux (makerspaces ou fablabs) qui consacrent une partie de leur activité à ces projets, comme par exemple le FlyLab de La Paillasse, à Paris. C'est là qu'une partie des usages de demain s'inventent et se testent. Ces voies d'exploration des idées émergentes sont, pour la CNIL, un moyen d'enclencher des réflexions d'avenir, autour de l'autonomisation des drones, de leur travail en « essaim » et in fine, sur l'éthique de la robotique.

5 / Site officiel de Parrot, informations financières : http://www.parrotcorp.com/en/financialpublications/initialearningsguidancefor2014andstrategyfor2015 - 6 / Source : site officiel de la DGAC, consulté en janvier 2015 : http://www.developpement-durable.gouv.fr/Exploitants-Effectuer-des.html - 7 / Xerfi, Le marché des drones civils*, mars 2014, http://www.xerfi.com/presentationetude/Le-marche-des-drones-civils_4EEE15.*

700 000

DRONES « GRAND PUBLIC » VENDUS DANS LE MONDE PAR LE *LEADER* FRANÇAIS DU SECTEUR EN 2014

73

CONSTRUCTEURS FRANÇAIS DE DRONES À USAGE CIVIL SELON LA DGAC

▸▸▸ exploitants français de drones, qui s'est élevé à 100 millions d'euros en 2013, devrait tripler d'ici 2015 pour atteindre 288 millions d'euros.

Deuxièmement, l'essor des caméras de loisirs à haute définition est un corollaire évident à l'essor du marché grand public des drones[8].

Des centaines de milliers de vidéos de vols de drones autour d'habitations ou en zone urbaine sont ainsi diffusées sur les plateformes en ligne de partage de vidéos. Ceci n'est pas sans risques pour le respect de la vie privée, d'autant que les drones deviennent de plus en plus furtifs et que leurs utilisateurs ne sont pas toujours à proximité immédiate de l'appareil, empêchant la personne filmée de s'enquérir du respect de ses droits. La responsabilisation des utilisateurs de drones est donc essentielle. ■

DRONES ET VIE PRIVÉE : DES QUESTIONS CONNUES DANS LEUR PRINCIPE ET INÉDITES DANS LEUR FORMULATION

Un cadre juridique existant dont les modalités d'application doivent être repensées

Les questions particulières soulevées par les drones en matière de vie privée ne paraissent pas nouvelles de prime abord. Ni la vidéosurveillance/vidéoprotection, ni la captation de sons, ni même les données de type connexions wifi et leur captation par des tiers ne sont inconnues. Ce qui est nouveau, en revanche, c'est le passage à une échelle de masse de dispositifs par nature mobiles et discrets, qui comportent trois paramètres opérationnels essentiels :

1. la position avantageuse en hauteur qui leur offre un accès à des lieux normalement difficiles d'accès ;
2. la discrétion (faible bruit, taille réduite, distance) ;
3. la « charge utile » (capteurs embarqués et capacité de calcul) qui constitue le cœur intelligent du dispositif.

Or, le cadre juridique n'a pas été écrit précisément pour de tels dispositifs.

Trois corpus juridiques, ayant portée générale, peuvent toutefois être utilement convoqués :

▸ Le premier et le plus évident est le cadre général de l'article 9 du code civil qui protège la vie privée. Ainsi, il n'est pas permis de filmer ses voisins depuis sa fenêtre avec son smartphone ou avec un drone. Mais, la distance de prise de vue ne rend pas toujours l'interdiction aussi perceptible.

▸ Le deuxième cadre, que la CNIL a pour mission de faire respecter, est celui de la loi informatique et libertés. L'essor des usages professionnels des drones (voire de certains usages privés qui sortiraient du cadre de l'exemption pour usage strictement personnel prévu par la loi, notamment lorsqu'une vidéo est mise en ligne) va nécessairement accroître le nombre d'activités soumises à ce cadre et à ses règles. Les exigences de loyauté de la collecte de données, d'information des personnes mais aussi de respect de leurs droits s'imposent, comme pour tout traitement de données à caractère personnelles.

▸ Le troisième cadre auquel on peut naturellement penser est celui de la vidéosurveillance/vidéoprotection et du Code de la sécurité intérieure, qui reprennent notamment les obligations d'information des personnes, ainsi que le droit d'accès, pour tous les dispositifs mis en œuvre sur la voie publique ou dans les espaces ouverts au public. ■

8 / De nombreux drones grand public permettent d'ailleurs d'embarquer une caméra de ce type. - 9 / Voir Cour de Justice de l'Union Européenne, C-212/13, arrêt de la Cour (quatrième chambre) du 11 décembre 2014 « František Ryneš contre Úřad pro ochranu osobních údajů »

QUELLES SOLUTIONS POUR COMBINER INNOVATION ET PROTECTION DES DROITS DES PERSONNES ?

Dans la recherche de solutions opérationnelles, il est contre-productif d'opposer artificiellement la protection de la vie privée et l'innovation. Il ne s'agit pas uniquement de protéger les personnes contre les risques des technologies ou de rendre celles-ci plus « acceptables » socialement, mais d'éviter que des atteintes volontaires ou involontaires aux droits des personnes se multiplient à l'avenir.

Animée de cet esprit, la CNIL a engagé des travaux dont l'objectif est clair : le cadre de régulation doit à la fois tracer des lignes rouges et offrir un espace de liberté aux innovations pour ces appareils dans le respect de la vie privée. Ce plan d'action s'incarne par exemple dans des échanges avec l'autorité nationale de sécurité aérienne, la DGAC. Il s'incarne également dans des travaux européens, au sein du G29 ainsi que dans des échanges avec des acteurs du secteur des drones, comme la Fédération Professionnelle du Drone Civil (FPDC). Trois axes ont ainsi été particulièrement approfondis : la pédagogie, l'information et le contrôle.

Quelle pédagogie collective et quelle prévention ?

C'est sans doute dans ce champ que l'action est la plus immédiatement possible. Avec le développement massif des drones, il est devenu nécessaire de diffuser des conseils et bonnes pratiques aux utilisateurs, leur rappelant notamment le champ de ce qui est permis ou interdit au regard des lois applicables. En ce qui concerne les particuliers, la CNIL a participé avec la DGAC à la rédaction d'une fiche pratique. Celle-ci a vocation à être remise à tout particulier acquéreur d'un drone de loisirs, afin de lui rappeler dans des termes simples les grands principes à respecter. Une déclinaison de cette fiche pourrait être imaginée pour les utilisateurs professionnels.

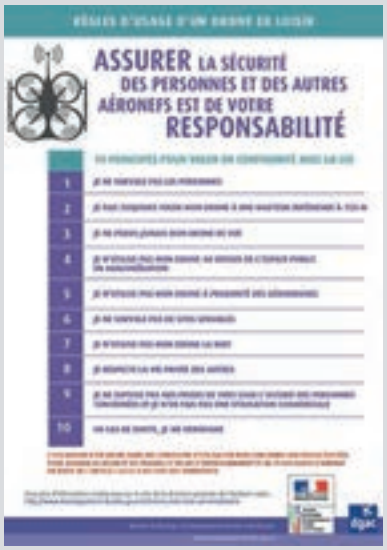
Quelle information des personnes ?

La loi informatique et libertés et le code de la sécurité intérieure relatif à la vidéoprotection prévoient l'information préalable des personnes. Or, si une telle information est aisée dans un périmètre déterminé, elle l'est beaucoup moins face à des dispositifs mobiles. Plusieurs pistes de réflexion ont déjà été émises par des professionnels ou chercheurs. On peut envisager un dispositif d'immatriculation des drones – mais la pertinence d'une telle solution est limitée pour des drones de petite taille. On peut également imaginer un système d'émission d'informations par l'appareil, sur le modèle des transpondeurs de l'aviation générale, ou un système dans lequel la liste des drones ayant survolé un site serait indiquée sur un site internet voire mise à disposition sous un format standard en « open data », permettant ainsi d'identifier les mouvements aériens et de faire valoir ses droits.

Quel contrôle possible ?

Les contrôles dépendent des lieux et des circonstances : la DGAC est compétente sur la partie strictement aérienne et la CNIL peut contrôler les systèmes de vidéosurveillance et de vidéoprotection (lieux ouverts au public), comme tous les traitements de données collectées à des fins non exclusivement personnelles. Il y a enfin, notamment pour les abus dans un cadre privé, le contrôle du juge.

La régulation des drones implique de lier la réglementation aérienne et la régulation de la protection des données personnelles. Retenir l'une sans l'autre, c'est probablement limiter considérablement, à long terme, le développement de cet outil. Comme dans l'ensemble de l'univers numérique, innovation et développement dépendent de la confiance et de la loyauté des usages. Cette confiance peut se construire notamment grâce à une information claire des personnes et des moyens effectifs pour exercer leurs droits. Il s'agit donc de bâtir des dispositifs innovants qui intègrent la protection de la vie privée le plus en amont possible. ■



LES DONNÉES PERSONNELLES AU CŒUR DES ENJEUX DE CONCURRENCE

CONCURRENCE, DONNÉES PERSONNELLES, NUMÉRIQUE : UN RAPPROCHEMENT IRRÉVERSIBLE

Il ne se passe pas un jour sans que, à l'occasion d'un nouveau produit ou service, de fusion ou de rapprochement entre entreprises ne soit mentionnés les conséquences ou les enjeux de ceux-ci en termes de protection de la vie privée. Un tel constat correspond à l'importance économique croissante que les données personnelles ont prise dans les dernières années.

On parle en effet de *big data*, de données qui constitueraient la puissance du futur, de modèles prédictifs d'une précision inégalée qui pourront être valorisés économiquement dans des domaines aussi variés que la lutte contre la criminalité, la grande distribution, les services de rencontres… Au-delà des slogans médiatiques ou marketing, les données alimentent désormais tous les services de la société de l'information, ceux des géants de l'Internet qui ont mis les données au cœur de leur modèle économique comme ceux de l'économie traditionnelle qui collectent et traitent des données pour leurs besoins quotidiens et ceux de l'innovation. Pour paraphraser un terme anglo-saxon, nous sommes donc entrés dans une sorte de « datification » du monde.

De ce fait, les données elles-mêmes se trouvent assimilées à des actifs, dont le commerce a dessiné des marchés totalement nouveaux et sur lesquels opèrent des forces économiques et des tensions concurrentielles qui étaient inimaginables il y a une décennie.

Cette valorisation économique des données conduit naturellement à leur entrée dans le monde de la concurrence : des rachats d'entreprise peuvent être motivés par la seule quantité de données détenues par l'entreprise ciblée ou par ses compétences en matière d'exploitation de données, notamment à des fins d'optimisation publicitaire ; des situations regardées comme des positions dominantes et des monopoles se constituent autour de l'accès et de la maîtrise de gigantesques bases de données, parfois contestées dans des procédures antitrust.

Concurrence et données personnelles se rapprochent avec des effets incertains sur les champs respectifs des unes et des autres.

Longtemps anecdotique, le débat est aujourd'hui maintes fois posé – par exemple lors du colloque organisé par la revue Concurrences au Sénat auquel participait la Présidente de la CNIL, le 1er décembre 2014[1]. Des cas concrets ont été d'actualité sur l'année 2014, comme la question de l'achat de Snapchat par Facebook, dont deux associations américaines a demandé qu'il soit gelé au nom du respect de la vie privée, l'opération

1 / Contribution d'Isabelle Falque-Pierrotin à l'ouvrage - À quoi sert la concurrence ? - Institut de droit de la concurrence ; Septembre 2014 ; 735 pages ; ISBN : 979-10-94201-00-8

de concentration en question étant selon elles de nature à susciter des « *pratiques déloyales et trompeuses* » en matière de collecte de données.

Il est donc important de réfléchir à la manière dont doivent être articulés ces deux pans du droit, étant entendu que chacun doit être considéré de manière équivalente, et non subordonnée, et que ces réflexions doivent être portées aux niveaux européen et international, au-delà du cadre national.

Aucune solution simple ne s'impose pour résoudre un sujet si complexe. Car, de même que les décisions des autorités de concurrence peuvent avoir des conséquences en matière de vie privée, les décisions des autorités de protection des données quant à certaines activités des acteurs du numérique sont susceptibles d'avoir des répercussions importantes sur les marchés pertinents.

Aujourd'hui, ce débat s'articule autour de quelques idées fortes. ■

LA PROTECTION DES DONNÉES PERSONNELLES, DROIT FONDAMENTAL, DOIT ÊTRE PRISE EN COMPTE DANS L'ANALYSE DE LA CONCURRENCE SUR LES MARCHÉS NUMÉRIQUES

Ceci n'a pas été entièrement le cas jusqu'à présent, si l'on se souvient des termes du débat généré par l'annonce, en 2007, du projet de rachat par Google de DoubleClick, alors fournisseur indépendant de solutions de gestion de campagnes en ligne.

Le 11 mars 2008, la Commission européenne a conclu que l'opération de concentration envisagée était compatible avec le marché commun et le fonctionnement de l'accord EEE. Dans son analyse, la Commission n'a envisagé les conséquences du projet qu'au regard des problèmes de concurrence qu'il était susceptible de poser sur les marchés de la commercialisation et de la gestion des annonces publicitaires en ligne, dans ses dimensions horizontale et verticale. Elle n'a donc pas intégré à sa réflexion les préoccupations des organisations de défense de la vie privée, qui faisaient valoir que la position dominante qu'entraînerait ce rachat permettrait à Google de suivre le comportement des internautes et d'en traiter les données personnelles dans des proportions excessives, ce qui justifiait à leurs yeux qu'on lui impose des garde-fous spécifiques. Avant elle, la FTC américaine avait également validé l'opération et ce, compte tenu de sa double compétence dans ces matières, en tenant compte tant de ses risques concurrentiels que de ses risques en matière de « privacy », ceux-ci n'étant selon elle pas constitués en l'espèce.

Les règles de protection des données ne sont pas *ab initio* des règles de régulation économique. En revanche, il est impératif que la logique de marché qui se dessine autour des données personnelles ne heurte pas frontalement celle de la protection et en tienne compte.

La protection de la vie privée, valeur fondamentale, s'impose en effet à l'économie de marché. Les données personnelles ne peuvent être considérées comme n'importe quelles « commodities ». Valeurs économiques, elles demeurent des données personnelles, auquel le législateur a attaché une protection particulière, liée au droit dont disposent les personnes à la protection de leurs libertés et droits fondamentaux. En effet, ces données, une fois enregistrées, compilées, analysées, croisées avec des données d'autres sources révèlent tout sur les personnes : leurs centres d'intérêts, leur vie familiale, leur état de santé, la cartographie de leurs relations sociales, … – les différentes dimensions de leur vie privée et de leur intimité, ouvertes à nu et stockées dans les serveurs d'opérateurs, souvent étrangers, qui sont susceptibles à tout moment d'injecter ces données dans des circuits de commerce divers et sans garantie de confidentialité.

La prise en compte de la protection des données comme droit fondamental est donc appelé à intervenir de manière croissante dans l'appréhension économique de ces questions.

Ceci explique ainsi que les atteintes causées à la vie privée des personnes doivent être distinguées des atteintes aux droits des consommateurs. Certes, le paiement d'un prix anticoncurrentiel n'est pas acceptable. Mais alors, que dire d'un dommage réputationnel grave, de la révélation de secrets qui blesseront l'intime au plus profond, dont la propagation et les conséquences ne seront pas mesurables et dont les effets ne cesseront peut-être jamais ?

Le souci d'entretenir la concurrence entre les acteurs des marchés de l'économie numérique ne peut donc légitimer que ceux-ci soient affranchis du respect des règles de protection des données ou même que ne soient pas pris en compte les effets d'une opération concurrentielle en termes de protection et d'accès aux donnés personnelles.

Des études récentes commencent d'ailleurs à analyser comment des traitements de données à caractère personnel qui seraient mis en œuvre de manière massive à des fins de distorsion, d'exclusion, voire de manipulation du marché seraient attentatoires aux droits des personnes concernées à la protection de leur vie privée.

La poursuite de l'équilibre entre ces deux dimensions est l'enjeu fondamental des négociations sur le projet de règlement européen sur la protection des données personnelles.

À cet égard, il est important de rappeler que les règles européennes de protection des données n'ont ni pour objet ni pour effet d'empêcher les entreprises de mettre en œuvre des traitements au service de l'innovation, dès lors qu'ils répondront généralement aux besoins des ▸▸▸

personnes. Le seul et unique objectif de ces règles est d'assurer que les nouvelles technologies demeurent « au service du citoyen », « dans le cadre de la coopération internationale », afin qu'elles ne portent atteinte « ni à l'identité humaine, ni aux droits de l'homme, ni aux libertés individuelles ou publiques » (article 1er de la loi Informatique et Libertés).

Le droit économique et le droit de la concurrence ne peuvent donc déroger aux exigences posées par la loi en matière de protection de la vie privée des personnes, qui constitue un droit fondamental.

Mais la protection de la vie privée des utilisateurs doit désormais être prise en compte en droit de la concurrence pour une autre raison : cette protection, droit fondamental, devient, en tant que telle, un objet de concurrence au même titre que le prix d'un bien ou d'un service.

La protection des données des utilisateurs, objet de concurrence

Sous l'effet conjugué des exigences du régulateur et des attentes des utilisateurs, la protection des données de ceux-ci devient en elle-même un élément de différenciation et de compétitivité.

De nombreux signaux convergents attestent de cette évolution.

Tout d'abord, les atteintes à la vie privée des personnes qui résultent de **négligences ou de la fragilité des précautions prises en matière de sécurité des données** ont des conséquences économiques lourdes pour les entreprises, si bien que les précautions prises en la matière conditionnent aujourd'hui tant la confiance des clients que celle des partenaires économiques et des investisseurs.

Plusieurs exemples en témoignent. En janvier 2014, l'annonce du groupe américain de grande distribution Target selon laquelle une faille de sécurité avait compromis 40 millions de données bancaires, puis 70 millions de données personnelles comme des adresses emails et postales, et des numéros de téléphone, a eu des conséquences spectaculaires : le cours de l'action de la société a chuté aussitôt, tout comme ses résultats nets, qui sont tombés de 2 999 millions de dollars en 2012 à 1 971 millions en 2013.

Mais de manière plus intéressante au regard du droit de la concurrence, la protection des données personnelles suscite de **nouvelles formes d'innovation**. Se développent aujourd'hui des offres de services plus protectrices de la vie privée que celles de leurs concurrents, généralement des opérateurs de la « première génération » de services en ligne. Au-delà de la sécurité des outils et des systèmes, ces jeunes acteurs revendiquent le fait que leur « *business case* » minimise la collecte et le traitement de données personnelles.

Apparaît ainsi le marché prometteur du « web éphémérique », dont Snapchat, service de messagerie éphémère via lequel photos et les vidéos sont supprimées après avoir été partagées, est emblématique.

Surfant sur cette vague alternative, des acteurs annoncent mettre en œuvre des modèles économiques radicalement différents des modèles « classiques », en minimisant l'exploitation de données à caractère personnel. Les moteurs de recherche DuckDuckGo ou Ixquick, par exemple, revendiquent le fait de ne pas enregistrer les requêtes de ses utilisateurs ; Wickr a annoncé avoir adapté son modèle économique en offrant son logiciel de chiffrement en licence et non plus en capitalisant sur la seule exploitation des données de ses utilisateurs.

Cette tendance s'installe durablement. Elle pousse même des acteurs dominants, « historiques », à changer leurs pratiques pour donner des gages à leurs utilisateurs quant à la protection de leur vie privée. Ainsi, Facebook, qui a toujours revendiqué la mise en œuvre d'une « *real name policy* », y a récemment renoncé pour ses applications périphériques.

La protection des données personnelles devient un terrain de concurrence autonome, sur lequel les entreprises se battent pour innover au bénéfice des utilisateurs.

La situation est loin d'être stabilisée et la concurrence est vive. Mais tous ces affrontements entre acteurs témoignent de l'installation d'une nouvelle tendance : les utilisateurs accordent de la valeur à la maitrise de leurs données personnelles et, quand ils en ont le choix, ils sont prêts à migrer vers des services qui leur proposent une véritable valeur ajoutée « vie privée ». À cet égard, on mesure le rôle essentiel que l'utilisateur européen pourra jouer, à terme, quand il sera doté d'un véritable « droit à la portabilité » de ses données personnelles sous l'empire du futur règlement européen sur la protection des données.

Des développements concurrentiels sur le terrain de la vie privée sont donc intrinsèquement sains pour les personnes. Ils le sont également pour les entreprises : car en l'absence d'alternative à des biens et services basés sur l'exploitation à outrance ou le contrôle excessif des données des utilisateurs, la situation finirait nécessairement par se retourner contre elles. La créativité humaine, alliée aux compétences technologiques de la génération Y, mènerait en effet les utilisateurs à des voies de contournement, au développement de services parallèles. La protection des données personnelles, qui apparait à certains comme un investissement coûteux, pourrait bien à terme, au contraire, garantir la stabilité du marché, considéré comme plus digne de confiance par le consommateur.

Face à ces interactions croissantes entre concurrence et vie privée, les régulateurs doivent donc s'adapter. Mais les questions qu'ils ont alors à traiter ne sont pas simples, en particulier dans la perspective de la réalisation des promesses du *big data*, qui, sous quelques années, accentuera la tension entre forces concurrentielles.

Aucune autorité de régulation ne pourra traiter ces sujets seule, sans chercher à bénéficier de l'expertise de ses homologues européens et internationaux, ni de celles des autorités disposant d'autres compétences. Interrégulation, concertation, partage d'analyses doivent dès lors être les maîtres mots de la réponse à ces questions. Avec, en trame de fond, une exigence : celle d'une véritable intelligence collective au service de nos valeurs. ■

2. BILAN D'ACTIVITÉ

Informer le grand public et les professionnels

Conseiller et réglementer

Accompagner la conformité

Protéger les citoyens

Contrôler et sanctionner

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'investie particulièrement 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 2014. Au total, ce sont 400 sujets qui ont été diffusés depuis 2007. La CNIL est intervenue chaque vendredi 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 a contribué 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 2014, les 50 chroniques diffusées portaient sur des sujets tels que : le droit au déréférencement, le cyberharcèlement, les compteurs communicants, les violations de données personnelles, la publication de photos sur internet, les objets connectés, etc.

Les publications à destination des professionnels

La CNIL a publié une série de fiches pratiques sur le commerce et les données personnelles à destination des particuliers (quels sont leurs droits ?) et des professionnels (quelles sont leurs obligations ?). Elles ont été téléchargées plus de 3 000 fois.

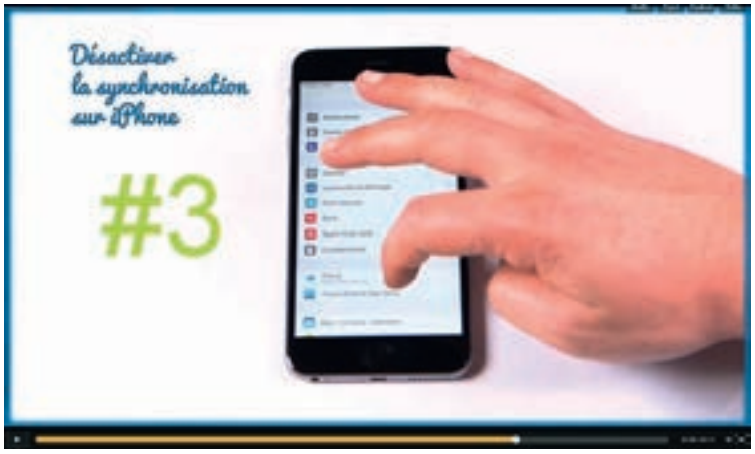
En 2014, la CNIL a publié 3 packs de conformité : compteurs communicants, logement social et assurance.

Le site internet www.cnil.fr

Le site de la CNIL bénéficie d'un très bon référencement naturel sur les moteurs de recherche.

Les contenus les plus plébiscités sont principalement les sanctions publiques, les fiches pratiques telles que la fiche pratique « Vidéosurveillance », le guide « Droit d'accès » ou encore les conseils sur « Comment effacer des informations me concernant sur un moteur de recherche ».

En 2014, le site a connu une légère hausse de son nombre de visiteurs par rapport à 2013 (+ 2,5 %), soit 2 371 710 visites pour une durée, en moyenne, de 4 minutes et 55 secondes par visite.



Sécuriser son smartphone, régler les options de confidentialité des réseaux sociaux, adopter des techniques d'anonymisation, effacer ses traces : les conseils de la CNIL sont diffusés en vidéo.

La CNIL sur les réseaux sociaux

La CNIL est principalement présente sur 5 plateformes sociales (Dailymotion, Facebook, Google+, LinkedIn, Twitter). Citoyens, relais d'influence, professionnels : l'institution tente de sensibiliser des publics très différents à la question des données personnelles et d'instaurer un dialogue constant avec ses usagers, quel que soit leur niveau de connaissance de la Loi « informatique et libertés ».

En s'appuyant sur des articles pertinents, des tutoriels simples, des visuels explicatifs, les publications de la CNIL ont également vocation à accompagner chaque internaute dans la maitrise de sa vie privée numérique. Et ça marche ! Les 18 000 fans, 36 000 followers, et 3 500 abonnés LinkedIn que compte l'institution se font ainsi d'excellents « prescripteurs » des bonnes pratiques auprès de leur propre réseau.

Enfin, depuis la fin de l'année 2014, la présence sociale de la CNIL intègre une dimension internationale via l'animation d'un compte Twitter @CNIL_en à destination de la communauté anglophone.

L'image de la CNIL

Depuis 2004, la CNIL mesure sa notoriété. L'enquête IFOP a été menée auprès d'un échantillon de 1 005 personnes, représentatif de la population française âgée de 18 ans et plus. Les interviews ont eu lieu par téléphone du 12 au 13 décembre 2014. ■

LES RÉPONSES AU PUBLIC

Le service des relations avec les publics (SRP) a pour mission principale de recevoir les demandes des usagers de la CNIL, qu'ils soient responsables de traitements désireux de connaître leurs obligations et d'obtenir des conseils, ou particuliers souhaitant être informés des modalités d'exercice des droits qui leur sont reconnus par la loi « Informatique et Libertés ». Il est par ailleurs chargé de l'enregistrement des courriers adressés à la Commission.

- **37 120 courriers reçus (35 524 en 2013, soit + 4,5 %)**
- **133 213 appels téléphoniques (124 595 en 2013, soit + 7 %)**

En 2015, la CNIL proposera un service de réponse en ligne, disponible sur cnil.fr permettant ainsi de mieux répondre aux attentes des différents publics de la CNIL (professionnels ou particuliers). ■

EN CHIFFRES

En 12 mois, la CNIL a doublé son audience sur Facebook. La CNIL figure à la 18ème position dans le top 20 des institutions les plus suivies sur Twitter.
(source Netscouade)

68 %
DES PERSONNES CONNAISSENT LA CNIL CONTRE 54 % EN 2013 ET 32 % EN 2004

36 000
FOLLOWERS SUR TWITTER

INFOS +

La permanence de renseignement juridique est assurée par 6 téléconseillers du lundi au vendredi (de 10 h à 12 h et de 14 h à 16 h). Elle a pris en charge 71 469 appels en 2014.

L'ÉDUCATION AU NUMÉRIQUE, UNE ACTION EN DÉVELOPPEMENT

L'éducation au numérique est une nécessité absolue. Chaque acteur, à son niveau, doit se mobiliser sur ce sujet qui relève d'une responsabilité partagée. C'est pourquoi la CNIL a pris l'initiative, en mai 2013, de constituer un collectif composé d'acteurs très divers, issus du monde de l'éducation, de la recherche, de l'économie numérique. En 2014, la CNIL a été très présente sur cette thématique, aussi bien à l'échelle nationale qu'au plan international.

Le collectif EDUCNUM sur le devant de la scène

Le collectif a organisé une conférence à Futur en Seine, le 13 juin 2014, sur le thème « Une culture générale du numérique pour tous ! ». Plusieurs actions innovantes visant à diffuser une culture générale du numérique auprès de publics variés ont été présentées par France Télévisions, la Web@cadémie ou la CNIL. Des experts se sont ensuite retrouvés autour d'une table-ronde pour échanger sur les freins et les leviers français à la compréhension du numérique.

À l'initiative de la CNIL, le collectif a lancé, pour la première fois en 2014, un concours destiné aux étudiants, Les Trophées EDUCNUM, afin de sensibiliser les plus jeunes aux bons usages du web. Les étudiants ont été invités à présenter, sur le support de leur choix (application mobile, dataviz, goodies, kit de survie sur les réseaux sociaux…), des projets pédagogiques et innovants. Ce concours a été placé sous le parrainage de la Présidente de la CNIL et de Jacques-Antoine Granjon, PDG et fondateur de vente-privee.com, co-fondateur de l'Ecole Européenne des Métiers de l'Internet, et avec le soutien du ministère de l'Éducation nationale.

L'ancrage international de l'éducation au numérique

L'éducation au numérique est également une priorité partagée par les autorités de protection des données au niveau international. La Conférence internationale des Commissaires à la Protection des Données et de la Vie Privée de Varsovie a ainsi mis en place un groupe de travail, animé par la CNIL, sur le sujet et a adopté une résolution intitulée « Une éducation au numérique pour tous ». La CNIL a organisé à ce titre un atelier en marge de la 36ème Conférence internationale des commissaires à la protection des données et à la vie privée, qui a porté sur le thème « Quels outils et pratiques les plus efficaces sur la vie privée pour diffuser une éducation au numérique pour tous ? » réunissant des autorités de protection des données, des entreprises, des représentants de la société civile (professeurs d'universités, associations) et des organismes internationaux (le Conseil de l'Europe). ■

> L'éducation au numérique est une responsabilité partagée qui nécessite une mobilisation générale.

« Les aventures croustillantes du Prince Chip »

« Data fiction, le site dont vous êtes le héros »

DERNIÈRE MINUTE

La remise des Trophées a été organisée à la CNIL en présence de la ministre de l'Éducation nationale Najat Vallaud-Belkacem, le 28 janvier 2015, lors de la journée européenne de protection des données. Les 2 projets lauréats ont bénéficié d'un soutien financier, de l'accès à un réseau professionnel et d'une forte visibilité dans les médias.
Le Grand Prix du jury a été attribué à des étudiants de l'Université Panthéon Sorbonne, pour leur projet « Les aventures croustillantes de Prince chip », destiné aux 6-10 ans. Le Prix spécial du jury a été attribué à des étudiants de l'école Boulle, pour leur projet « Datafiction, le site dont vous êtes le héros ! », destiné aux 14-18 ans.

CONSEILLER ET RÉGLEMENTER

L'activité de conseil et de réglementation de la CNIL est variée : avis sur des projets de texte d'origine gouvernementale concernant la protection des données personnelles ou créant de nouveaux fichiers, élaboration de cadres juridiques simplifiant l'accomplissement des formalités préalables, autorisations, recommandations, conseils. 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 et la mise en œuvre d'outils opérationnels par les organismes publics et privés.

DES OUTILS DE SIMPLIFICATION DES FORMALITÉS

En 2014, la Commission a poursuivi les mesures de simplification administrative, avec l'adoption ou la mise à jour de 15 **autorisations uniques** et de 3 **normes simplifiées.**

Accélérer l'innovation thérapeutique et renforcer la sécurite dans le domaine de la santé

Un accès plus rapide à l'innovation thérapeutique

Les autorisations temporaires d'utilisation (ATU) ont pour objet d'accélérer l'accès à l'innovation thérapeutique en permettant l'accès précoce aux médicaments qui sont en phase finale d'évaluation avant l'obtention de leur autorisation de mise sur le marché (AMM) en France.

Les recommandations temporaires d'utilisation (RTU) ont, quant à elles, pour objet de sécuriser les prescriptions de médicaments en dehors des indications prévues dans leur AMM. Elles fixent un cadre dans lequel des médicaments bénéficiant d'une AMM peuvent être prescrits pour de nouvelles indications en attendant une mise à jour de celle-ci.

La sécurité des dispositifs d'ATU et de RTU suppose une étroite collaboration entre l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), les laboratoires et les professionnels de santé (médecins prescripteurs et pharmaciens dispensateurs). Un suivi est mis en place afin d'assurer la sécurité des patients et de garantir que le rapport entre les bénéfices et les risques du médicament reste présumé favorable pour la situation thérapeutique identifiée.

Les modalités de ce suivi sont, le cas échéant, définies dans un protocole qui prévoit la mise en œuvre par les laboratoires d'un traitement de données de santé à caractère personnel relatif aux patients. Ainsi, les laboratoires doivent contrôler, pour chaque patient, le respect des critères d'inclusion, recueillir les données de suivi transmises par les médecins prescripteurs, les analyser et établir des rapports périodiques de synthèse.

Afin de simplifier les démarches des laboratoires et permettre un accès rapide à l'innovation thérapeutique dans des conditions respectueuses de la vie privée des personnes concernées, la Commission a adopté, le 11 décembre 2014, une autorisation unique (AU-041) relative au ATU et RTU, après avoir mené une concertation avec les autorités sanitaires (l'ANSM) et les Entreprises du Médicament (LEEM). ▸▸▸

2 277
DÉCISIONS ADOPTÉES

551
DÉLIBÉRATIONS ADOPTÉES EN SÉANCE PLÉNIÈRE

958
AUTORISATIONS DE TRANSFERTS DE DONNÉES HORS UE

626
AUTORISATIONS DE RECHERCHE EN MATIÈRE DE SANTÉ

142
AUTORISATIONS D'ÉVALUATION DES PRATIQUES DE SOINS

La messagerie sécurisée de santé : un gage de sécurité et de confidentialité

Les pratiques les plus répandues d'échanges d'informations dématérialisés entre professionnels de santé s'opèrent de façon usuelle par le biais de messageries électroniques standard mises à la disposition du public par les fournisseurs d'accès internet, qui ne présentent pas de garanties de sécurité et de confidentialité suffisantes, au regard du caractère sensible des données de santé à caractère personnel échangées.

Le déploiement d'une messagerie sécurisée de santé est une priorité pour la CNIL, les pouvoirs publics, les ordres professionnels et les associations de patients afin de disposer d'un outil garantissant la sécurité et la confidentialité lors d'échanges de données de santé à caractère personnel. Elle constitue une composante importante de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) à laquelle travaille la CNIL en concertation avec les pouvoirs publics.

Dans le cadre de son action d'accompagnement à la conformité des professionnels (utilisateurs et éditeurs de logiciels), la CNIL a adopté le 12 juin 2014 (délibération n°2014-239 publiée au JO du 16 juillet 2014) une autorisation unique relative à la messagerie sécurisée de santé (AU-037). Cette autorisation fournit ainsi un cadre juridique et technique commun et conforme aux exigences de la loi.

Ce cadre permet l'échange de données de santé au moyen d'un service de messagerie sécurisée de santé entre professionnels de santé et, plus largement, entre les professionnels des secteurs sanitaire, social et médico-social habilités par la loi à échanger des données de santé à caractère personnel dans le cadre de la prise en charge des personnes concernées.

Cette autorisation unique a été élaborée en concertation avec les ordres professionnels concernés, les associations de patients et les éditeurs de logiciels. À travers ce mode de régulation, la CNIL sécurise les pratiques des professionnels concernés qui sont invités à se conformer à l'AU-037 en procédant à un engagement de conformité à cette autorisation unique.

Adoption d'une autorisation unique en matière de prévention de la délinquance pour les communes

Les communes sont, en particulier depuis la loi du 5 mars 2007, au cœur de la mise en œuvre des politiques publiques en matière de prévention de la délinquance. Pour leur permettre d'exercer leurs missions tout en assurant la protection des données personnelles de leurs administrés, la CNIL a adopté le 26 juin 2014 une autorisation unique permettant d'encadrer les traitements mis en œuvre dans ce cadre (AU-038).

Lors de plusieurs contrôles menés en 2011 et 2012, la Commission avait constaté que les acteurs locaux rencontraient des difficultés pour respecter les obligations légales en matière de traitement des données personnelles dans l'accomplissement de leurs missions de prévention de la délinquance. Elle a donc souhaité prévoir un cadre général permettant aux acteurs concernés de sécuriser les traitements mis en œuvre, tout en allégeant les formalités à accomplir. Ce cadre a été élaboré en concertation étroite avec les acteurs locaux et le Comité interministériel de prévention de la délinquance (CIPD).

L'AU-038 a vocation à constituer la première étape de l'élaboration d'un pack de conformité destiné à permettre l'encadrement des pratiques locales relatives à la prévention de la délinquance. En effet, cette autorisation unique encadre uniquement les traitements mis en œuvre dans le cadre du fonctionnement des groupes relevant directement des pouvoirs du maire en matière de prévention de la délinquance, à savoir les Conseils locaux de sécurité et de prévention de la délinquance (CLSPD) et les Conseils pour les droits et devoirs des familles (CDDF).

L'autorisation de la Commission précise les finalités exactes qui peuvent être poursuivies et les utilisations qui doivent être exclues. Sont ainsi notamment exclus les échanges de données individuelles qui interviendraient au sein de la formation plénière et restreinte des CLSPD, les traitements mis en œuvre par les groupes

de travail relevant de l'autorité du préfet ou du procureur de la République. Ce cadre général précise également les données pouvant être collectées (données d'identité, niveau scolaire, situation professionnelle, etc.), les personnes pouvant y avoir accès directement (tels que le maire ou le coordonateur), les modalités d'exercice des droits des personnes (information particulière des personnes faisant l'objet d'un suivi), les durées de conservation applicables ou encore les mesures de sécurité à mettre en œuvre (mesures de protection physique, logique, etc.). La Commission ayant relevé, lors de ses contrôles, certaines carences dans les conditions de partage de certaines informations sensibles entre les différents acteurs concernés ou encore en matière de traçabilité des actions, elle a rappelé l'importance de prendre les mesures nécessaires pour préserver la sécurité des données à l'occasion de leur recueil, de leur consultation, de leur communication et de leur conservation. Elle a toutefois adopté des dispositions transitoires en la matière, afin de prendre en compte les réalités de terrain et faciliter ainsi la mise en conformité des responsables de traitement.

Conçu comme un outil de simplification à la disposition des collectivités, ce cadre général doit permettre aux maires de ne plus adresser de demandes d'autorisations spécifiques dès lors que les traitements mis en œuvre sont conformes aux règles fixées par cette autorisation unique. Il leur suffit en effet de prendre connaissance du cadre général fixé par cette norme et de s'engager à le respecter par le biais d'un engagement de conformité adressé à la CNIL via le site internet de la CNIL pour être autorisés à le mettre en œuvre.

Ce premier outil de mise en conformité des traitements mis en œuvre aux fins de prévention de la délinquance sera progressivement complété pour tenir compte du retour des différents acteurs et ajuster ce cadre général à leurs pratiques. Les traitements à ce jour exclus par ce dispositif (comme ceux mis en œuvre au niveau des intercommunalités, par exemple) pourront ainsi faire l'objet d'un même encadrement. Pour permettre une meilleure compréhension des pratiques locales, la Commission est toujours associée au groupe de travail sur le partage d'informations en matière de prévention de la délinquance piloté par le secrétariat général du CIPD. ■

LES AVIS ET AUTORISATIONS

Lors des séances plénières qui ont lieu trois fois par mois en moyenne, la Commission examine les demandes d'avis et les demandes d'autorisations qui sont de plus en plus nombreuses.

Données de connexion et données de contenu

Les données dites « de connexion » sont les informations produites ou nécessitées par l'utilisation des réseaux de communications électroniques, qu'il s'agisse des communications téléphoniques ou des connexions au réseau internet (données de trafic, de localisation, de facturation, etc.). Elles sont principalement techniques et concernent les communications émises par les opérateurs, hébergeurs ou fournisseurs d'accès : numéros de téléphone appelant et appelé, date et durée de l'appel ou de la connexion, identifiant et localisation de l'appareil utilisé, adresse IP, etc.

Les données dites « de contenu » sont celles échangées par les différents acteurs d'une communication : appels téléphoniques (fixes ou mobiles), télécopies, courriers électroniques, messageries instantanées, etc.

Si l'accès aux données de contenu est par nature plus intrusif que l'accès aux données de connexion, ces dernières peuvent néanmoins révéler des indications très précises sur la vie privée des personnes, comme les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées ou les relations sociales. Comme l'a rappelé la Cour de justice de l'Union européenne, qui a invalidé en avril 2014 la directive européenne sur la conservation de ces données (Arrêt du 8 avril 2014), l'accès aux données de connexion doit dès lors être particulièrement encadré. ▸▸▸

390
AUTORISATIONS

7
REFUS D'AUTORISATION

100
AVIS

FOCUS

Les suites de la loi de programmation militaire

Dans son rapport annuel 2013, la CNIL avait évoqué les dispositions de la loi de programmation militaire (LPM) et en particulier son article 20, relatif aux réquisitions administratives des données de connexion par les agents des services de renseignement. Rappelant qu'elle n'avait pas été consultée sur ces dispositions, elle avait déploré que la rédaction définitive du texte semble autoriser un accès aux données de contenu, et non seulement aux données de connexion, et avait rappelé que le décret d'application devrait dès lors clarifier ce point.

▸▸▸ À cet égard, la CNIL a eu l'occasion de rappeler, à plusieurs reprises, que les données détenues par les opérateurs et qui peuvent être demandées par des autorités sont de plus en plus nombreuses, accessibles à un nombre de plus en plus important d'organismes (sur réquisitions judiciaires ou administratives ou en exécution d'un droit de communication), et ce pour des finalités très différentes. Elle a dès lors appelé l'attention du Gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques.

Dans son avis (Avis du 4 décembre 2014) sur le décret d'application, publié le 24 décembre 2014 (Décret n° 2014-1576), la CNIL a demandé que le décret définisse avec précision les données qui pourront être demandées aux opérateurs, notamment afin de s'assurer que les services concernés ont accès aux seules données de connexion et non aux données de contenu. Une extension des données pouvant être requises par les services de renseignement aurait en effet risqué d'entraîner une atteinte disproportionnée au respect de la vie privée. Le décret finalement publié a pris en compte cette demande, en précisant que seules des données de connexion limitativement énumérées étaient concernées par cette procédure.

En ce qui concerne l'accès à ces informations « *sur sollicitation du réseau et transmis[es] en temps réel* » (nouveauté introduite par la LPM), le décret d'application a également précisé que cette sollicitation serait effectuée par les opérateurs exploitant le réseau. Il s'agit d'une garantie essentielle : cette formulation interdit en effet toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs.

Ce décret contient enfin d'autres dispositions concernant les réquisitions administratives de données de connexion, relatives aux conditions d'accès des agents des services de renseignement, aux modalités de demandes, de transmission et de conservation des données recueillies, ainsi qu'à la traçabilité et aux modalités de contrôle de ces opérations. Dans l'ensemble, la Commission a estimé que l'encadrement de ces réquisitions de données de connexion, dont le principe est acté dans la loi, était suffisant. ■

DES ÉCHANGES PERMANENTS ENTRE LE PARLEMENT ET LA CNIL

L'activité du Parlement en 2014 reflète la place centrale occupée désormais par la protection des données personnelles dans tous les aspects de la vie quotidienne des individus et dans la vie économique. Les parlementaires ont ainsi été amenés à se prononcer sur ces questions, en 2014, dans le cadre soit de projets ou propositions de lois, soit des travaux de contrôle et de prospective des assemblées. Dans ce contexte, les échanges avec la CNIL ont été nombreux.

Au cours de l'année 2014, **la CNIL a participé à plus d'une trentaine de rendez-vous au Parlement, parmi lesquels les auditions par les commissions permanentes occupent une place prépondérante**. La CNIL a été auditionnée, notamment, sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme et le projet de loi relatif à la santé, ou bien encore la proposition de loi déposée au Sénat visant à limiter l'usage des techniques biométriques et la proposition de loi déposée à l'Assemblée nationale relative à la déclaration de domiciliation.

La CNIL a également apporté sa contribution dans le cadre de missions d'information (listes électorales, Open data et protection des données) ou bien encore de travaux de réflexion et de prospective sur des sujets tels que la gouvernance de l'Internet à l'échelle européenne ou le cadre juridique relatif à la sécurité des réseaux numériques.

S'agissant des travaux de contrôle du Parlement, la CNIL a été entendue par la Délégation parlementaire au renseignement sur le cadre juridique des services de renseignement. Le rapport rendu par cette Délégation pour l'année 2014 comporte des nombreuses propositions, en vue de l'élaboration d'un projet de loi attendu en 2015.

Enfin, la CNIL s'est rendue à une audition de la Commission ad hoc de réflexion

et de propositions sur le droit et les libertés à l'âge numérique créée à l'Assemblée nationale et qui a débuté ses travaux en juin 2014. À cette occasion, la CNIL a pu s'exprimer autour des principaux thèmes pouvant en particulier animer la réflexion dans le cadre de la préparation du projet de loi numérique annoncé par le gouvernement pour l'année 2015 (voir encadré) : les principes à adopter en ce qui concerne la protection et la responsabilisation des individus ; l'usage que font les utilisateurs privés de ces données à caractère personnel ; l'équilibre entre la protection de la vie privée et les impératifs d'ordre public.

L'expertise de la CNIL est donc fréquemment sollicitée pour apporter aux parlementaires un éclairage à la fois juridique et technologique sur les questions liées au numérique. ■

FOCUS

Les évolutions de la loi informatique et libertés dans le cadre du projet de loi numérique

Le Gouvernement avait annoncé, au mois de février 2013, à l'occasion d'un séminaire sur le numérique, son intention de déposer un projet de loi au cours de la législature. La CNIL a alors engagé une réflexion qui l'a conduite, en mars 2014, à présenter plusieurs propositions d'évolution législative au Gouvernement.
Les propositions rendues publiques au mois de janvier 2015, dans le cadre de la consultation confiée au Conseil national du numérique, concernent les quatre principaux acteurs de l'écosystème « informatique et libertés » : la personne, les entreprises, les pouvoirs publics et la CNIL.
Ces propositions sont organisées autour de cinq axes : le renforcement de l'effectivité des droits pour les personnes, la simplification des formalités et des règles applicables pour les entreprises, l'amélioration du cadre juridique de certains traitements publics, le renforcement des relations entre la CNIL et les pouvoirs publics, l'adaptation des pouvoirs de la CNIL, notamment en vue de renforcer l'efficacité et la crédibilité de la politique de contrôle et de sanction.
La discussion autour d'une réforme du cadre juridique fixé par la loi pourrait être utilement complétée par une réflexion sur la constitutionnalisation du droit à la protection des données personnelles.
Document complet consultable sur le site Internet de la CNIL.

ACCOMPAGNER LA CONFORMITÉ

Le respect de la loi « informatique et libertés » implique, de la part des acteurs, une mise en conformité « dynamique ». Il ne s'agit pas en effet seulement de démarches administratives – dont une bonne partie vont disparaître avec le règlement européen – il s'agit de respecter, pendant toute la vie d'un traitement de données, les principes, droits et obligations posées par la loi, tout en les déclinant de manière opérationnelle. Les avantages de la conformité pour les professionnels sont nombreux : assurer une sécurité juridique aux acteurs ; tirer parti du droit pour en faire un facteur de succès ; accroître le capital de confiance vis-à-vis des interlocuteurs. La CNIL a développé en 2014 une gamme d'outils complémentaires permettant d'accompagner aux mieux les différents métiers et secteurs d'activité.

LES PACKS DE CONFORMITÉ

Élaborés en concertation avec les acteurs d'un secteur d'activité, les packs représentent un nouveau mode de régulation pour la CNIL. Ils visent à définir et diffuser des bonnes pratiques pour un secteur, tout en simplifiant les formalités administratives des acteurs qui s'y conforment. Ils peuvent ainsi contenir :

- Des mesures de simplification des formalités (autorisations uniques et/ou normes simplifiées),
- Des guides pratiques et pédagogiques,
- Des tests de vérification de conformité à la loi (par exemple des grilles d'auto-évaluation).

À ce jour, la CNIL a finalisé 3 packs : assurance, compteurs communicants et logement social.

Lancement du pack de conformité « banques et organismes financiers »

Le secteur banque regroupe l'ensemble des établissements bancaires et organismes financiers qui offrent leurs services aux particuliers notamment. Il s'agit d'un secteur fortement réglementé, soumis à de nombreuse contraintes qui concernent tout à la fois les modalités de gestion de la relation client mais aussi et de plus en plus la mise en œuvre de traitements destinés à s'assurer de la légalité des transactions.

Par ailleurs et comme beaucoup de secteurs économiques, le secteur banque connait une évolution sous l'influence du numérique tant dans ses fonctions traditionnelles que sur le segment du paiement à distance.

Les échanges entre la CNIL et le secteur financier sont anciens et ont conduit à des mesures de simplification des démarches des organismes du secteur, ainsi que d'un accompagnement au quotidien de leurs activités au regard de la loi informatique et libertés.

!

Pour la CNIL, le secteur « banque et organismes financiers » est particulièrement important au regard de la place qu'occupent ces organismes dans la vie quotidienne de leurs clients. Le recours aux services bancaires et financiers donne lieu à la production et à l'utilisation d'une masse de données qui révèlent très précisément les habitudes de vie mais aussi la situation personnelle de chacun. À ce titre, la CNIL souhaite faciliter la mise en conformité et accompagner ces professions dans leur mutation numérique.

Au regard de la loi « Informatique et libertés », le secteur social présente un enjeu particulier : créer des traitements automatisés de données permettant un suivi personnalisé et efficace des personnes aidées, sans porter atteinte au respect de leur vie privée.

Le lancement d'un pack dans ce secteur concrétise une volonté partagée d'aborder les traitements mis en œuvre par la profession dans leur globalité et de fournir des outils encore mieux adaptés aux besoins actuels. Outre un travail de reprise de l'existant et notamment des normes les plus anciennes, le travail commun doit permettre d'aborder des questions nouvelles ou particulièrement sensibles tant pour la profession, les particuliers ou l'État. C'est ainsi que le premier cycle de discussion débuté en octobre 2014 devrait aboutir à la production d'une autorisation unique consacrée à la fraude et permettre la révision des normes métiers liées à la gestion des crédits ou des prêts et à la tenue de compte. Une seconde étape permettra d'aborder au second semestre 2015 les questions restées en suspens comme celle de l'abus de marché.

Lancement du Pack de conformité « Social »

Le secteur social et médico-social regroupe l'ensemble des établissements et services ayant vocation à venir en aide à des populations aussi diversifiées que les personnes âgées, les malades, les personnes en situation de handicap ou encore celles en situation d'exclusion sociale, professionnelle ou autre.

Ce secteur nécessite la mise en œuvre de traitements comportant de nombreuses données dites « sensibles » (données de santé, appréciations sur les difficultés sociales, etc.).

Or, dans le cadre de ses missions d'instruction des demandes d'autorisation, d'avis ou de plaintes, et des contrôles effectués dans ce secteur, la CNIL a constaté une méconnaissance des principes de la protection des données personnelles ainsi que des difficultés dans l'application de la loi par les acteurs intervenant dans le domaine social et médico-social. Ces derniers ont par ailleurs exprimé leur volonté d'être mieux informés sur les règles relatives à la protection des données personnelles.

Dans une première étape, la CNIL a organisé des réunions de travail avec ces acteurs en vue de connaître leurs pratiques, leurs besoins ainsi que les difficultés rencontrées dans l'application de la loi « Informatique et Libertés ». Elle a ainsi engagé, le 3 octobre 2014, une large concertation avec des représentants des organismes qui œuvrent dans le champ de l'action sociale et des travailleurs sociaux afin de mener une action globale de soutien à la mise en conformité de ce secteur à la loi « Informatique et Libertés » et de définir les bases de travail pour la réalisation d'un « pack social ».

La seconde étape consiste pour la CNIL à concevoir des outils juridiques de simplification des formalités (normes simplifiées, autorisations uniques, dispenses…) et des bonnes pratiques spécialement adaptées au secteur social, à l'instar de ce qui a été effectué avec le secteur de l'assurance et les bailleurs sociaux. ■

LE CIL, UN ACTEUR DE LA CO-RÉGULATION

Emblème des nouveaux outils de conformité, le CIL s'affirme année après année comme le pilote naturel en charge de veiller à la sécurité juridique et technique du patrimoine informationnel au sein des organismes publics ou privés.

Depuis la création effective du CIL par le décret du 20 octobre 2005, les entreprises, les associations et les administrations peuvent désigner un CIL pour s'assurer de la conformité de leurs traitements à la loi « Informatique et Libertés ». Son rôle de conseil lui permet de diffuser les bonnes pratiques en matière de protection des données personnelles et participe à la réduction des risques. Ainsi, avec plus de 14 400 organismes qui ont désigné un CIL en 2014, protéger les données personnelles est devenu un enjeu de crédibilité vis-à-vis des clients, des usagers ou des adhérents.

Bénéficier de l'expertise des CIL

La CNIL bénéficie régulièrement de l'expertise des CIL, bons connaisseurs des impératifs de leur secteur d'activités, afin d'adopter des cadres de références ou d'élaborer des outils destinés à la communauté des CIL. Ainsi, pour construire les « packs de conformité » dans le secteur de l'Assurance ou du logement social, ou pour tester l'efficacité d'un outil de prise de fonction, la CNIL a sollicité la contribution des CIL directement ou par le biais de réseaux de professionnels ▸▸▸

> Protéger les données personnelles est devenu un enjeu de crédibilité vis-à-vis des clients, des usagers ou des adhérents.

> La désignation d'un CIL est un atout différenciant permettant, soit de valoriser l'éthique de son organisme, soit de se distinguer dans un marché concurrentiel.

(AFCDP) ou de CIL (SUPCIL, Club CIL de l'APRONET). La même démarche a été choisie pour l'élaboration du nouveau référentiel aux fins de labellisation des procédures de gouvernance Informatique et Libertés au sein des organismes.

Le CIL au cœur du label Gouvernance informatique et Libertés

En adoptant un nouveau référentiel qui fait du CIL la pierre angulaire du dispositif, la CNIL a fait le choix de valoriser ce métier. En effet, le label Gouvernance Informatique et Libertés prévoit des exigences relatives aux mesures et bonnes pratiques permettant pour un organisme de gérer les données personnelles et rendant compte des actions menées dans ce sens (*accountability*). Premier pas dans le sens que prend la législation européenne en préparation, ce nouveau référentiel pourra être utilisé par les CIL comme guide des procédures à suivre ou comme objectif d'obtention, en tant que tel.

L'accompagnement des CIL tourné vers l'efficacité

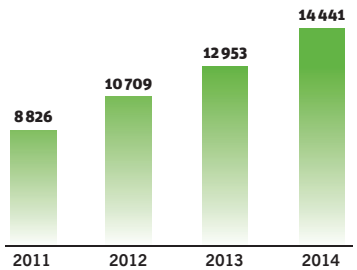
Depuis 2005, la CNIL a fait le choix d'accompagner cette communauté de professionnels de la protection des données par la création d'un service dédié. Ainsi, ce sont plus de 2 567 demandes de conseil juridique (+17 % par rapport à 2013) et 4 808 appels traités par l'équipe du service des CIL, qui concrétisent cette volonté forte d'animer et fédérer le réseau.

En outre, si l'efficacité d'un CIL est directement liée aux moyens et ressources affectés par le responsable de traitement, le niveau de formation est également fonction de son niveau de formation. À cet effet, la CNIL propose des ateliers d'informations réservés aux CIL dont le succès s'est confirmé en 2014 (plus de 1 000 participants ont suivis 34 ateliers) tout en révélant des attentes exprimées par les CIL (cf. focus). En effet, contribuer au développement des compétences du CIL reste un objectif essentiel pour la CNIL car elles feront la différence sur le terrain pour appliquer les grands principes de la loi de façon opérationnelle. ■

PLUS DE
1 000
PARTICIPANTS AUX 34 ATELIERS D'INFORMATION

14 441
ORGANISMES ONT DÉSIGNÉ UN CIL SOIT 4 035 CIL

Nombre d'organismes ayant désigné un CIL entre 2011 et 2014



FOCUS

Synthèse de l'enquête téléphonique IFOP

Une enquête téléphonique a été menée par l'IFOP du 12 au 17 novembre 2014 auprès d'un échantillon de 401 Correspondants Informatique et Libertés ayant été en contact avec la CNIL au cours des 12 derniers mois. Un fort taux de satisfaction des CIL vis-à-vis de la CNIL ressort de cette enquête puisque qu'ils sont 95 % à se déclarer satisfaits des services de la CNIL. En effet, les résultats montrent que les demandes de conseil, les ateliers et l'extranet des CIL sont particulièrement appréciés. Forte de ce constat positif, la CNIL a cherché à identifier par ailleurs les pistes d'amélioration pour répondre à ceux qui ne se sont pas déclarés « très satisfaits » (52 % sont « assez satisfaits »).
Ainsi, des attentes se sont exprimées, relatives à la réduction des délais de réponse, aux contenus proposés sur l'Extranet des CIL, aux ateliers CIL et à l'amélioration de l'annuaire des CIL.
Pour y répondre, la CNIL élabore actuellement des outils et services qui permettront d'obtenir une réponse dans un délai plus court, tout en donnant accès à des documents sectoriels et métiers en cours d'enrichissement. Ce nouvel environnement devrait permettre à la CNIL de traiter les demandes de conseil plus efficacement. Enfin, pour mieux accompagner les CIL au quotidien, un annuaire de CIL par secteur d'activités et par région sera proposé sur l'extranet afin d'être identifié (sur démarche volontaire) dans le réseau des CIL et d'être contacté par ses homologues, pour échanger sur le métier de CIL.

LE LABEL : UN INDICATEUR DE CONFIANCE

Un label, c'est la reconnaissance par la CNIL qu'un produit ou une procédure est conforme aux exigences des référentiels élaborés et publiés par la CNIL.

Le label permet notamment à un organisme de :

- Se distinguer en garantissant un haut niveau de protection des données personnelles,
- Afficher un indicateur de confiance pour les consommateurs, clients, internautes…,
- Renforcer la crédibilité d'un organisme lorsque le label a été obtenu pour une procédure interne.

Multiplication des demandes

La dynamique de labellisation connue depuis la création des premiers référentiels de labels CNIL ne s'est pas amoindrie en 2014, puisque l'année a été marquée par plus d'une dizaine de demandes de labellisation et l'octroi de dix labels.

Un nouveau référentiel pour les services de coffre-fort numérique

Adopté le 23 janvier 2014, ce référentiel permet à la CNIL de délivrer des labels aux services de coffre-fort numérique. Il s'agit du premier label « produit » de la CNIL.

À l'heure où les offres de stockage dématérialisées se multiplient, ce label permet aux utilisateurs d'identifier 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.

Un nouveau référentiel pour la gouvernance Informatique et Libertés

Face au besoin grandissant des entreprises et organismes publics d'identifier clairement les procédures à mettre en place pour une bonne gestion des données personnelles, la CNIL a décidé d'élaborer un nouveau référentiel : le label « gouvernance informatique et libertés ». La gouvernance « Informatique et Libertés » définit les règles et les bonnes pratiques permettant à un organisme d'assurer une gestion de ses données respectueuse des principes Informatique et Libertés.

Le référentiel, adopté en séance plénière le 11 décembre 2014, s'adresse aux organismes disposant d'un correspondant Informatique et Libertés (CIL). Il a été préparé en concertation avec les associations de CIL et fait du CIL la pierre angulaire du dispositif qui orchestre et veille au respect des procédures et de la loi Informatique et Libertés. Acteur essentiel d'une bonne gouvernance, le CIL peut aussi utiliser ce référentiel comme mode d'emploi ou guide des procédures à suivre et se fixer comme objectif l'obtention du label pour son organisme.

En pratique, les 25 exigences de ce nouveau référentiel sont organisées en trois thématiques qui concernent :

- l'organisation interne liée à la protection des données ;
- la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés ;
- la gestion des réclamations et incidents.

Véritable outil de responsabilisation des organismes traitant des données personnelles, le label est un indicateur de confiance pour leurs clients ou usagers. Il constitue, pour les entreprises, collectivités, associations ou administrations, un cadre éthique et juridique adapté, témoignant de la volonté de l'organisme d'innover et de traiter les données personnelles de manière responsable. Enfin, cette démarche permet de préparer les organismes aux règles du futur règlement européen en intégrant notamment le principe d'*accountability*. ■

LABEL CNIL GOUVERNANCE

> Le CIL est la pierre angulaire du label «gouvernance».

> Le label « gouvernance » témoigne de la volonté de l'organisme d'innover et de traiter les données personnelles de façon responsable.

4
RÉFÉRENTIELS EXISTANTS

55
DEMANDES DE DÉLIVRANCE DE LABELS REÇUES

44
LABELS DÉLIVRÉS

6 MOIS
DÉLAI MOYEN DE DÉLIVRANCE

LES BINDING CORPORATE RULES (BCR) ET LES RÈGLES CONTRAIGNANTES D'ENTREPRISE (RCE) FRANCOPHONES

Les BCR et RCE francophones sont des codes de conduite définissant la politique d'un groupe d'entreprises en matière de transferts de données personnelles. Les BCR sont destinées à encadrer les transferts de données effectués en dehors de l'Espace économique européen, tandis que les RCE francophones encadrent les transferts effectués entre États de l'espace francophone et vers des États tiers.

6 bonnes raisons de mettre en place des BCR et RCE francophones :

- **Assurer un niveau de protection suffisant aux données transférées,**
- **Prévenir les risques inhérents aux transferts,**
- **Uniformiser les pratiques relatives à la protection des données personnelles au sein d'un groupe,**
- **Éviter de conclure un contrat pour chacun des transferts,**
- **Communiquer sur la politique d'entreprise en matière de protection des données à caractère.** ■

> 1 organisme sur 3 désigne la CNIL comme autorité chef de file.

INFOS +

Création d'un pôle dédié aux BCR et aux RCE francophones

Les BCR impliquent un investissement substantiel de la part des organisations qui, en plus d'intégrer les principes de la directive 95/46/CE, doivent mettre en œuvre des mesures proactives – dites d'*accountability* (responsabilisation).

Ainsi, au-delà d'être un simple outil d'encadrement des transferts, les BCR sont de véritables programmes de mise en conformité et de gouvernance, puisqu'elles permettent de définir les grandes valeurs du groupe en matière de protection des données à l'échelle mondiale, mais aussi les mécanismes internes qui permettront d'assurer concrètement leur respect (audit, formation, réseau de délégués à la protection des données, etc.). Les BCR s'inscrivent donc dans la même démarche de responsabilisation des entreprises que celle envisagée dans le projet de règlement européen sur la protection des données personnelles.

À l'occasion de la réorganisation de la CNIL, un Pôle dédié aux BCR a été créé. Les missions principales du Pôle BCR sont les suivantes :

- **promotion des BCR et des RCE francophones,**
- **instruction des projets de BCR et de RCE francophones,**
- **coordination des procédures de coopération avec les autorités homologues, dont l'expérience ne cesse de croître à mesure que le nombre de BCR adoptés augmente,**
- **participation aux travaux du G29 et de l'APEC pour la création de liens entre les BCR et les CBPR.**

Outre l'amélioration de la visibilité des BCR et RCE francophones, la création de ce pôle contribue également à réduire les délais d'instruction des projets de BCR lorsque la CNIL est chef de file ou autorité secondaire. À titre d'exemple, la procédure d'approbation d'un projet de BCR soumis à la CNIL (chef de file) après la création du Pôle BCR n'a duré que 6 mois.

FOCUS

Répartition par secteur d'activité des entreprises ayant officiellement adopté des BCR (au 31 décembre 2014)

Banque-Assurance : ABN AMRO, AXA, Citigroup, ING Bank, JP Morgan Chase & Co., Rabobank, Société Générale
Industrie : Airbus Group, AkzoNobel, ArcelorMittal, BMW, BP, Cargill, D.E. Master Blenders 1753 (ex Sara Lee), DSM, General Electric, Michelin, Osram, Safran, Schlumberger, Schneider Electric, Shell, Siemens, Total
Luxe : Hermès, LVMH
Nouvelles technologies : Atmel, Atos, CA, HP, Intel, Linkbynet, Motorola Mobility, Motorola Solutions, OVH, Philips Electronics
Santé : Align Technology, AstraZeneca, Bristol Myers Squibb, Cardinal Health, CareFusion, GlaxoSmithKline, IMS Health, Novartis, Novo Nordisk, Sanofi
Services : Accenture, American Express, Ardian (ex AXA Private Equity), CMA-CGM, Deutsche Post DHL, Deutsche Telekom, eBay, Ernst & Young, First Data, Hyatt, International SOS, Legrand, Linklaters, Sopra HR Software (ex HR Access), Spencer Stuart, TMF Group

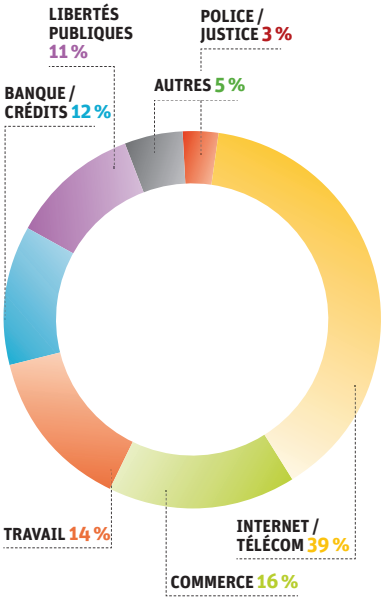
PROTÉGER LES CITOYENS

AUGMENTATION DU NOMBRE DE PLAINTES LIÉES À INTERNET

5 825
PLAINTES EN 2014

39 %
DES PLAINTES CONCERNENT INTERNET

Répartition des plaintes par secteur



En 2014, la CNIL a reçu 5 825 plaintes. 39 % des plaintes relèvent du secteur de l'internet. La e-réputation, c'est-à-dire l'image numérique d'une personne sur internet, constitue un enjeu important tant pour la vie professionnelle que pour la vie personnelle. Il est donc important de la contrôler et de la maîtriser. La loi « informatique et libertés » donne des outils, et permet notamment à chacun d'accéder aux données qui le concernent ou d'en obtenir la rectification si elles sont inexactes. Par ailleurs, les personnes peuvent, pour des motifs légitimes, demander la suppression de données les concernant diffusées sur internet : comptes piratés, faux profils, suppression de photographies, de vidéos, de publications ou encore de coordonnées.

Le secteur du commerce/marketing représente 16% des plaintes reçues. Les principaux motifs de plaintes sont relatifs à la prospection publicitaire. Les demandes portent ainsi sur la radiation de fichiers publicitaires, la conservation des coordonnées bancaires, le défaut de confidentialité des données. Comme en 2013, le principal motif de saisine de la CNIL sur ce secteur est l'opposition à recevoir des courriels publicitaires (spams), puis les sollicitations par téléphone et les publicités postales.

Les plaintes du secteur du travail (14 %) se stabilisent. Les demandes émanent généralement de salariés ou de syndicats. Un grand nombre de plaintes portent sur la vidéosurveillance (un peu plus de 300 en 2014) et plus généralement sur des dispositifs de contrôle mis en œuvre par les employeurs (vidéosurveillance, géolocalisation, cybersurveillance). Sont également souvent mises en cause l'absence d'information des salariés ou des difficultés rencontrées dans l'exercice du droit d'accès au dossier professionnel. ▸▸▸

> Le principal motif de plaintes demeure l'opposition à figurer dans un fichier : suppression de photographies, de commentaires, de vidéo.

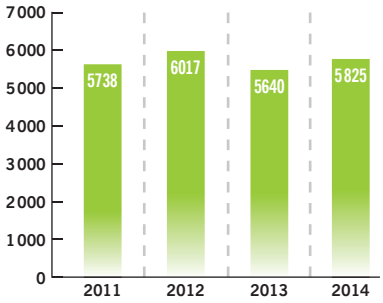
INFOS +

Depuis l'arrêt de la CJUE du 13 mai 2014 sur le « droit au déréférencement », il est possible de demander que des informations associées à ses nom et prénom soient supprimées des résultats délivrés par les moteurs de recherche. Le déréférencement d'une information n'entraine donc pas sa disparition en ligne. Seule une demande en ce sens adressée au site à l'origine de la diffusion peut conduire à la suppression des données. La CNIL a reçu, en 2014, 150 plaintes consécutives à des refus de déréférencement par les moteurs de recherche.

12 % des plaintes concernent le secteur banque/crédit. Le principal motif de plaintes reste la contestation de l'inscription dans les fichiers tels que le fichier des incidents de crédit et de paiement (FICP), le FCC (fichier central des chèques). Toutefois, la diffusion de cartes bancaires sans-contact a constitué un nouveau motif de plainte en 2014. Les clients se plaignant d'être peu informés et de ne pouvoir s'opposer à ce nouveau dispositif de paiement.

Les plaintes relatives aux **libertés publiques et aux collectivités locales (11 %)** ont augmenté en 2014 (élections, presse en ligne, mise en ligne de documents publics par les collectivités locales, réutilisation des données publiques), notamment dans le contexte des élections municipales, avec principalement des demandes liées à l'e-mailing politique et aux demandes d'opposition ou de déréférencement concernant des articles de presse.

Nombre de plaintes reçues par la CNIL entre 2011 et 2014



Quasiment la moitié des plaintes adressées à la CNIL sont formulées via le service de « plainte en ligne » accessible depuis le site de la CNIL (www.cnil.fr). Une refonte de ce service est prévue au premier semestre 2015 pour mieux accompagner les plaignants dans leurs démarches et élargir le dispositif à de nouveaux types de plaintes.

Parallèlement, une refonte de la rubrique « vos droits » a permis d'améliorer l'information des personnes et de proposer une approche plus opérationnelle, de manière à mieux distinguer les plaintes des simples demandes de conseil. ■

… HISTOIRES VÉCUES

Travail / ressources humaines

▸ **Madame R. signale à la CNIL des informations excessives figurant dans un questionnaire de recrutement. La CNIL est intervenue auprès de la société qui a modifié son questionnaire. Les questions relatives à l'entourage familial du candidat, au nombre d'enfants à charge ou à la qualité de propriétaire ou de locataire de son logement ont été supprimées.**

▸ **Une monitrice d'auto-école saisit la CNIL car son employeur a mis en place, sur sa voiture, un système de géolocalisation alors qu'elle est autorisée à l'utiliser en dehors de son temps de travail. La CNIL a effectué un contrôle sur place à l'issue duquel le gérant a enlevé le dispositif de géolocalisation.**

▸ **Plusieurs salariés se plaignent d'être filmés de manière permanente dans leur espace de travail. Après un rappel à la loi, la société s'est engagée à supprimer la caméra qui filme de manière continue les postes de travail.**

Droit au déréférencement

▸ **Monsieur D. demande le déréférencement d'un article publié dans un quotidien régional au sujet d'une garde à vue, non suivie d'une condamnation, datant de 1998. Google a accepté de le déréférencer.**

Libertés publiques

▸ **Un propriétaire dont le bien a été vendu aux enchères retrouve l'ensemble des documents concernant la vente, en ligne, sur le site d'un cabinet d'avocat. La CNIL est intervenue auprès de ce professionnel du droit pour lui rappeler ses obligations en matière de confidentialité des données. Les éléments ont été supprimés du site.**

Assurance, défaut de confidentialité des données

▸ **Mme O. a envoyé à la CNIL une plainte relative à sa compagnie d'assurance. Elle a été remboursée de frais médicaux qu'elle avait engagés quelques mois auparavant. Elle s'est étonnée de la mention sur son relevé bancaire du libellé « frais déplacement, psy ». La CNIL est intervenue auprès de la compagnie pour lui rappeler qu'elle devait assurer la confidentialité des données qu'elle traite. Celle-ci a renoncé à la mention de cette information et a procédé à une sensibilisation de ses services s'agissant de la confidentialité des libellés des virements bancaires.**

Commerce/marketing

▸ **Monsieur P. s'est fait poser des implants capillaires par une clinique de chirurgie esthétique. Cette clinique lui adresse ensuite par courriels, en tant qu'ancien patient, des informations sur de nouvelles techniques en matière d'implants capillaires à un prix préférentiel.**
À la suite de l'exercice de son droit d'opposition, l'envoi de sollicitations cesse pendant un temps, mais après quelques mois, reprend. Le plaignant craint que son entourage ne découvre qu'il a eu recours à cette intervention. La CNIL est intervenue auprès de la clinique, ce qui a permis de faire supprimer définitivement de sa base de prospects les adresses électroniques et postales de Monsieur P.

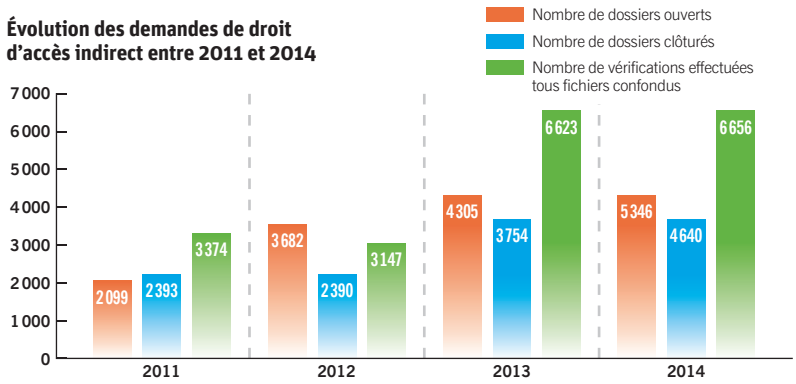
LE DROIT D'ACCÈS AUX FICHIERS DE POLICE, GENDARMERIE, RENSEIGNEMENT, FICOBA : NOUVELLE PROGRESSION DES DEMANDES

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 (fichiers de renseignement, Système d'Information Schengen etc.) ou qui ont pour mission de prévenir, rechercher ou constater des infractions (traitement d'antécédents judiciaires....) ou d'assurer le recouvrement des impositions (fichier FICOBA) peuvent en effectuer la demande par écrit auprès de la CNIL.

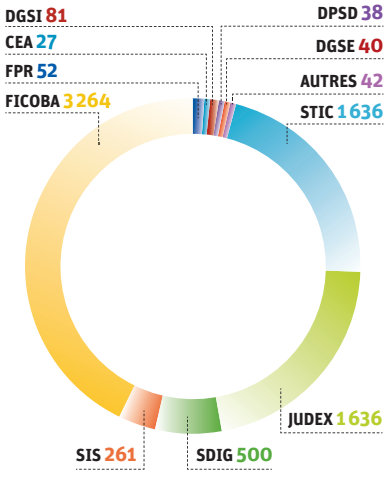
5 246 personnes se sont adressées à la CNIL en 2014 pour exercer leur droit d'accès indirect, ce qui représente **une augmentation de 22 %** par rapport à 2013. Le nombre de demandes a ainsi progressé de 45% en l'espace de deux années sous l'effet de l'afflux des sollicitations portant sur le fichier FICOBA de l'administration fiscale dans le cadre du règlement des successions.

5 246
DEMANDES DE DROIT D'ACCÈS INDIRECT
SOIT + 22 % PAR RAPPORT À 2013

Évolution des demandes de droit d'accès indirect entre 2011 et 2014



Demandes de droit d'accès indirect 2014 : répartition par fichiers des vérifications à effectuer



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 **5 246 demandes reçues au cours de l'année 2014 représentent un total de 7 577 vérifications à mener** qui concernent, à titre principal, le fichier FICOBA et le Traitement d'Antécédents Judiciaires (TAJ). ■

INFOS +

Le droit d'accès indirect, comment ça marche ?

À réception de 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 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.

FICOBA : Fichier des Comptes Bancaires et Assimilés / TAJ police : Traitement d'Antécédents Judiciaires (procédures police) / TAJ gendarmerie : Traitement d'Antécédents Judiciaires (procédure gendarmerie) / SRT : services de renseignement territorial (successeurs depuis le mois de mai 2014 des services de l'information générale) / SIS : Système d'Information Schengen / FPR : Fichier des Personnes Recherchées / CEA : Direction Centrale de la Sécurité du Commissariat à l'Energie Atomique / DGSI : Direction Générale de la Sécurité Intérieure (ex DCRI) / 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...

Résultats des vérifications concernant le Traitement d'Antécédents Judiciaires (TAJ)

	TAJ (procédures établies par la police nationale)	TAJ (procédures établies par la gendarmerie nationale)
Nombre de vérifications individuelles effectuées	1 623	1 626
Nombre de personnes inconnues	328	1 151
Nombre de personnes enregistrées uniquement en tant que victimes	335	118
Nombre de fiches de personnes « mises en cause » vérifiées	960	357
dont nombre de fiches supprimées	17 %	21 %
dont nombre de fiches mises à jour par mention de la décision judiciaire favorable intervenue (classement sans suite, non-lieu, relaxe...) rendant la personne inconnue du fichier sous profil de consultation administrative (enquêtes administratives)	18 %	24 %
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)	64 %	54 %

6656 vérifications ont été menées au cours de l'année 2014 dont 49 % concernant le Traitement d'Antécédents Judiciaires (TAJ) qui a succédé, au 1er janvier 2014, aux fichiers STIC et JUDEX.

Si ce fichier est désormais commun aux forces de police et de gendarmerie, les vérifications menées au titre du droit d'accès indirect demeurent, à la demande des gestionnaires du fichier, toujours dissociées selon les services à l'origine des procédures. Les personnes sont donc destinataires de deux courriers distincts portant notification du résultat des vérifications effectuées respectivement auprès de la police et de la gendarmerie nationales.

Compte tenu des difficultés structurelles de mise à jour de ce fichier, maintes fois relevées par la CNIL, l'ensemble des vérifications menées en 2014 pour les procédures établies par la police nationale se sont traduites par la suppression de 18 % des enregistrements examinés, ainsi que par la mise à jour par mention des suites judiciaires favorables intervenues dans 19% des cas ayant pour effet de rendre les personnes « inconnues » de ce fichier sous son profil de consultation administrative (enquêtes pour l'obtention d'un agrément ou d'une habilitation pour l'exercice d'un emploi, d'un titre de séjour, d'une distinction honorifique).

6 656
VÉRIFICATIONS ONT ÉTÉ MENÉES AU COURS DE L'ANNÉE

Le contentieux en matière de droit d'accès indirect

L'année 2014 a été marquée par l'engagement d'un nombre important de recours contentieux (33) par des personnes n'ayant pu obtenir, au terme de la procédure de droit d'accès indirect, la communication des données détenues dans certains fichiers soumis au droit d'accès indirect (système d'information Schengen, fichiers des services de renseignement des ministères de l'intérieur et de la défense).

Ce régime dérogatoire au droit commun n'emporte pas, en effet, un droit à communication systématique, par l'intermédiaire de la CNIL, des données enregistrées dans les fichiers qui y sont soumis. Conformément aux dispositions combinées des articles 41 et 42 de loi du 6 janvier 1978 et de l'article 88 de son décret d'application, en cas d'opposition de l'administration gestionnaire, y compris en l'absence de toute donnée, 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.

Ces recours doivent ainsi être dirigés contre le ministère à l'origine du refus, devant le tribunal administratif, compétent en premier ressort pour ce type de contentieux.

Le Conseil d'État est uniquement appelé à en connaître en cassation et sera d'ailleurs appelé prochainement à se prononcer sur des pourvois formés par les ministères contre des jugements du tribunal administratif de Paris les enjoignant à communiquer les données aux personnes concernées.

Fichier d'antécédents judiciaires : première condamnation de la France par la Cour Européenne des Droits de l'Homme (affaire Brunet contre France)

Pour la première fois, la Cour européenne des droits de l'homme (CEDH) a été appelée à se prononcer sur le fichier STIC et a condamné la France le 18 septembre 2014 pour violation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme (droit au respect de la vie privée).

Si la CEDH ne remet pas en cause l'enregistrement des personnes n'ayant pas fait l'objet de condamnations dans ce fichier d'antécédents judiciaires, elle s'attache à relever que le requérant, qui avait bénéficié d'un classement sans suite pour « médiation pénale », n'a pas pu disposer d'une possibilité de recours afin d'obtenir un effacement des faits avant le terme du délai de conservation (20 ans) et que, de fait, « cette durée est en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum ».

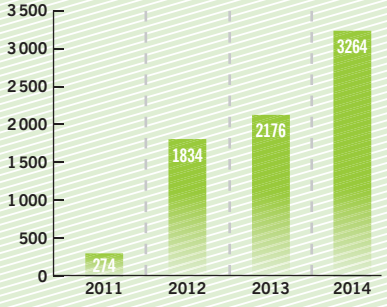
Cette décision juridictionnelle n'a pas d'effet direct et immédiat dans l'ordre juridique national et ne peut conduire, dans le cadre de l'exercice du droit d'accès indirect, à l'effacement dans le fichier TAJ des faits ayant bénéficié d'un classement sans suite pour « médiation pénale » ou « rappel à la loi », par exemple. Seule une modification législative pourrait le permettre car l'article 230-8 du code de procédure pénale limite actuellement les possibilités d'effacement de ce fichier, sous réserve que le procureur de la République le prescrive, aux seules décisions de classement sans suite pour « insuffisances de charges » ou « absence d'infraction ». ■

FOCUS

Le droit d'accès au fichier FICOBA : un nouveau dispositif applicable à compter du 1er janvier 2016 pour les héritiers et les notaires

Depuis la reconnaissance en 2011 par le Conseil d'État, du droit d'accès des héritiers au fichier FICOBA de l'administration fiscale, la CNIL est destinataire d'un nombre important de demandes, qui s'est encore accru en 2014 (+50 %).
La forte attente ainsi exprimée s'explique par le fait que l'exercice d'un tel droit constitue actuellement la seule possibilité ouverte aux héritiers, ainsi qu'aux notaires agissant en leur nom, d'obtenir les données d'identification des comptes utiles pour assurer le règlement des successions (80 % des demandes).
Le nombre de demandes induit actuellement des délais de traitement de l'ordre de plusieurs mois compte tenu de la nécessité pour l'administration fiscale de procéder, pour chacune d'entre elles, à un examen de la situation fiscale. Il tend à lui permettre de déterminer s'il existe des motifs s'opposant à la communication au regard de la finalité de ce fichier qui concourt au recouvrement des impositions et à la lutte contre la fraude fiscale. Seuls 6 % des dossiers examinés en 2014 ont ainsi fait l'objet d'un refus de communication.

Progression des demandes de droit d'accès indirect au fichier FICOBA-2011/2014



Les modalités d'accès à ce fichier vont être modifiées au 1er janvier 2016, date d'entrée en vigueur de la loi n°2014-617 du 13 juin 2014 relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence. Cette loi consacre, en effet, le droit pour les héritiers d'obtenir directement les données d'identification des comptes détenus par le défunt auprès de l'administration fiscale. Les notaires en charge d'une succcession auront, quant à eux, non seulement un droit mais une obligation de l'interroger pour avoir communication de ces mêmes données.
À compter de cette date, les héritiers et notaires ne devront donc plus s'adresser à la CNIL qui demeurera compétente, au titre du droit d'accès indirect, pour les seules demandes formulées à titre personnel (exemple : double détention de livret A).

... HISTOIRES VÉCUES

Effacement des enregistrements

▸ Madame B a souhaité exercer son droit d'accès indirect en raison d'une inscription pouvant lui être préjudiciable dans le cadre de l'exercice de sa profession d'avocate. Elle avait été entendue dans le cadre d'une enquête relative à une affaire de « détention illicite de stupéfiants » concernant son compagnon de l'époque et aucune substance de cette nature n'avait été trouvée lors de la perquisition effectuée, par la police nationale, à son domicile. Au terme des vérifications, cet enregistrement a été supprimé, en accord avec le procureur de la République, car elle avait bénéficié d'un classement sans suite pour « insuffisances de charges ».

▸ Madame L a adressé à la CNIL une demande de droit d'accès indirect car, si dans le cadre d'une enquête de moralité dans le cadre du concours d'accès à l'École Nationale de la Magistrature, un avis favorable a été émis, elle a appris à cette occasion qu'elle faisait l'objet d'une inscription dans le fichier d'antécédents judiciaires pour des faits qu'elle n'avait pas commis. Tel était bien le cas et cette affaire de « complicité d'escroquerie », qui aurait pu lui faire perdre le bénéfice de ce concours, a été effacée.

▸ Monsieur D, 55 ans a saisi la CNIL après que le Préfet de son département lui a signifié une probable abrogation de son agrément en qualité d'agent de police municipale au motif de son inscription dans le fichier d'antécédents judiciaires. Au terme des vérifications, l'affaire concernée (« refus d'obtempérer, mise en danger de la personne, défaut de permis de conduire ») a été supprimée dans la mesure où il n'était nullement le mis en cause, mais la victime.

▸ Monsieur L., 54 ans, préoccupé par l'absence de réponse obtenue quant à la délivrance de sa carte professionnelle d'agent de sécurité privée a souhaité exercer son droit d'accès indirect. Aux termes des vérifications menées, une affaire de « violences volontaires et d'outrage à agent de la force publique » enregistrée à son nom dans ce fichier a été supprimée car, commise par un tiers qui avait usurpé son identité.

Mise à jour du fichier par mention des décisions judiciaires favorables obtenues

▸ Madame L., souhaitant entrer dans la police nationale, s'est inquiétée de son inscription pour un « vol simple » à la suite d'une plainte de son ancien employeur pour le vol d'une pochette d'autocollants d'une valeur de 1,40 euros. Au terme des vérifications, cette affaire a fait l'objet d'une mise à jour par mention de la décision de classement sans suite dont elle avait bénéficié. Dès lors, elle ne sera plus accessible lors de la consultation de ce fichier dans le cadre de l'enquête moralité à laquelle elle sera soumise.

▸ Monsieur R., 36 ans, travaillant depuis plus de 8 ans dans le domaine du nucléaire a saisi la CNIL compte tenu de la perte imminente de son emploi à la suite du refus du préfet de son département de lui accorder l'agrément nécessaire pour accéder à un site nucléaire. À la suite des démarches de la CNIL, les informations relatives à l'affaire concernée (« violation de la vie privée ») ont fait l'objet d'une mention car il avait bénéficié d'un classement sans suite pour « rappel à la loi ».

CONTRÔLER ET SANCTIONNER

Dans le cadre de son pouvoir de contrôle a posteriori, la CNIL a réalisé **421 vérifications en 2014**, dont les premiers contrôles « en ligne », conformément à la loi relative à la consommation de mars 2014.

La CNIL a procédé à **333 contrôles « Informatique et Libertés » en 2014 (280 en 2013), dont 58 ont été réalisés « en ligne »**. La mise en œuvre effective de ce nouveau pouvoir de contrôle porte le nombre de contrôles opérés sur le fondement de la seule loi « Informatique et libertés » à 79 %. Les 21 % restant correspondent aux **88 contrôles relatifs aux systèmes vidéo**, également soumis aux dispositions du Code de la sécurité intérieure (CSI).

S'agissant de la répartition des missions, 75 % concernaient le secteur privé, 25 % le secteur public. En revanche, en matière de vidéo, 62 % ont été réalisés dans le secteur public, essentiellement auprès de collectivités locales. L'objectif était notamment de s'assurer que les caméras utilisées sur la voie publique et disposant de zooms très puissants, ne filmaient pas dans les habitations. Depuis 2011, la CNIL a réalisé plus de 500 contrôles sur ce type de dispositifs, soit plusieurs dizaines de milliers de caméras vérifiées sur l'ensemble du territoire national. ■

421
CONTRÔLES

DONT
58 CONTRÔLES EN LIGNE
88 CONTRÔLES VIDÉO

INFOS +

L'origine des contrôles

• 28 % résultent du programme annuel décidé chaque année par la Commission ;
• 24 % s'inscrivent dans le cadre de l'instruction de plaintes ;
• 40 % sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;
• 6 % font suites à un courrier d'observation adressé après un premier contrôle ;
• 2 % sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction.

FOCUS

Premiers bilans

Le paiement en ligne au travers de la lutte contre la fraude et la conservation des données bancaires

Cette question a conduit la Commission à procéder à 20 contrôles sur place : 14 auprès d'e-commerçants et 6 auprès de leurs prestataires. Il est apparu que plus d'un quart des organismes contrôlés mettaient en œuvre un traitement d'exclusion (aux fins de prévention de la fraude) sans autorisation de la CNIL. Les principaux manquements constatés concernaient les conditions de collecte et de conservation de données issues des cartes bancaires : copies du recto/verso de la carte bancaire, conservation du cryptogramme visuel au-delà de la durée nécessaire au paiement, absence de chiffrement des informations en base, etc. Enfin, plusieurs e-commerçants conservaient les données relatives à la carte bancaire, en vue de faciliter d'éventuels achats ultérieurs sur le même site, sans recueillir le consentement exprès des consommateurs concernés.

Les réseaux sociaux de rencontre en ligne

En 2014, la CNIL a réalisé 10 contrôles de sites de rencontre parmi les plus connus, choisis en fonction de leur fréquentation ou de leurs particularités. Les constatations effectuées ont permis de mieux appréhender les pratiques de ce secteur, ainsi que les modalités de gestion des données personnelles. À cet égard, et compte tenu de la nature « sensible » des données des utilisateurs de ces sites, la CNIL a constaté que les mesures prises pour assurer la protection de ces données n'étaient globalement pas satisfaisantes. Il a notamment été relevé que les données des utilisateurs sont le plus souvent conservées sans limitation de durée. Aussi, la CNIL encourage-t-elle d'ores et déjà vivement les sites de rencontre à mieux prendre en compte les enjeux de la protection des données, vecteur de confiance pour leurs utilisateurs.

Les autres thèmes inscrits au programme des contrôles 2014 sont en cours d'achèvement et leurs bilans respectifs seront établis au cours du premier semestre 2015. Les premiers éléments disponibles sont les suivants :

FOCUS

Premiers éléments - Bilans prévus en 2015 :

Le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV)

Le programme de contrôle s'attache à vérifier les deux volets de ce fichier du ministère de la justice : le suivi des personnes inscrites et le contrôle des personnes en charge de l'encadrement de mineurs (notamment le ministère de l'éducation nationale et les collectivités locales). La quinzaine de missions planifiées vise à s'assurer, auprès de l'ensemble des acteurs autorisés à y accéder (notamment les services de police et unités de gendarmerie, les juridictions, les préfectures) de la légalité des conditions d'alimentation, de mise à jour et d'exploitation du fichier.

Le fonctionnement du Fichier des Incidents de remboursement des Crédits aux Particuliers (FICP)

Les problématiques relatives aux conditions d'utilisation du FICP génèrent chaque année un volume important de plaintes. Les contrôles ont pour objectif de s'assurer d'une application rigoureuse des textes relatifs au FICP, et notamment de l'arrêté du 26 octobre 2010 qui définit ses règles de fonctionnement. Il s'agit d'appréhender les conditions de mise en œuvre des traitements relatifs à ce fichier, et en particulier des traces des inscriptions et désinscriptions qui peuvent être conservées au sein des traitements de gestion de la clientèle par les établissements financiers.
Les enjeux de cette thématique sont particulièrement importants car toute négligence des organismes de crédit (notamment en cas de fichage injustifié ou d'absence de « défichage » après remboursement) a des répercussions graves pour les particuliers concernés, déjà souvent fragilisés par une situation d'endettement. Une vingtaine de contrôles, tant sur pièces que sur place, est envisagée.

Les traitements mis en œuvre au titre du paiement et du recouvrement de l'impôt sur le revenu

Les traitements visés par cette thématique concernent une grande partie de la population (19,2 millions de contribuables imposés en 2013) et ont fait l'objet de fortes évolutions avec l'introduction des procédures en ligne. En outre, certains fichiers sont relativement sensibles car en lien avec la lutte contre la fraude, ce qui justifie de vérifier les modalités concrètes de leur mise en œuvre.
Les contrôles portent sur les principales étapes que doit suivre un dossier d'un particulier, en partant de l'identification du contribuable, de sa déclaration de revenus, de son règlement, de la vérification des données déclarées ainsi que de l'éventuelle mise en recouvrement susceptible de conduire à un contentieux. En conséquence, des missions ont d'ores et déjà eu lieu auprès de services des impôts des particuliers (SIP), d'établissements de service informatique (ESI), de centres de données ou de structures en charge du contrôle fiscal. Les mesures de sécurité et de confidentialité font l'objet d'une attention spécifique.

LES DONNÉES DES PERSONNES DÉTENUES EN ÉTABLISSEMENTS PÉNITENTIAIRES

Au titre du programme annuel de contrôles de la CNIL en 2013, figuraient « les données des personnes détenues en établissements pénitentiaires ».

Fin 2013-début 2014, ce sont **18 contrôles sur place qui ont été réalisés sur l'ensemble du territoire national** auprès d'établissements pénitentiaires (7 contrôles en maisons d'arrêt, centres de détention, maisons centrales), de services de l'administration pénitentiaire (7 contrôles au sein des services centraux et interrégionaux), ou d'acteurs privés agissant pour le compte de l'administration (4 contrôles).

Ces vérifications, qui ont pu donner lieu à des échanges avec le Contrôleur général des lieux de privation de liberté (CGLPL), ont permis d'appréhender de façon exhaustive l'ensemble des acteurs et des activités donnant lieu au traitement

de données concernant les personnes placées sous écrou.

L'objectif visait en effet à analyser et apprécier le fonctionnement des fichiers utilisés dans les établissements pénitentiaires, tant au niveau national que local.

C'est ainsi que près d'une dizaine de thématiques ont fait l'objet de contrôles, notamment :

- Les traitements utilisés en prison : fichiers GIDE (gestion informatisée des détenus en établissement) et CEL (cahier électronique de liaison) relatifs à la gestion de la détention de la personne sous écrou ;
- Les traitements relatifs à la surveillance des détenus ;
- Les systèmes de caméras installés au sein et aux abords des prisons ;
- Les dispositifs biométriques utilisés en prison ;
- Les applications et dispositifs de surveillance électronique (bracelets électroniques) ;
- Les fichiers des intervenants extérieurs (sollicités notamment dans les domaines de l'emploi, de la formation et de la restauration des détenus).

Au terme de ces contrôles, il apparaît que les conditions de traitement des données des personnes sous écrou sont contrastées.

L'utilisation et le fonctionnement des applications et traitements nationaux apparaissent en effet globalement satisfaisants.

Néanmoins, les fichiers mis en œuvre et gérés au niveau local (au sein des établissements et par les intervenants extérieurs) ne bénéficient pas de la même rigueur concernant le respect des dispositions de la loi du 6 janvier 1978 modifiée et des textes prévus.

Il apparaît nécessaire de mieux formaliser et unifier leur fonctionnement et leur contrôle – notamment lors d'échanges de données avec des acteurs collaborant avec l'administration pénitentiaire - afin de permettre une mise en œuvre des fichiers à la fois efficace pour les services du ministère de la justice et respectueuse des droits des citoyens.

Ces conclusions ont été portées à la connaissance de Mme la Garde des Sceaux et ont notamment donné lieu à la mise en conformité de traitements jusqu'alors non déclarés. ■

BILAN DES ACTIONS COORDONNÉES AU NIVEAU EUROPÉEN & INTERNATIONAL

En 2014, la CNIL a de nouveau participé à des actions coordonnées d'audits à l'échelle internationale en collaboration avec d'autres autorités de protection de données. Elle a, en particulier, mené deux actions aux côtés de ses homologues pour lesquelles les autorités ont travaillé sur la base d'une grille d'analyse commune.

Applications mobiles - Mobile privacy sweep Day -

En mai 2014, la CNIL et 26 homologues membres du GPEN (« Global Privacy Enforcement Network » – réseau international d'autorités en charge de la protection de la vie privée) ont mené une opération conjointe d'audit en ligne des principales applications mobiles. Cette campagne avait pour objectif de vérifier si l'information délivrée aux utilisateurs concernant le traitement de leurs données personnelles était satisfaisante. Pour ce faire, **la CNIL a choisi d'examiner les 100 applications mobiles les plus utilisées en France**. Les audits effectués ont permis de révéler que les applications collectaient massivement des données personnelles, parfois sans lien avec l'objet de l'application elle-même. De même, à cette occasion, il a été constaté que l'information des utilisateurs est souvent incomplète et/ou difficilement accessible. Au-delà d'un constat à l'échelle international sur les pratiques d'un secteur, cette opération a permis de sensibiliser les utilisateurs de smartphones aux questions relatives à la protection des données et de promouvoir les bonnes pratiques auprès des acteurs concernés.

Cookie Sweep Day

En septembre 2014, la CNIL et 7 de ses homologues européens compétents en matière de cookies, dont 5 membres du G29, ont réalisé un audit simultané des sites internet européens les plus fréquentés en matière d'utilisation des cookies. Au total, **478 sites internet ont été analysés, dont près de 100 par la CNIL**. Ce « Cookie Sweep Day » a été l'occasion pour les « CNIL » européennes de dresser un état des lieux des pratiques en la matière. En particulier, il a mis en lumière une tendance généralisée au dépôt d'un nombre important de cookies, particulièrement par les sites médias. Il a également permis de constater que la majorité des cookies provient de sites tiers (dits « cookies tiers ») et est déposée dès l'arrivée de l'internaute sur la page d'accueil. Enfin, si l'information relative à ces traceurs s'améliore, des progrès significatifs sont encore nécessaires concernant le recueil du consentement des internautes. L'ensemble de ces enseignements sera utile à la CNIL et à ses homologues dans le cadre des actions de mise en conformité à initier à l'échelle européenne auprès de la chaîne d'acteurs concernés par cette problématique (éditeurs de sites, annonceurs, régies publicitaires, etc.). ■

CONTRÔLES EN LIGNE

À l'occasion de l'adoption de la loi relative à la consommation du 17 mars 2014, la CNIL s'est vue reconnaître la possibilité d'effectuer des contrôles en ligne, lui permettant de constater à distance, depuis un ordinateur connecté à internet, des manquements à la loi Informatique et Libertés.

Cette adaptation du pouvoir d'investigation de la CNIL au développement numérique, vient s'ajouter aux autres moyens d'enquête déjà existants : contrôles sur place au sein des organismes, auditions sur convocation à la CNIL et contrôles sur pièces.

Elle offre à la CNIL l'opportunité d'être plus efficace et réactive dans un univers en constante évolution. Elle peut ainsi plus rapidement constater et agir contre les atteintes à la protection des données et à la vie privée sur internet.

En pratique, les constatations sont effectuées depuis les locaux de la CNIL sans la présence du responsable de traitement, qui en est informé une fois les vérifications effectuées.

Pour ce faire, un environnement technique particulier est mis en place au sein du service des contrôles de la CNIL, afin de garantir l'authenticité des constatations effectuées par les agents. Lors des contrôles, les éléments recueillis ainsi que les constatations sont consignés dans un procès-verbal.

En raison des contraintes techniques liées à la mise en place d'un tel projet et de la nécessité de définir une stratégie de vérification opérationnelle ainsi que des outils juridiques adéquats, le premier contrôle en ligne a été réalisé en octobre 2014.

Au total, 58 contrôles en ligne ont ainsi pu être effectué en 2014, sur plusieurs thématiques, dont :

- La conformité des pratiques des acteurs du web à la recommandation cookies et autres traceurs, adoptée par la CNIL le 5 décembre 2013 ;
- La publication des listes d'électeurs sur les sites web des Universités ;
- La sécurité relative aux formulaires de demande en ligne d'actes d'état civil sur les sites des communes.

Ces premiers contrôles ont eu principalement pour objet de de vérifier certains aspects de la loi « Informatique et Libertés » tels que :

- La pertinence des données collectées (article 6 de la loi « informatique et libertés ») ;
- Les mentions d'information à destination du public (article 32) ;
- La sécurité des données collectées et traitées (article 34) ;
- La réalité des formalités indiquées (articles 22 et suivants).

Par ailleurs, les vérifications en ligne ont également porté sur des failles de sécurité. Ce mode de contrôle a ainsi permis à la CNIL de procéder aux constatations nécessaires et d'en informer les organismes concernés dans des laps de temps réduits.

Sur ce point, les investigations ont porté sur des « données librement accessibles ou rendues accessibles » en ligne et qu'à aucun moment la CNIL n'a forcé les mesures de sécurité mises en place pour pénétrer dans un système d'information. ■

UNE ACTIVITÉ RÉPRESSIVE EN HAUSSE

Le bilan de l'année 2014 est marqué par l'augmentation substantielle du nombre de mises en demeure adoptées par la Présidente de la CNIL.

En effet, 62 mises en demeure ont été adoptées cette année, dont 4 ont été rendues publiques.

Ces mises en demeure font suite à l'instruction de plaintes (15 %), à la réalisation de contrôles sur le fondement de plaintes (30 %) et à des contrôles résultant du programme annuel défini par la CNIL ou effectués à l'initiative de la CNIL en lien avec l'actualité (55 %).

En 2014, **68 % des mises en demeure adoptées ont donné lieu à une mise en conformité et ont été clôturées, les autres étant en cours ou ayant été suivies d'une procédure de sanction faute pour l'organisme de s'y conformer**.

Enfin, 31 % des mises en demeure clôturées ont donné lieu à un contrôle post-mise en demeure révélant pour la majorité des organismes une mise en conformité effective.

Cette année encore, cette stratégie d'accompagnement a prouvé son efficacité auprès des organismes, ceux-ci devant corriger leurs traitements conformément aux obligations résultant de la loi « Informatique et Libertés » dans un délai déterminé.

Ce taux important de conformité au stade de la mise en demeure explique le nombre limité de sanctions proposées à la formation restreinte, même si ce dernier a augmenté d'un tiers par rapport à 2013 : ce sont en effet 18 rapports de sanction qui ont été examinés par la formation restreinte en 2014 contre 14 en 2013. Ces dossiers ont donné lieu à 8 sanctions pécuniaires (dont 7 publiques), et 3 relaxes. En outre, 7 avertissements dont 4 publics ont également été décidés par la formation restreinte directement sans mise en demeure préalable. ■

62
MISES EN DEMEURE

18
RAPPORTS DE SANCTION

8
SANCTIONS PÉCUNIAIRES DONT 7 PUBLIQUES

7
AVERTISSEMENTS DONT 4 PUBLICS

3
RELAXES

D'IMPORTANTS ARRÊTS DU CONSEIL D'ÉTAT

L'aspiration de données issues de réseaux sociaux est soumise à une information préalable des personnes concernées

Le 12 mars 2014, le Conseil d'État a confirmé l'avertissement public prononcé par la CNIL à l'encontre d'une société éditant un annuaire en ligne en septembre 2011[1]. Cette société avait, pour étoffer son annuaire en ligne, aspiré les informations de 25 millions de personnes issues de leurs profils accessibles sur divers réseaux sociaux, sans qu'aucune information ne leur ait été délivrée au préalable.

Dans cet arrêt, le Conseil d'État relève que cette collecte de données est déloyale et illicite en raison de l'absence d'information préalable des intéressés et faute de recueillir leur « *consentement explicite et éclairé* ». En effet, contrairement à ce qui était soutenu par la société, ces deux points n'exigeaient pas d'« *efforts disproportionnés par rapport à l'intérêt de la démarche* ». Le Conseil d'État confirme par ailleurs que la collecte d'adresses IP dans le but de répondre aux demandes d'information des autorités administratives et judiciaires n'est pas adéquate, comme l'avait relevé la Formation restreinte de la CNIL. En effet, en l'espèce, une telle collecte ne répondait à aucune obligation légale.

À RETENIR

Le Conseil d'État confirme qu'une mise en demeure de la CNIL ne constitue ni une sanction, ni l'une des autres décisions individuelles défavorables nécessitant que le mis en cause présente ses observations préalablement.

Un courriel professionnel constitue bien une donnée à caractère personnel

Le 11 avril 2014, le Conseil d'État a confirmé la décision de mise en demeure de la Présidente de la CNIL à l'encontre d'une entité[3], du fait de la collecte et de la publication à l'insu de professionnels du droit de leurs coordonnées professionnelles dans l'annuaire du site internet de l'Association, ainsi que le non respect de leur droit d'opposition à figurer dans cet annuaire.

Contestant avoir violé la loi du 6 janvier 1978 modifiée, l'association avait demandé l'annulation de cette délibération devant le Conseil d'État, le 4 avril 2011, considérant que la CNIL avait estimé à tort que les coordonnées d'un professionnel exerçant à titre individuel constituaient des données à caractère personnel au sens de la loi précitée. Estimant que cette distinction n'apparaît pas dans la loi, le Conseil d'État qualifie les coordonnées professionnelles de personnes physiques de « données à caractère personnel ».

La CNIL confortée dans son appréciation du responsable de traitement

Dans un arrêt rendu le 12 mars 2014, le Conseil d'État a confirmé l'avertissement public prononcé par la CNIL à l'encontre d'une société de gestion immobilière en octobre 2011 du fait de l'enregistrement, dans ses fichiers, de commentaires excessifs portant sur des clients ou prospects d'agences immobilières, filiales du groupe. En effet, les vérifications conduites par la CNIL avaient permis de constater la présence d'insultes, de données relatives à des condamnations, à l'état de santé ou encore aux opinions religieuses des personnes.

Cette décision du Conseil d'État est particulièrement intéressante car elle retient que la société mère doit en l'espèce être considérée comme le responsable du traitement. En effet, c'est bien la maison mère qui a déterminé les finalités et les moyens de ce traitement, en ce qu'elle a décidé de la nature des données collectées, déterminé les droits d'accès à celles-ci, mais également fixé la durée de conservation des données et apporté les correctifs nécessaires après le contrôle de la CNIL. La circonstance que les filiales du groupe ont désigné un correspondant informatique et libertés ne suffit pas à les qualifier de responsables de traitement du fichier concerné. ■

À RETENIR

Le Conseil d'État confirme dans cet arrêt que la procédure de sanction de la CNIL respecte les principes d'indépendance et d'impartialité notamment par une séparation effective des fonctions d'instruction et de sanction[2].

À RETENIR

Le Conseil d'État confirme une nouvelle fois que la procédure suivie par la CNIL pour prononcer des sanctions respecte les principes d'indépendance et d'impartialité. En effet, la Présidente de la CNIL ne siégeant pas dans la formation restreinte qui prononce les sanctions, la séparation des fonctions de poursuite et de sanction est assurée.

1/ Délibération de la Formation restreinte n°2011-203 du 21 septembre 2011. 2/ Cette position avait déjà était celle du Conseil d'État dans une autre affaire opposant la CNIL à la société Profil France en référé. Il avait en outre précisé dans cette décision, que les stipulations de l'article 6 précité pas plus qu'aucun principe général du droit, n'imposent la séparation des phases d'instruction et de jugement au sein d'un même procès.

Liste des sanctions prononcées en 2014

Date	Nom ou type d'organisme	Thème	Manquements principaux retenus par le rapporteur	Décision adoptée
03/01/2014	GOOGLE INC*	Moteur de recherche/ internet	Défaut d'information, non définition d'une durée de conservation, défaut de base légale pour la combinaison des données, défaut de recueil du consentement	Sanction pécuniaire publique de 150 000 euros
29/01/2014	SOCIÉTÉ DE TRANSPORT	Vidéosurveillance	Non pertinence et caractère excessif des données, défaut d'information	Sanction pécuniaire non publique de 10 000 euros
29/01/2014	COMMERCE	Fichier client - NIR	Non pertinence et caractère excessif des données	Avertissement non public
29/01/2014	ASSOCIATION FRANCAISE DES URBANISTES	Droit opposition d'une personne à ce que son CV soit retiré du site de l'association	Défaut de formalités préalables, non respect du droit d'opposition des personnes, défaut de réponse aux demandes de la CNIL	Sanction pécuniaire publique de 1 euro
29/01/2014	ASSOCIATION JURICOM ET ASSOCIES*	Droit opposition des personnes à ce que les données professionnelles soient mises en ligne sur le site de l'association	Non respect du droit d'opposition des personnes	Sanction pécuniaire publique de 10 000 euros
12/06/2014	DHL INTERNATIONEL EXPRESS France	Fuite de données	Défaut de sécurité et de confidentialité des données, durée de conservation excessive	Avertissement public
26/06/2014	REGIME COACH	Collecte de données via un site internet d'accompagnement de régime	Défaut d'information, défaut de sécurité et de confidentialité des données, défaut de coopération avec la CNIL	Avertissement public
17/07/2014	FEDERATION FRANCAISE D'ATHLETISME	Publication des résultats des compétitions sur le site internet de la fédération	Défaut d'information, défaut de sécurité et de confidentialité des données	Sanction pécuniaire publique de 3 000 euros
17/07/2014	PROVIDIS	Vidéosurveillance	Défaut d'information, défaut de sécurité et de confidentialité des données, absence de définition de durée de conservation, collecte excessive de données	Sanction pécuniaire publique de 5 000 euros
17/07/2014	SOCIETE DE RESTAURATION	Vidéosurveillance	Défauts d'adéquation, de pertinence des données	Relaxe
22/07/2014	LOC CAR DREAM*	Géolocalisation	Absence de formalité préalable, collecte excessive des données, défaut d'information, défaut de sécurité des données, défaut de coopération avec la CNIL	Sanction pécuniaire publique de 5 000 euros
07/08/2014	ORANGE*	Fuite de données	Défaut de sécurité et de confidentialité des données	Avertissement public
07/08/2014	CA CONSUMER FINANCE (CREDIT AGRICOLE)	Inscriptions illicites et maintien d'inscription au FICP malgré la régularisation de la situation - confidentialité	Absence de mise à jour des données, collecte illicite, défaut de sécurité et de confidentialité des données	Avertissement public
25/09/2014	ETABLISSEMENT PUBLIC	Gestion des usagers	Durée de conservation des données, sécurité et confidentialité des données	Avertissement non public
20/11/2014	SOCIETE DU SECTEUR DE L'AUDIOVISUEL	Droit d'opposition	Droit d'opposition, défaut de coopération avec la CNIL	Relaxe
27/11/2014	SITE INTERNET D'INFORMATIONS	Fuite de données	Défaut de confidentialité et de sécurité des données	Avertissement non public
27/11/2014	SPHERE	Droit d'opposition	Droit d'opposition, défaut de coopération avec la CNIL	Sanction pécuniaire publique de 3 000 euros
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 Conseil d'État en cours*

ANTICIPER ET INNOVER

Dans le cadre de son activité d'innovation et de prospective, la CNIL s'efforce de concilier deux objectifs : anticiper très en amont de nouveaux usages, tendances, ou technologies émergents, et aborder des sujets d'étude et d'analyse par l'intermédiaire d'outils et de projets innovants. En 2014, cette double approche s'est incarnée notamment dans la poursuite du projet Mobilitics.

LE PROJET MOBILITICS CONTINUE

Depuis trois ans, la CNIL et l'équipe « Privatics » d'Inria travaillent ensemble sur le projet Mobilitics, qui a été pour la CNIL le premier véritable projet de R&D piloté dans le cadre de son laboratoire d'innovation. Ce projet a permis de développer à des fins de recherche un outil capable de détecter les accès à des données personnelles dans les smartphones (accès à la localisation, aux photos, au carnet d'adresses, à des identifiants du téléphone, etc.). En 2013, plusieurs agents de la CNIL volontaires ont ainsi utilisé des iPhones du laboratoire et ont permis le test de 189 applications sur 3 mois et en conditions réelles. L'expérience a été répétée en 2014, sur des smartphones équipés d'Android version « Jelly Bean », ce qui a permis de tester 121 applications dans cet environnement.

Dès la première vague sous iOS, il a été possible de tirer trois séries d'enseignements :

- le statut particulier de la géolocalisation, reine des données du smartphone ;
- la tendance des développeurs et éditeurs d'applications à recourir à des stratégies d'identification aux objectifs très divers (mesures d'audience, statistiques d'utilisation, *analytics*, monétisation et publicité, …) ;
- la difficulté à corréler les accès aux données avec les actions de l'utilisateur ou des besoins légitimes des applications.

Comparaison entre les deux saisons

	iOS 5 (tests de novembre 2012 à janvier 2013)		**Android « Jelly Bean »** (tests de juin à septembre 2014)	
Nombre d'applications	**189**		**121**	
Qui communiquent sur le réseau	176	93 %	80	66 %
Qui accèdent à l'UDID/android ID	87	46 %	41	34 %
Qui accèdent à la géolocalisation	58	31 %	29	24 %
Qui accèdent au carnet d'adresses	15	8 %	20	17 %
Qui accèdent au calendrier	3	2 %	4	3 %
Qui accèdent au nom de l'appareil	30	16 %	N/A	
Qui accèdent au nom d'opérateur	N/A		28	23 %
Qui accèdent à l'IMEI (identité d'équipement mobile)	N/A		24	20 %
Qui accèdent à l'adresse MAC WiFi	N/A		9	7 %
Qui accèdent au numéro de téléphone	N/A		7	6 %
Qui accèdent à l'identifiant de carte SIM (ICCID)	N/A		6	5 %
Qui accèdent à la liste des points d'accès WiFi (SSID)	N/A		5	4%

La course aux identifiants pour tracer l'utilisateur

Lors de la première vague, prés d'une application testée sur deux avait accédé à un identifiant unique alphanumérique de l'appareil appelé UDID (*Unique Device Identifier*). 40 % des applications accédant à l'UDID l'avaient en outre envoyé « en clair » (c'est-à-dire sans le chiffrer) sur le réseau.

À l'époque, cet identifiant était encore accessible à toutes les applications. Les versions suivantes du système d'exploitation iOS d'Apple ont limité l'accès à cette donnée tout en créant deux identifiants, l'un dédié à la publicité (*Advertising Identifier*), et l'autre, qui est unique pour chaque éditeur d'application (*Identifier for vendor*).

L'expérimentation Android montre des logiques similaires, mais dans un environnement par nature plus ouvert et moins contrôlé *a priori* que celui d'iOS. L'Android ID est ainsi un identifiant persistant comparable à l'UDID d'Apple tel qu'il fonctionnait en 2013, c'est-à-dire qu'il s'agit d'une série alphanumérique non modifiable. L'*advertising ID* (ad ID) est, quant à lui, un identifiant dédié à la publicité que les utilisateurs peuvent réinitialiser. Depuis le 1er aout 2014, Google impose à toute nouvelle application (ou à toute application mise à jour) de n'utiliser que cet identifiant pour des fins publicitaires.

Les systèmes d'exploitation et leurs magasins d'application, des acteurs pas comme les autres

La saison 1 de Mobilitics avait montré une présence non négligeable d'Apple dans son propre écosystème en tant que collecteur de données issues de l'iPhone[1].

Déjà dans iOS, Google était un acteur extrêmement présent à travers ses différents services (Google maps, gmail, Google search) mais également en tant que fournisseur de fonctionnalités (publicité, analytics).

Les résultats issus des smartphones Android renforcent ce constat, en particulier pour certains services installés par défaut sur les appareils :

- L'application Play Store, qui est quasiment indispensable au fonctionnement d'un téléphone Android, est ainsi l'une des plus grosses consommatrices de données puisqu' elle a accédé en 3 mois et pour un seul utilisateur 1 300 000 fois à la localisation cellulaire et 290 000 fois au GPS ;
- L'application-*widget* « Actualités et météo » a accédé 1 560 926 fois à la localisation de l'utilisateur pendant les trois mois de l'expérimentation.

Or, ces applications étant présentes par défaut sur l'appareil et ne pouvant être supprimées, l'utilisateur n'a pas pu consulter les informations collectées, qui sont généralement affichées avant le téléchargement et l'installation d'une application sur Android.

La mise en œuvre de mesures d'information et de réglages spécifiques pourrait dès lors être envisagée. Il serait par

1 / Par exemple, Apple utilise les iPhones pour mettre à jour ses bases de données de localisation des antennes wifi, sur lesquelles reposent ses propres services de cartographie. Il utilise également l'envoi de données vers ses propres serveurs pour des services tels que Siri, qui est basé sur l'analyse de la voix.

> La mise en œuvre de mesures d'information et de réglages spécifiques pourrait être envisagée.

exemple possible de créer des réglages dédiés, par exemple un tableau de bord (*dashboard*) explicitant leurs accès et transmissions de données et les raisons associées, avec des possibilités de refuser (*opt out*) ou de ne pas accepter (*opt in*) certaines fonctions.

Ces résultats permettent à la CNIL d'affiner son accompagnement de la mise en conformité de cet écosystème complexe, dans lequel cohabitent de nombreux acteurs dont les tailles et modèles économiques diffèrent. Editeurs de systèmes d'exploitation, fabricants de téléphone, développeurs et éditeurs d'applications, publicitaires, fournisseurs de services (monétisation, analyse d'audience), chacun doit prendre la mesure des progrès à faire pour donner une meilleure information et plus de contrôle aux utilisateurs. ■

INFOS +

Qu'est-ce que le quantified self ?

Le *quantified self* ou le « soi quantifié » renvoie à un ensemble de pratiques variées qui ont toutes pour point commun, de retranscrire en chiffres, de mesurer et de comparer avec d'autres personnes des variables relatives au mode de vie : nutrition, activités physiques, poids, sommeil…

QUANTIFIED SELF, M-SANTE : LE CORPS EST IL UN NOUVEL OBJET CONNECTÉ ?

Mesurer le nombre exact de pas parcourus dans la journée, suivre son poids avec une balance connectée, mesurer la qualité de son sommeil avec un bracelet, un podomètre ou une montre, autant de possibilités offertes aux adeptes de la « quantification de soi ». Ces objets connectés posent des questions nouvelles. Quel contrôle l'individu doit-il avoir sur la transmission et l'utilisation de ces données ? Quels sont les modèles économiques associés à ces données ? Et surtout, qui sont les acteurs qui doivent et peuvent y avoir accès ?

C'est pourquoi, à l'occasion de la publication du Cahier innovation et prospective consacré à ce sujet, la CNIL a organisé une table-ronde afin d'éclairer le débat, ainsi que des ateliers avec les professionnels.

Quelles applications ?

Que ce soit au travers d'une application mobile de santé ou d'une balance connectée, ces usages se fondent sur des captures de données de plus en plus automatisées et induisent la circulation de grandes masses de données personnelles, parfois intimes. Ces échanges de données se font à l'initiative des individus eux-mêmes qui souhaitent partager leurs données ; ils aliment aussi les modèles économiques de ce marché émergent.

Aujourd'hui, il s'agit essentiellement de bracelets, de podomètres, de montres ou d'applications mobiles recourant aux capteurs du smartphone. Si le *quantified self* en tant que mouvement reste marginal, il s'étend progressivement et rapidement auprès du grand public. **On estime qu'en 2017 un utilisateur de smartphone sur deux aura installé au moins une application dédiée au bien-être ou à la santé** (source : Research2Guidance, 2013). On parle déjà pour demain d'un marché des wearables technologies (intégrant lunettes, bijoux, vêtements…) estimé à 30 milliards de $ à l'horizon 2018 ▸▸▸

La numérisation de nos activités humaines n'a pas de limites : elle concerne désormais notre corps et ce que nous en faisons.

▸▸▸ où les capteurs seront présents sur de nouveaux supports (source : Wearable World, 2014).

En tout état de cause ce sont bien des données du corps qui sont concernées. C'est à cette aune que les axes de réflexion sur une éventuelle régulation à venir doivent être débattus : va-t-on vers un habeas corpus de l'Homme capté ? ■

INFOS +

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 d'un trajet de sa navigation. CookieViz est proposé en téléchargement gratuit.
C'est le premier outil logiciel développé en interne et mis à disposition dans une première version « beta » qui peut être enrichie. CookieViz a été téléchargé plus de 100 000 fois depuis son lancement en décembre 2013.

INFOS +

Le cahier IP

Pour développer une réflexion ouverte sur le sujet, la CNIL a conduit une série de travaux : entretiens avec des experts (chercheurs, acteurs économiques, institutionnels, médecins) ; état des lieux à l'international sur les régulations à l'œuvre dans

le domaine des applications mobiles de santé et des capteurs connectés ; étude du marché et du modèle économique des acteurs ; lancements de tests de capteurs et d'applications dans le cadre du laboratoire d'innovation de la CNIL, etc.
Tous ont servi à alimenter le deuxième numéro des Cahiers Innovation et Prospective.
Il met en évidence que si la plupart des pratiques actuelles peuvent sembler ludiques au premier abord, la frontière avec des applications relevant du monde médical peut s'avérer particulièrement ténue. Des transformations profondes sont à l'œuvre : évolution, voire bouleversement des pratiques médicales et émergence de nouveaux entrants sur le « marché » de la santé susceptibles de concurrencer les acteurs traditionnels.

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. Elle préside le G29 depuis février 2014.

2014, ANNÉE CHRYSALIDE POUR L'EUROPE

La protection des données intervient dans un environnement en constante évolution, aussi bien en termes d'usage, de technologies ou d'encadrement juridique. Sur ce dernier point, l'Europe connaît deux révisions importantes, portant respectivement sur la législation de l'Union européenne et la Convention 108 du Conseil de l'Europe.

Un cap a été franchi en mars 2014 par le Parlement européen avec l'adoption à l'unanimité d'une position sur la proposition de règlement européen en matière de protection des données. Cette avancée est cruciale puisque le règlement – d'applicabilité directe – devra à terme remplacer le texte fondateur actuel, la Directive 95/46/EC et l'ensemble des lois nationales de transposition prises sur son fondement. Les 28 gouvernements rassemblés sous l'égide du Conseil de l'UE ont de leur côté progressé sur plusieurs points essentiels du nouveau cadre juridique. L'année 2015 doit être l'année du trilogue et de l'adoption finale du nouveau modèle européen en matière de protection des données.

2014 a été également l'année de **négociations intenses** entre les 47 membres du Conseil de l'Europe sur le premier instrument juridique européen, la Convention 108, dont le protocole d'amendement sera transmis à l'ultime instance de décision, le Comité des Ministres, pour adoption en 2015.

La CNIL suit de près ses évolutions réglementaires qui s'influencent mutuellement et révolutionneront, une fois adoptées, le paysage européen.

En ces temps de transformation pour l'Europe, le G29 a été amené en février 2014 à désigner un nouveau président pour le G29, capable d'enclencher sa mutation et d'accompagner la mise en œuvre du nouveau cadre juridique européen. Isabelle Falque-Pierrotin, Présidente de la CNIL, a ainsi été élue par ses pairs à la tête du G29 pour une durée de deux ans. Celle-ci a rappelé lors de son élection la nécessité, plus que jamais, d'être unis et de porter nos valeurs en matière de protection des données d'une seule voix. L'Union européenne doit demeurer pilote. Elle se doit de bâtir un modèle de gouvernance assurant à la fois une meilleure protection à ses citoyens, représentant un atout compétitif pour les entreprises et une coopération plus performante entre autorités. Il en va de sa crédibilité au plan international et auprès des citoyens de l'Union européenne.

2014 a été **une année riche en développements normatifs et politiques** pour le G29. En effet, le G29 a publié une série d'analyses et de prises de position importantes sur un grand nombre de sujets clés tels que le futur règlement, la révision de la Convention 108, le droit à l'oubli, le Safe Harbor, le Big Data, l'Internet des ▸▸▸

INFOS +

Le G29 (groupe des « CNIL » européennes)

En 2014, le G29, c'est :
42 documents adoptés,
8 groupes de travail, 5 plénières regroupant les 29 autorités de protection des données de l'Union Européenne.
Le G29 a collaboré à l'adoption de plusieurs documents clés sur le futur règlement européen, la révision de la Convention 108, le droit à l'oubli, la surveillance généralisée et les mécanismes de transferts.
Le G29 s'est également prononcé sur plusieurs thématiques importantes telles l'internet des objets, le « fingerprinting », les standards OCDE en matière financière, le Big Data, l'Internet des objets, les politiques de vie privée de certains grands acteurs de l'Internet et les concepts d'intérêt légitime et de nécessité dans le secteur public.

objets, les politiques de vie privée de certains grands acteurs de l'Internet, les concepts de nécessité et d'intérêt légitime et l'interopérabilité en matière de transferts avec l'adoption d'un référentiel commun APEC-G29.

Par ailleurs, l'existence de programmes de surveillance de masse, telle que révélée par Edward Snowden a été un sujet largement débattu par les délégations du G29, avec plusieurs avis techniques et une déclaration politique importante sur ce sujet. Il y est rappelé que la surveillance généralisée, secrète et indiscriminée est inacceptable dans un État de droit. ■

LE SUIVI DES RÉFORMES RÉGLEMENTAIRES EUROPÉENNES

Le projet de Règlement

2014 a été marquée par un accord politique important au **Parlement Européen** : le vote à l'unanimité des amendements proposés au projet de la Commission européenne et ce dans un contexte mouvant de renouvellement des législatures à la fois à la Commission Européenne et au Parlement européen.

De son côté, le **Conseil de l'UE** a vu le rythme de ses travaux s'accélérer sous l'égide de la présidence grecque puis italienne.

Malgré quelques réticences, cette nouvelle dynamique a permis des avancées notables.

Ainsi, les Conseils des ministres de l'UE de juin, d'octobre puis celui de décembre, ont permis l'obtention d'un accord général partiel sur les points suivants :

- Le champ d'application territoriale du Règlement ;
- Le chapitre relatif aux transferts (Chapitre V) avec l'introduction de nouveaux outils d'encadrement des transferts (codes de conduite et mécanismes de certification« approuvés ») ;
- Le chapitre relatif aux obligations des responsables de traitement et des sous-traitants (chapitre IV) avec une approche par les risques comme outil de modulation des obligations applicables aux responsables de traitement et aux sous-traitants ;
- Les dispositions relatives au secteur public.

Lors du Conseil des ministres de Décembre 2014 la majorité des Etats membres ont également approuvé les éléments constitutifs du guichet unique et notamment les suivants :

- L'autorité et le juge national restent compétents pour les cas locaux ;
- Pour les cas transfrontaliers, une coordination entre l'autorité chef de file et les autres autorités de protection concernées est nécessaire ;
- Le groupe des CNIL européennes – l'EDPB (futur G29) – dispose de la personnalité morale et de la possibilité d'adopter des décisions contraignantes.

La CNIL a réitéré l'impératif de voir le projet de Règlement adopté en 2015. En effet, une telle adoption apparait désormais cruciale pour les citoyens, les entreprises mais également pour les autorités de protection afin d'assurer et de garantir un haut niveau de protection pour tous.

La CNIL a également contribué activement à l'élaboration de plusieurs documents en lien avec l'avancée des travaux communautaires, notamment sur les éléments clés du Guichet unique, les transferts et l'approche basée sur les risques.

L'approche basée sur les risques est effet un concept clé du projet de Règlement.

Le G29 a estimé que si une telle approche pouvait justifier une modulation dans la mise en œuvre des outils de conformité/obligations du responsable de traitement ou du sous-traitant, notamment en termes de sécurité(ex : analyses d'impact, système de notification des failles de sécurité), elle ne pouvait en aucun cas remettre en cause les droits des citoyens (ex : droit d'accès, rectification, effacement, etc.), lesquels constituent des droits fondamentaux non modulables.

Par ailleurs, le G29 a également considéré que l'utilisation de pseudonymes ou données pseudonymisées, afin de limiter les risques, était insuffisante en elle-même pour justifier un régime allégé concernant les obligations des responsables de traitement et des sous-traitants. Ces données demeurent en effet des données personnelles, et doivent bénéficier du régime de protection applicable à toutes les données.

La 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 Conseil de l'Europe (dite « Convention 108 ») du 28 janvier 1981 et son Protocole additionnel furent le premier instrument juridique européen contraignant en matière de protection des données.

Le Comité des Ministres du Conseil de l'Europe a décidé en 2010 la moder-

nisation de la Convention 108, afin de l'adapter aux évolutions technologiques actuelles, d'y inclure éventuellement de nouveaux principes et de pallier certaines lacunes, avec un souci d'assurer une cohérence avec les textes adoptés par l'OCDE et par l'ONU, ainsi qu'avec le projet de règlement européen.

Les travaux de révision ont débuté en 2011 au sein du Comité consultatif de la Convention 108 (dit « T-PD »), lequel a adopté un projet de texte le 30 novembre 2012 qui a été transmis à un comité intergouvernemental ad hoc pour la révision de la Convention 108 (CAHDATA).

Le CAHDATA a approuvé le texte lors de sa 3ème réunion du 1er au 3 décembre 2014. Toutefois la Commission européenne a dû maintenir sur ce texte un certain nombre de réserves de fond. En effet, au-delà de la question de la cohérence avec le règlement européen en gestation, l'adhésion de l'UE à la Convention 108 ferait prévaloir celle-ci sur le futur règlement en tant que droit primaire de l'UE.

Un projet de Protocole d'amendement de la Convention 108 sera transmis, avec une nouvelle version de projet de rapport explicatif clarifiant les points soulevés par la Commission européenne, au Comité des Ministres pour examen et devrait être soumis pour adoption dans le courant du premier semestre 2015.

Le G29 et les autorités européennes de la conférence de printemps ont réitéré, en juin 2014, la nécessité de maintenir un haut niveau de protection en Europe. À cet effet, elles ont adopté une résolution appelant les États parties à la Convention 108 à préserver le niveau actuel de protection des données et dans la mesure du possible à le renforcer. Parmi les propositions concrètes formulées dans la résolution se trouvent le besoin de maintenir un champ d'application large de la Convention (secteur public et secteur privé), de limiter les dérogations, ou encore d'améliorer le droit des personnes concernées (accès, rectification, suppression, etc.). ■

L'ACCÈS PAR LES AUTORITÉS PUBLIQUES AUX DONNÉES PROTÉGÉES PAR LE DROIT DE L'UNION EUROPÉENNE

La surveillance de masse par les autorités publiques

Plusieurs gouvernements dans le monde se sont dotés de législations de portée extraterritoriale visant à permettre à leurs services de renseignements d'accéder hors de leur territoire national à des informations et données personnelles relatives, notamment, à des résidents de l'Union européenne. 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.

Consécutivement aux révélations d'Edward Snowden sur les programmes de surveillance électronique de masse des États-Unis, le G29 a adopté en avril 2014 un avis sur la problématique de la surveillance de masse. Il rappelle que 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 Gautorités publiques étrangères de garantir un tel niveau de protection. Par conséquent, les 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. **Pour ces raisons, le G29 prône la négociation d'un accord international propre à garantir que les agences de renseignement du pays tiers offrent un niveau de protection adéquat.**

Une analyse juridique plus précise du G29 a été adoptée et rendue publique sous la forme d'un document de travail le 5 décembre 2014.

La convention du Conseil de l'Europe sur la cybercriminalité

La Convention sur la Cybercriminalité, dite Convention de Budapest, est un traité international rédigé par le Conseil de l'Europe et adopté le 23 novembre 2001. Son objectif est d'harmoniser les droits nationaux et de créer une coopération internationale afin de lutter contre la criminalité dans le cyberespace.

La négociation d'un protocole additionnel à la convention est actuellement en discussion. Ce protocole permettrait notamment de faciliter l'accès transfrontière aux données. Compte tenu des conséquences importantes que de tels accès pourraient impliquer, le G29 échange activement avec le comité du Conseil de l'Europe en charge de cette convention afin que ce dernier prenne en compte l'ensemble des principes de protection des données lors de la rédaction du protocole. ■

INFOS +

Le Safe Harbor

La « Sphère de sécurité » ou « Safe Harbour » renvoie à un ensemble de principes de protection des données personnelles, négociés entre la Commission européenne et le Département du commerce américain et adoptés en juillet 2000. Le « Safe Harbour » permet d'apporter un niveau de protection adéquat aux données transférées vers des entreprises américaines s'étant engagées à respecter ces principes.

VERS UN ENCADREMENT PLUS EFFICACE ET COHÉRENT DES TRANSFERTS DE DONNÉES EN DEHORS DE L'UNION EUROPÉENNE

Négociations entre le Commission européenne et les autorités américaines sur la décision « Safe Harbour »

Depuis quelques années, le « Safe Harbour » fait l'objet de certaines interrogations quant à son efficacité. Les critiques portent principalement sur le niveau de protection, la lisibilité des documents « Safe Harbour », le contrôle de la mise en œuvre, l'accessibilité et l'efficacité des voies de recours. À la suite des révélations de juin 2013 sur les programmes de surveillance aux États-Unis, la Commission européenne a reçu un mandat pour renégocier la décision « Safe Harbour » avec les autorités américaines. L'objectif de ces négociations est de restaurer la confiance dans les flux transfrontières entre l'Union européenne et les États-Unis en renforçant les garanties apportées par le « Safe Harbour ». Dans cette optique, **la Commission a fixé 13 recommandations autour de 4 grandes thématiques : la transparence, les voies de recours, les contrôles et l'accès par les autorités américaines**. Très vigilant sur ces questions et sur le déroulement des discussions entre la Commission et les autorités américaines, le G29 s'est également saisi de cette problématique et, par lettre du 10 avril 2014 à la Commission européenne, a formulé des recommandations complémentaires.

Poursuite des travaux du G29 et de l'APEC pour la création d'un lien entre BCR et CBPR

Fruit d'un travail de coopération inédit entre le G29 et l'APEC, forums rassemblant près d'une cinquantaine de pays, le référentiel regroupant les exigences relatives aux BCR et aux CBPR (WP212) a été adopté en février 2014. Les deux forums ont concentré leurs efforts sur les similitudes entre les deux systèmes avec pour objectif commun d'aider les multinationales souhaitant se conformer aux exigences des BCR et des CBPR via une politique de vie privée mondiale, et ainsi obtenir une double certification.

À la suite de cette adoption, le G29 et l'APEC ont décidé de poursuivre leurs travaux au moyen de cas pratiques, basés sur l'expérience d'entreprises volontaires qui visent à la fois l'approbation de leurs BCR par les autorités européennes de protection des données et la certification de leurs CBPR par les tiers certificateurs agréés par l'APEC. ■

> L'adoption de ce référentiel BCR/CBPR est un acte politique et symbolique fort.

LA COOPÉRATION INTERNATIONALE ET EUROPÉENNE

Les technologies évoluent également constamment depuis déjà plusieurs années et la mondialisation ancre les enjeux informatique et libertés sur la scène internationale. C'est pourquoi la question de la coopération internationale et européenne apparait comme un sujet particulièrement stratégique et d'ampleur croissante, qui nécessite un investissement dans toutes les initiatives qui se développent. Cette coopération s'effectue au sein de plusieurs forums dont la Conférence Internationale, la Conférence de Printemps, ou encore dans des forums plus spécifiques tel que l'Association Francophone des Autorités de Protection des Données (AFAPDP).

La 36ème Conférence Internationale

La Conférence Internationale des autorités de protection des données est l'un des rendez-vous les plus importants pour la communauté de la protection des données. Cette année plus de 80 autorités ont participé à la 36ème conférence internationale qui se tenait à l'île Maurice. La session fermée a permis d'échanger plus particulièrement sur les problématiques liées à l'internet des objets. Plusieurs documents ont également été adoptés :

- Une **déclaration sur l'internet des objets** : la déclaration rappelle les défis que pose l'internet des objets en termes de protection des données et de sécurité, en particulier dans le contexte du « *big data* ». La protection des données commence dès la collecte. C'est pourquoi les concepts de « *privacy by design* » et « *privacy by default* » doivent être considérés comme centraux lors de la conception de nouvelles technologies.
- Une **résolution sur la coopération internationale en matière de contrôle et d'enquête** : cette résolution a pour objet principal d'adopter **un cadre mondial non-contraignant en matière de coopération transfrontière et d'appeler au développement d'une plateforme sécurisée et neutre d'échanges d'informations pour les membres de la conférence internationale**. Cette initiative vise à renforcer la coopération transfrontière entre membres de la Conférence internationale puis à élargir cette collaboration, dans la limite des lois nationales applicables, à d'autres autorités en charge du contrôle de l'application des lois en matière de vie privée.
- Une **résolution sur le « big data »** : cette résolution appelle tous les acteurs du « big data » à respecter les principes de protection des données tels que la limitation des finalités, la proportionnalité de la collecte et de la conservation, la transparence, et le respect des droits des personnes (accès, rectification, information).
- Une **résolution sur la protection de la vie privée à l'ère du numérique** : elle donne mandat au comité exécutif de la Conférence internationale pour participer à la discussion multipartites sur la protection de la vie privée à l'ère du numérique annoncée par le Haut Commissaire au droits de l'homme des Nations unies dans son rapport « Le droit à la vie privée à l'ère du numérique ».

Par ailleurs, à l'issue de cette session, Isabelle Falque-Pierrotin, Présidente de la CNIL et du G29, a été élue au comité exécutif de la Conférence internationale.

La coopération européenne au sein de la Conférence de Printemps

En Europe, et au-delà de la coopération entre autorités de l'UE au sein du G29, la Conférence européenne des autorités de protection des données constitue un forum de coopération privilégié pour les autorités européennes au sens large.

Lors de la dernière édition, organisée par les CNIL et le Conseil de l'Europe, un groupe de travail, co-présidé par le Conseil de l'Europe et la CNIL, a été crée avec pour objectif d'améliorer la coopération européenne, notamment au moyen d'une plateforme collaborative. Il s'agit d'étendre la coopération européenne au-delà de l'UE et d'inclure les autres membres du Conseil de l'Europe, au sein d'un outil fonctionnel et pratique permettant de favoriser l'échange d'information.

FOCUS

THE EUROPEAN DATA GOVERNANCE FORUM
UNESCO-PARIS 8 DÉCEMBRE 2014 / 8 DECEMBER 2014

European Data Governance Forum

Le G29 a organisé une conférence internationale à l'UNESCO, à Paris le 8 décembre 2014, intitulée Protection des données, innovation et surveillance : quel cadre éthique européen ? La conférence a réuni, au travers de quatre sessions, des représentants et experts d'horizons divers – institutions nationales, européennes et internationales, industrie, ONG et société civile. Ils ont présenté leur point de vue sur les défis actuels de la surveillance numérique et sur la manière d'y répondre de manière adéquate dans une société démocratique. Le Premier ministre Manuel Valls a inauguré cette conférence à laquelle 350 personnes ont participé.
La conférence s'est achevée par la présentation d'une Déclaration adoptée par le G29 lors de sa séance plénière du 25 novembre 2014. Les autorités de l'Union européenne souhaitent réaffirmer les valeurs communes de l'Europe et proposer des actions concrètes pour élaborer un cadre éthique européen. Cette Déclaration souligne la responsabilité collective de toutes les parties prenantes dans la définition et le respect d'un cadre éthique pour la collecte et l'utilisation de données personnelles dans l'économie numérique. La déclaration est ouverte aux commentaires de toutes les parties intéressées.

L'AFAPDP

En 2014, sept ans après sa création, l'Association francophone des autorités de protection des données personnelles (AFAPDP), dont la CNIL assure le secrétariat général, compte 16 membres dont désormais la moitié est issue du continent africain. En Afrique se trouve la **progression du droit la plus importante** avec de nouvelles lois adoptées récemment en Côte d'Ivoire, à Madagascar et au Mali, et plusieurs projets de loi en préparation.

En parallèle de cette dynamique législative soutenue par l'AFAPDP, plusieurs expériences de coopération ont été menées en 2014 : mise en œuvre des **règles contraignantes d'entreprise francophones (RCEF)** qui permet un rapprochement avec les pratiques de l'Union européenne en matière d'encadrement des transferts internationaux de données ; participation coordonnée des autorités francophones à la **Conférence internationale** des commissaires à la protection des données à Maurice en octobre 2014 pour faire entendre la voix francophone en matière de protection des données personnelles ; publication par trois réseaux institutionnels francophones dont l'AFAPDP d'un **guide pratique** qui propose des solutions concrètes pour la consolidation des fichiers d'état civil et électoraux et pour la protection des données personnelles.

À partir de ces expériences et dès 2015, l'AFAPDP sera amenée à développer le nombre de ses membres et les expériences de coopération de son réseau, et à prendre une part active aux débats au sein de la Francophonie et de la communauté internationale des autorités de protection des données. ■

3. LES SUJETS DE RÉFLEXION EN 2015

Pour qui les véhicules connectés roulent-ils ?

La ville intelligente à votre service

La place des données personnelles dans la consommation de contenus culturels et ludiques

Les nouvelles frontières de l'identité numérique

Vers un encadrement des dispositifs de caméras mobiles

POUR QUI LES VÉHICULES CONNECTÉS ROULENT-ILS ?

Consciente des enjeux stratégiques attachés au développement du véhicule connecté, la CNIL souhaite accompagner en 2015 cette dynamique et apporter son expertise à l'écosystème afin de construire des innovations durables et respectueuses de l'utilisateur. Elle anime ainsi une réflexion collective qui associe les multiples créateurs du véhicule connecté et qui vise la co-construction d'outils de conformité adaptés.

UN ÉCOSYSTÈME EN MOUVEMENT

Le véhicule connecté est un enjeu stratégique majeur pour les constructeurs automobiles et pour d'autres acteurs parfois issus de secteurs très éloignés de l'industrie automobile traditionnelle. Les géants technologiques comme Google ou Apple, les équipementiers, les opérateurs de transports, les assureurs, les start-ups, les acteurs publics, tous contribuent à la création de nouvelles mobilités porteuses d'usages ou de services inédits et créatrices de nouvelles données.

Les nouveaux entrants, globalement issus des écosystèmes numériques, apportent des cultures de l'innovation différentes : l'automobile n'échappe pas au développement du logiciel. Les voitures deviennent ainsi de véritables smartphones sur roues, et pas uniquement parce qu'elles facilitent l'intégration des smartphones aux habitacles. Entre API (interfaces de programmation) et OS (systèmes d'exploitation) dédiés, les logiques propres aux entreprises technologiques s'immiscent progressivement dans l'industrie automobile. ■

> En 2018, 420 millions d'automobiles seront connectées, contre 45 millions en 2013.
>
> Source : IDATE, Connected Cars, April 2014

DERNIÈRE MINUTE

La CNIL à l'écoute

La CNIL a organisé le 7 janvier la première rencontre de l'ensemble de l'écosystème français du véhicule connecté. En partenariat avec les animateurs du plan « Big data » du programme « Nouvelle France Industrielle », ce rassemblement était l'occasion pour les différents acteurs d'explorer ce nouveau territoire, voué à produire et consommer de grandes quantités de données. Étaient réunis à cette occasion : des constructeurs, des opérateurs de transport, des assurances, des start-ups, des représentants des pouvoirs publics et des porteurs de projet dans le domaine de la mobilité.

> Les revenus issus de la connexion des véhicules devraient excéder 8,2 milliards d'euros en 2018, contre 477 millions en 2013.
>
> Source : IDATE, Connected Cars, April 2014

DE NOUVEAUX USAGES DE LA MOBILITÉ

Friands des nouveaux modes de consommation du véhicule, notamment propres à l'économie collaborative, les usagers de la mobilité sont également à l'origine de changements majeurs pour l'industrie automobile : covoiturage, location entre particuliers, « jonglage » entre différents moyens de transport. Ces nouveaux usages produisent des traces numériques, qui suivent la personne dans ses déplacements et alimentent les mécanismes de confiance des services de mobilité à travers la création de profils utilisateurs de plus en plus complets.

Les logiques d'optimisation de l'usage du véhicule intéressent également le monde de l'assurance, qui cherche à proposer des offres au plus près des usages effectifs du véhicule. Après la prise en compte du kilométrage dans la tarification des primes d'assurance (le Pay As You Drive), de nouvelles données issues de l'habitacle permettent maintenant de penser un ajustement de la prime d'assurance en fonction du comportement du conducteur (le Pay how you Drive). Conduite « sportive », freinage brutal, les habitudes de conduite des usagers de la route pourraient bientôt ne plus avoir de secret pour les assureurs et les constructeurs, constituant certains à préconiser une logique assurantielle au plus près des usages du conducteur.

Enfin, les traces de mobilité anonymisées sont particulièrement utiles pour une planification efficace des politiques publiques. Au-delà du symbole du véhicule connecté, c'est donc l'idée même de la mobilité qui se trouve en pleine mutation. ■

INFOS +

Un véhicule de plus en plus autonome : de la voiture connectée à la robotisation de la mobilité

Les images impressionnantes de tests de voitures autonomes se déplaçant sans action du conducteur ne doivent pas faire oublier que l'autonomisation des voitures vis-à-vis de leur conducteur est un processus déjà largement enclenché. Radars intégrés, conseils personnalisés, voire assistance à la conduite : beaucoup de conducteurs partagent d'ores et déjà une part de leur conduite avec leur voiture. Jusqu'où cette délégation pourra-t-elle aller ? L'ajout de nouveaux capteurs et capacités de traitement de données permettent de passer progressivement des paliers d'autonomie à travers les systèmes avancés d'aide à la conduite. A chaque étape de ce processus vers la voiture autonome, des nouvelles questions d'éthique et de responsabilité se poseront, notamment en lien avec l'automatisation de la prise de décision. A cet égard, plus une voiture sera autonome, plus elle sera en réalité dépendante d'informations contextuelles et souvent personnelles.

LA VILLE INTELLIGENTE À VOTRE SERVICE

Smart city, smart grid, smart citizen, etc. Le «smart» semble avoir envahi nos villes et nos vies, mais de quoi s'agit-il exactement et quel rôle le citoyen peut-il y jouer ?

La ville intelligente traduit avant tout un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. La « smart city » recouvre ainsi un ensemble de promesses de réponses à la complexité urbaine[1] renvoyant à un idéal de contrôle qui serait rendu possible par les données.

Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment :

1. **les infrastructures publiques (bâtiments, mobiliers urbains, domotique…) ;**
2. **les réseaux (eau, électricité, gaz, télécoms) ;**
3. **les transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied…) ;**
4. **les e-services et e-administrations.**

Ces différentes réalités de la « ville intelligente » montrent d'ailleurs l'ambigüité de la formule. Dans certains cas, elle semble faire référence à la connectivité ubiquitaire et à l' « *internet of everything* ». Elle aurait alors finalement peu à voir avec les enjeux spécifiquement urbains. Dans d'autres, elle semble plutôt promouvoir une vision prospective de la ville, résolument transformée par des systèmes gestionnaires intelligents et omniprésents.

Avec la ville intelligente, de nouveaux imaginaires émergent à travers des projets favorisant une distribution des données auprès de multiples acteurs de la ville : entreprises, pouvoirs publics, société civile et habitants ou usagers de la ville. Les données sont alors coproduites par les différents acteurs, en particulier par les individus qui contribuent à créer des traces numériques. ■

COMMENT LES DONNÉES SERONT-ELLES PRODUITES OU ÉCHANGÉES ?

À la lumière des applications mises en œuvre ou envisagées, il est possible de catégoriser les différents projets selon la manière dont les données vont être produites et échangées. Elles peuvent notamment être :

- **mises à disposition** à travers des informations ouvertes et disponibles à tous, qu'il s'agisse de plateformes open data, d'alertes à la population concernant des catastrophes naturelles ou la pollution, ou de routes communicantes pour les feux rouges et les arrêts de bus ;
- **transmises de manière ciblée,** par exemple entre deux voitures, entre deux individus, entre un usager et une infrastructure ;
- **diffusées de manière restreinte, uniquement en mode unipersonnel,** par exemple via des bracelets de mesure de l'exposition à la pollution, la lecture d'informations contenues dans une puce RFID (ex. : pour le m-tourisme), ou la mesure des temps de trajet personnel ;
- enrichies sur **un mode participatif** à travers la remontée des informations individuelles vers une plate-forme collective, par exemple pour le comptage de flux de personnes, le suivi de personnes (tourisme), ou le suivi de l'utilisation de transports publics (RATP, Vélib, Autolib) ;
- enfin, diffusées largement, en **mode réseau social,** avec un niveau de visibilité paramétrable, comme pour le covoiturage ou la garde d'enfants.

En conséquence, la ville intelligente ne peut se réduire à une série de problèmes qui attendent d'être résolus par le *smart*, la supervision et le *big data* : le véritable enjeu consiste à inventer une gouvernance démocratique et citoyenne adaptée à une ville « mise en données ». ■

> Le véritable enjeu consiste à inventer une gouvernance démocratique et citoyenne adaptée à une ville « mise en données ».

[1] *Dans une certaine mesure, les considérations sur les smart cities peuvent être étendues à d'autres types de territoires que les villes, telles que les zones rurales, notamment pour le télétravail.*

QUELS ENJEUX EN TERMES DE VIE PRIVÉE ?

Du point de vue de la loi informatique et libertés, la ville intelligente englobe tous les traitements de données à caractère personnel liés, directement ou indirectement, à l'espace public en zone urbanisée. Il peut notamment s'agir des voies publiques en surface (routes, rues, trottoirs), des infrastructures publiques souterraines (réseaux), des infrastructures publiques aériennes (éclairage public, capteurs de pollution, drones etc.) ainsi que des bâtiments publics (hôpitaux, mairies, bibliothèques, musées…). La CNIL se penche donc particulièrement sur :

- les conditions de production et diffusion de l'information ;
- le contrôle et les possibilités de maîtrise par les individus ;
- les modalités de partage et de réutilisation des données.

Certains risques sur la vie privée sont assez similaires à ceux déjà rencontrés sur les réseaux sociaux (échanges de données entre particuliers), ou encore avec les objets connectés (domotique).

Mais le développement des smart cities va soulever des questions nouvelles, relatives à l'information et, le cas échéant, au consentement des personnes dont les données sont collectées. La possibilité que les infrastructures transmettent des informations en permanence ne représente pas un risque en soi. En revanche, le « ciblage » individuel des données collectées sur les passants par cette même infrastructure soulève plus de questions, notamment quant aux modalités de cette collecte et d'anonymisation des données personnelles. L'anonymat apparaît ainsi plus difficile à garantir pour certaines données, comme celles attachées à une position géographique.

À l'heure où la ville, espace dense, se dote de capteurs et d'une mémoire, le risque de traçabilité des individus est démultiplié. L'adhésion des citoyens dépend donc du cadre de confiance dans lequel le développement de la ville intelligente doit s'inscrire. ■

QUEL RÔLE POUR LA CNIL ?

L'objectif de la CNIL est d'accompagner un développement responsable et durable, qui sera la clé de voûte de l'acceptation sociale des *smart cities*. En particulier, la CNIL met l'accent sur l'accompagnement des responsables de traitements dès la conception (*privacy by design*) et la mise en œuvre des infrastructures et des services numériques.

Dans différents domaines d'activité, la CNIL a déjà proposé des mesures pour garantir l'anonymat des personnes lorsque leurs données sont collectées sans leur consentement. Elle a ainsi accompagné dans leur choix de solutions d'anonymisation[2] des opérateurs de télécommunications, des gestionnaires d'infrastructures de transport ou encore d'énergie. L'anonymisation permet alors à ces acteurs de proposer dans le cadre d'offres de type « big data », des produits et services basés sur des cartes représentant des flux agrégés de personnes dans des lieux touristiques ou l'affluence à des événements, d'analyser des zones de chalandise, de prédire des pics de consommation ou des congestions (ex. : réseau routier), etc. De multiples enjeux seront donc explorés en 2015 : comment les citoyens pourront-ils identifier les acteurs (collecte, autres traitements) afin de pouvoir exercer leurs droits ? Comment seront-ils informés ? Comment leur consentement sera-t-il recueilli de manière éclairée ? Comment concevoir des services respectueux de la loi Informatique et libertés ? Comment s'engager dans une démarche de « *privacy by design* » et mener des PIA (*Privacy Impact Assessment*) ? Comment les municipalités, devenues gestionnaires de ressources intégrées et interconnectées telles de véritables « villes-ordinateurs », pourront-elles se prémunir d'éventuels virus, piratages voire bugs ? ■

> Un développement responsable et durable sera la clé de voûte de l'acceptation sociale des *smart cities*.

[2] *Voir l'avis G29 sur les techniques d'anonymisation http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf*

LA PLACE DES DONNÉES PERSONNELLES DANS LA CONSOMMATION DE CONTENUS CULTURELS ET LUDIQUES

Les données, en particulier personnelles, sont souvent qualifiées de « pétrole » de la transformation numérique. Mais quelle est réellement la place de ces données dans les offres de services et dans les modèles économiques ? Pour répondre à cette question, la CNIL a lancé à l'automne 2014 un chantier d'exploration prospective autour du marché des contenus culturels et ludiques (lecture, musique, vidéo, jeu vidéo). Ce travail alimentera un 3ème cahier « Innovation et Prospective » en 2015.

Les modèles économiques du marché des contenus culturels ou ludiques ont déjà connu plusieurs bouleversements majeurs liés aux questions de financement de la création, de préservation de la diversité culturelle, de partage de la valeur ajoutée entre les acteurs, de propriété intellectuelle et de piratage.

Si, parmi ces enjeux, les questions de protection des données personnelles et de la vie privée étaient initialement peu présentes, la situation est en train de changer. La CNIL a donc souhaité étudier la numérisation des contenus culturels produits, distribués, consommés et en particulier l'impact de ce mouvement sur la capacité à « enrichir en données personnelles » les modèles d'affaires de ce secteur.

En effet, la véritable plus-value des services émergents de distribution de contenus numériques culturels et ludiques se concentre aujourd'hui sur leur capacité à traiter les données de consommation et d'habitude des utilisateurs afin de les accompagner.

Les services se trouvent alors dans une position privilégiée pour cibler les individus et leur proposer des recommandations pertinentes en cumulant plusieurs types d'informations :

- des informations personnelles « classiques » (profilage sociodémographique) ;
- des informations de consommations et d'achats, donc des données concernant leurs goûts ;
- des informations concernant la consommation en elle-même, telles que la quantité ou les moments auxquels le contenu est consommé, mais potentiellement bien plus, comme par exemple, encore ; par exemple sur un livre, il peut s'agir des passages surlignés, de la vitesse de lecture, ou du nombre de fois que le livre a été consulté ;
- des données descriptives des contenus, à l'exemple d'IMdb, propriété d'Amazon pour le cinéma, ou des milliers de genres et sous-genres décrivant les films sur Netflix ;
- des données contextuelles, par exemple la localisation, pour en déduire si la personne consomme à domicile, pendant les transports, ou au travail.

À travers ces possibilités, la collecte de données et la recommandation personnalisée deviennent des enjeux majeurs de différenciation concurrentielle. ■

LES ENTREPRISES CULTURELLES ET DE LOISIRS EN PLEINE TRANSFORMATION

Qu'il s'agisse du livre numérique, de la musique en streaming, de la vidéo à la demande, ou encore des jeux vidéo sur des plateformes en ligne, des « nouveaux entrants » ont bouleversé les équilibres de marché dans chaque domaine, faisant tomber les barrières à l'entrée qui protégeaient les acteurs traditionnels.

Les liseuses permettent ainsi de collecter un grand nombre d'informations lors de l'utilisation de l'appareil et de la lecture des ouvrages électroniques, à des degrés et avec des portées différents[1]. Par exemple, certains éditeurs pourraient mettre en avant sur des publicités, les passages le plus souvent surlignés ou sauvegardés. Le

[1] *Voir Electronic Frontier Foundation, E-Reader Privacy Chart, 2012 Edition : https://www.eff.org/pages/reader-privacy-chart-2012*

Wall Street Journal avait décrit ce paysage dès 2012 : « un lecteur moyen met juste 7 heures pour lire le livre final de la trilogie *Hunger Games* de Suzanne Collin sur la liseuse Kobo, soit à peu près 57 pages par heure. Environ 18 000 lecteurs sur Kindle ont surligné la même ligne du deuxième livre de la série (…) et sur le Nook de Barnes & Noble, la première chose que font la plupart des lecteurs dès qu'ils ont achevé le premier tome de *Hunger Games* est de télécharger le suivant. »

Côté vidéo à la demande, l'exemple Netflix est tout aussi parlant dans la mesure où l'entreprise a affirmé elle-même que 75 % de ce qui est visionné par ses clients vient d'une recommandation personnalisée de son moteur[3].

La donnée permet ainsi au diffuseur de tenir la main du consommateur dans ses pérégrinations au cœur d'une offre foisonnante, afin d'assurer un taux d'utilisation important du service et donc de réduire l'attrition des abonnements (le « *Churn* »). Mais ces informations peuvent également être valorisées pour faire des choix éditoriaux informés sur les programmes que l'entreprise produit.

Concernant la musique, la situation est similaire. Des services comme Rdio, Deezer ou Spotify sont en mesure de faire des recommandations de plus en plus pertinentes à partir d'un ensemble de données sur les morceaux, croisées avec les données de consommation et les données de réseaux sociaux. Ces acteurs souhaitent maintenant tirer parti de toutes ces informations pour

> Selon Netflix, 75 % des programmes visionnés par ses clients seraient issus d'une recommandation personnalisée de son moteur.

les partager avec des tiers d'une manière agrégée et aider les producteurs à faire de la musique « qui plaît »[4]. Demain, ces services utiliseront probablement aussi des données de géolocalisation ou d'autres capteurs du smartphone pour deviner si l'utilisateur est au travail, en voiture, à une soirée et lui fournir ainsi des recommandations améliorées en fonction du contexte.

Enfin, le domaine du jeu vidéo n'échappe pas à cette tendance. Sans même parler du jeu sur smartphone, par nature connecté et très gourmand en données[5]. Le fait que les joueurs (aussi bien sur console que sur ordinateur) soient dorénavant connectés sur des plateformes comme Steam, permet la collecte d'informations pendant que le client joue. Ces données sont pour le moment encore limitées à de l'analyse d'usage et de la recommandation, mais demain, de véritables tests de comportement à l'intérieur même de jeux pourraient voir le jour, afin d'analyser et mesurer les réactions de la personne[6].

Jusqu'où ira l'accroissement de l'utilisation des données personnelles dans ces marchés ? Quelles autres valorisations des données personnelles pourraient apparaître ? ■

UNE EXPLORATION INNOVANTE QUI SERA PRÉSENTÉE DANS UN CAHIER « INNOVATION ET PROSPECTIVE » NUMÉRO 3

Depuis l'automne 2014, la CNIL a donc choisi d'explorer ces nouveaux enjeux.

Accompagnée par deux agences d'innovation, elle a animé une démarche collaborative spécifiquement orientée vers des acteurs émergents, qui participent à transformer ces industries. Les travaux vont se poursuivre et aboutiront, au cours du premier semestre 2015, à la publication d'un troisième cahier « Innovation et Prospective (IP), qui succédera aux cahiers IP « le Corps, nouvel objet connecté » et « Vie Privée à l'horizon 2020 »[7]. ■

INFOS +

Deux agences d'innovation en accompagnement de la CNIL

Pour accompagner cette démarche innovante et sortir des sentiers battus, l'équipe d'innovation et prospective de la CNIL a fait appel à deux agences d'innovation. Ce choix marque la volonté de travailler en bonne intelligence avec les écosystèmes d'innovation, en particulier français. *Five by Five* est une task force d'innovation qui fait bouger les lignes des grandes organisations, en agissant sur deux fronts : l'ouverture et l'intrapreneuriat. *We design services* invente le futur de l'innovation et du design de services par l'accompagnement des organisations, en France et à l'international.

Crédit : Five by Five

[2] *ALTER, Alexandra, "Your E-Book Is Reading You" in Wall Street Journal, 19 juillet 2012* http://www.wsj.com/news/articles/SB10001424052702304870304577490950051438304
[3] http://www.techradar.com/us/news/internet/how-spotify-netflix-and-amazon-s-powerful-discovery-tools-control-our-habits-1216211
[4] http://www.theguardian.com/technology/2014/apr/09/music-analytics-is-helping-the-music-industry-see-into-the-future
[5] *Comme le montrent les résultats du projet CNIL-Inria « Mobilitics » [voir chapitre correspondant]*
[6] http://abonnes.lemonde.fr/technologies/article/2012/03/13/la-science-des-jeux-sociaux_1666663_651865.html
[7] *Tous deux téléchargeables sur la page :* http://www.cnil.fr/linstitution/ip/publications/

LES NOUVELLES FRONTIÈRES DE L'IDENTITÉ NUMÉRIQUE

La transition numérique de l'économie s'accompagne d'une disparition progressive des frontières entre les univers des transactions physiques et en ligne. Aux banques et opérateurs télécoms, acteurs traditionnels du monde du paiement, s'ajoutent désormais de nouveaux intermédiaires issus du monde numérique, qui cherchent à relier leurs solutions de paiement aux identités numériques de leurs utilisateurs. Dans ce contexte, la CNIL accompagne la politique volontariste de l'Etat en matière d'identité numérique dans le cadre de la mise en œuvre progressive du nouveau règlement européen sur l'identification électronique et les services de confiance.

L'IDENTITÉ NUMÉRIQUE, CLÉ DE VOÛTE DE NOMBREUSES TRANSACTIONS SUR INTERNET

L'identité numérique se matérialise de différentes manières : identifiant, adresse IP, certificat électronique, adresse email, identité numérique régalienne… Une approche courante consiste à l'appréhender à travers des attributs de l'identité (pseudonyme, identifiant, âge, adresse, centres d'intérêt) permettant de distinguer une personne au sein d'un groupe. Dans le monde numérique, les identités sont multiples et fragmentées : un individu est ainsi amené à gérer différentes identités en fonction des univers dans lesquels il évolue, qu'il s'agisse par exemple des réseaux sociaux, du e-commerce, de la banque en ligne, de la e-administration.

Comme la gestion de multiples identités est particulièrement complexe pour les utilisateurs, des systèmes de fédération d'identités se sont largement développés. Au travers d'une authentification unique, ils permettent essentiellement de simplifier l'accès à des services appartenant à des fournisseurs différents. Certaines sociétés permettent ainsi une connexion à leurs services à l'aide d'un identifiant et mot de passe Facebook.

Toutefois, dans un contexte où l'identité numérique est majoritairement déclarative, la confiance n'est pas toujours au rendez-vous. Certains services requièrent donc des modalités d'identification plus sécurisées pour vérifier, voire garantir, l'identité d'un internaute. C'est par exemple le cas pour l'accès à des sites de jeux de hasard et d'argent en ligne, qui ont pour obligation de s'assurer de l'identité des nouveaux joueurs. Ils doivent en particulier vérifier que la personne est majeure et contrôler la destination des fonds (vérification du compte bancaire) pour prévenir les possibilités de blanchiment.

Il est essentiel de permettre aux personnes de contrôler les attributs qu'elles divulguent. Par exemple, une transaction de e-commerce peut nécessiter de communiquer un nom, prénom et une adresse de livraison, mais la date de naissance n'est en général pas nécessaire. A contrario, l'année de naissance sera pertinente pour l'achat d'une carte de réduction à destination des jeunes de moins de 25 ans.

Ces enjeux deviennent d'autant plus importants dans un environnement qui se numérise, au niveau des habitats, des villes et même du quotidien avec le développement de l'internet des objets. En effet, le commerce en magasin devient lui aussi connecté et les méthodes du e-commerce s'étendent peu à peu à ces espaces. ■

> En 2013, un internaute français disposait en moyenne de 16,4 comptes en ligne – contre 12 en 2010 et 13,6 en 2011.
>
> Source : Baromètre de la confiance numérique des français CDC - ACSEL, réalisé par l'IDATE, février 2013

LE COMMERCE AU CŒUR DE LA FUSION DES MONDES PHYSIQUE ET NUMÉRIQUE

L'étape faisant actuellement l'objet du plus grand nombre d'innovations est celle du paiement. On assiste à une convergence d'acteurs très différents avec d'un côté des spécialistes (*pure players*) qui, se sentant à l'étroit dans l'univers en ligne, descendent la chaîne de valeur, et de l'autre, des intermédiaires traditionnels (banque, enseignes) soucieux de numériser davantage leurs activités. Au milieu, les nouveaux services tels que Google Wallet, Paypal, Apple Pay, V.me ou Square s'appuient sur l'infrastructure bancaire traditionnelle en étant reliés à une carte de paiement. En pratique, ces solutions se matérialisent généralement par des applications mobiles qui intègrent des modes de paiement et des services en lien avec la fidélité en mobilisant l'ensemble des données de la relation commerciale. La fourniture de données par l'utilisateur fait donc partie intégrante du modèle économique.

Plus généralement, l'équipement croissant des utilisateurs en smartphones favorise la disparition des frontières entre commerce électronique et commerce traditionnel. Grâce au développement de technologies tels que le QR code, le NFC, la géolocalisation ou plus récemment les *beacons (cf. encadré)*, les identités numériques sont désormais enrichies en combinant par exemple des recherches sur internet en lien avec des achats et des déplacements physiques en magasin. Les acteurs optimisent ainsi le parcours client, du site internet au magasin, mais aussi à l'intérieur même du magasin en s'appuyant sur des dispositifs d'analyse de fréquentation. ■

> Plus de 60 millions de *beacons* devraient être déployés à l'horizon 2019 – essentiellement destinés à l'univers du commerce.
>
> Source : ABI Research, 2014

FOCUS

Les *beacons*, des cookies dans la vraie vie

Les *beacons* sont de petites balises physiques sans fil, capables de communiquer avec des *smartphones* au travers du protocole Bluetooth. Ils permettent en particulier de pouvoir « réveiller » une application mobile lorsqu'un utilisateur passe à proximité, pour lui indiquer une opération en cours ou lui proposer une réduction. Ces dispositifs rendent les commerces connectés et, parce qu'ils ont une portée limitée, permettent de connaître avec précision le parcours des clients dans le magasin.
Apple a été le premier à les utiliser à grande échelle, depuis fin 2013 dans ses Apple Stores américains. Cette technologie émergente intéresse de plus en plus de grandes enseignes et il devrait y en avoir plus de 60 millions déployés à travers le monde à l'horizon 2019 selon une étude de ABI Research (2014).

LES DONNÉES COMPORTEMENTALES : NOUVEAU FACTEUR D'AUTHENTIFICATION ?

Les parcours clients imaginés autour des beacons et de l'application Paypal témoignent de la mutation à l'œuvre dans les domaines du commerce et de l'identité numérique, visant à fluidifier la phase du paiement en la rendant la plus transparente possible pour l'utilisateur. Ce dernier se voit identifié dès son entrée en magasin au travers de son application mobile, reçoit des suggestions en fonction de son historique de transactions (auquel le commerçant peut accéder) et procède au règlement par un simple clic sans avoir à produire d'autres moyens de paiement.

Traditionnellement, la confiance en l'identité nécessitait la validation d'attributs par des acteurs comme les banques (validation d'une carte bancaire ou d'un compte), les opérateurs téléphoniques ou postaux (validation d'un numéro de téléphone ou d'une adresse) qui ont à la fois besoin de vérifier l'identité de leur client et la capacité technologique ou humaine de le faire (possibilité d'enrôler en face à face).

Mais depuis peu, l'identité en ligne intègre davantage de données comportementales concernant « ce que font » les individus (historique d'achats, de navigation web…). Une nouvelle dimension vient donc s'ajouter aux traditionnels « ce que je sais » (ex : mot de passe), « ce que j'ai » (ex : une carte à puce) et « ce que je suis » (ex : biométrie) qui sont utilisés pour identifier ou authentifier un individu.

Les nouveaux entrants nourrissent de grandes ambitions autour de la valorisation des données de transactions et du profilage, ce qui va nécessairement amener à s'interroger sur les nouveaux modèles économiques et la capacité des individus à exercer leurs droits.

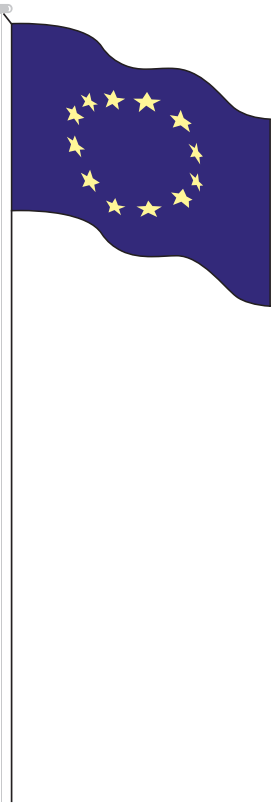
La CNIL anticipe ces changements. Elle analyse leur impact en termes de confiance et de protection des données, pour renforcer son rôle d'acteur majeur de la régulation des plateformes au niveau européen et être ainsi garante d'une innovation responsable.

Pour ces raisons, les mutations à l'œuvre à la croisée du paiement, de l'identité numérique et du commerce, constituent l'un des sujets d'étude prospective qui fera l'objet de publications en 2015. ■

FOCUS

Le règlement européen sur l'identification électronique

Le 23 juillet 2014 a été définitivement adopté le règlement 910/2014/CE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Ce règlement, qui abroge la directive 1999/93/CE sur la signature électronique, a pour objectif d'améliorer la reconnaissance mutuelle des systèmes d'identification électronique nationaux afin de faciliter le développement de services interopérables d'administration en ligne dans toute l'Union européenne.
Il harmonise ainsi la sécurité des services publics en ligne au sein de l'Union européenne.
Le règlement, qui doit être complété par différents actes d'exécution et qui sera applicable à partir du 1er juillet 2016, insiste sur le principe du « *privacy by design* » ou respect de la vie privée dès la conception. Ceci doit passer par :
• la préservation des solutions permettant l'accès au minimum d'informations d'identité nécessaires ;
• la préservation de l'utilisation de pseudonymes et d'identifiants sectoriels ;
• la limitation de la centralisation de l'authentification et de la vérification.



VERS UN ENCADREMENT DES DISPOSITIFS DE CAMÉRAS MOBILES

La CNIL a été saisie de plusieurs demandes de conseil relatives à l'utilisation de ces nouveaux dispositifs vidéo, par des personnes privées ou par des représentants des forces de l'ordre. Ces dispositifs soulèvent des enjeux différents des caméras vidéo « classiques » (vidéoprotection et vidéosurveillance), dont les conditions de mise en œuvre sont clairement encadrées (code de la sécurité intérieure et loi « Informatique et Libertés »).

LES DISPOSITIFS DE VIDÉO MOBILES

En matière de vidéoprotection, la loi prévoit l'interdiction de visualiser les images de l'intérieur des immeubles d'habitation et, de façon spécifique, celles de leurs entrées. Elle prévoit également que le public doit être informé, « *de manière claire et permanente* », de l'existence du système de vidéoprotection et de l'autorité ou de la personne responsable.

Ces garanties sont difficilement applicables aux dispositifs de caméras mobiles : par définition, la détermination *a priori* des lieux filmés par des caméras mobiles est difficile, de même que l'installation de panneaux d'informations sur le dispositif vidéo. Il importe dès lors de prévoir un encadrement adapté à de tels dispositifs et entourant leur mise en œuvre de garanties suffisantes pour assurer le respect de la vie privée.

Le cadre juridique actuel ne permettant pas un tel encadrement, la CNIL a engagé une réflexion sur ces dispositifs, utilisés à des fins très diverses et avec des moyens techniques variés (caméras-boutonnières, drones, etc.). L'objectif est de proposer des premières recommandations en vue de l'élaboration de cadres juridiques adaptés à l'utilisation de ce nouveau type de caméras tout en préservant l'équilibre entre la protection de la vie privée et la sécurité des biens et des personnes.

Un tel cadre doit s'inspirer des bonnes pratiques existantes en la matière. C'est pourquoi la CNIL procède actuellement au contrôle de certains dispositifs de caméras mobiles, comme par exemple le contrôle de caméras employées par le personnel de sécurité d'un établissement de nuit dans le Nord. Elle a ainsi pu constater que l'enregistrement est déclenché à l'initiative de chaque portier équipé et qu'il est signalé aux personnes présentes par un voyant rouge clignotant sur la partie visible de la caméra portable.

D'autres contrôles devraient permettre de proposer des recommandations plus complètes et adaptées à chaque catégorie de dispositifs. À cet égard, le ministère de l'intérieur a annoncé un projet d'encadrement spécifique concernant les caméras boutonnières destinées aux forces de l'ordre, déterminant les conditions d'emploi de ces caméras mobiles, la nature des lieux dans lesquels un enregistrement peut être réalisé (lieu public, lieu privé ouvert ou non au public, etc.) et la durée de conservation des données collectées. La CNIL se montrera particulièrement attentive à l'encadrement qui sera proposé s'agissant de ces dispositifs. ■

4. BILAN FINANCIER ET ORGANISATIONNEL

Les membres de la CNIL

Ressources humaines

Bilan financier

Organigramme des directions et services

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 septembre 2011. Elle a été réélue à la Présidence de la CNIL en février 2014.
Elle préside le G29 (Groupe des CNIL européennes) depuis février 2014, pour une durée de deux ans.

Vice-président déléguée

Marie-France MAZARS, conseiller honoraire à la Cour de cassation
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

Jean-François CARREZ, président de chambre honoraire à la Cour des comptes
Secteurs : police, immigration, coopération internationale
Jean-François Carrez est membre de la CNIL depuis janvier 2009. Il préside 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, co-fondateur et associé de la société de capital-risque *TheFamily*
Secteur : éducation, enseignement supérieur
Nicolas Colin est membre de la CNIL depuis février 2014.

Loïc HERVE, sénateur de la Haute-Savoie
Secteur : santé (assurance maladie / recherche/ e-santé)
Loic Hervé est membre de la CNIL depuis septembre 2014.

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
Secteur : justice, eurojust
Gaëtan Gorce est membre de la CNIL depuis décembre 2011.

Philippe GOSSELIN, député de la Manche
Secteurs : collectivités locales, vidéoprotection, téléservices.
Philippe Gosselin est membre depuis février 2015.

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
Secteur : santé (assurance maladie/recherche/e-santé)
Alexandre Linden est membre de la CNIL depuis février 2014.

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

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.

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

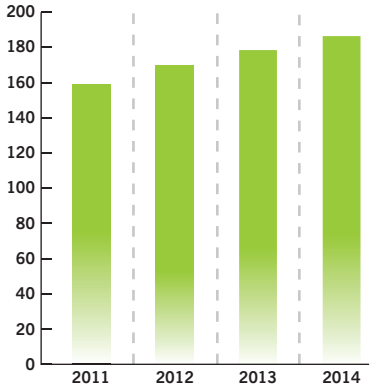
Pour faire face à l'augmentation soutenue de ses missions traditionnelles et à l'accroissement de son périmètre d'intervention par l'entrée en vigueur de nouveaux textes législatifs, la CNIL a bénéficié, en 2014, d'une allocation complémentaire de 7 postes par le législateur. Ainsi, elle est passée de 178 postes à 185, soit une progression de 4 %.

Les 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 la qualité du service rendu aux usagers et les délais de traitements des demandes, ainsi que de renforcer les équipes pour répondre aux nouvelles missions et compétences confiées par le législateur (contrôles en ligne, labels).

Dans la perspective d'évolution croissante de l'activité de la CNIL, les moyens en personnel vont continuer à progresser, à raison d'une moyenne de 6 créations de postes en 2016 et 2017.

Dix ans après la loi du 6 août 2004, à quelques mois de l'adoption du projet de règlement européen, la CNIL s'est dotée d'un plan d'orientations stratégiques pour la période 2012-2015, et 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 ses préoccupations. C'est dans la logique de cette stratégie et pour accélérer sa mutation qu'une réorganisation des services a été décidée (cf. organigramme des directions et services).

Nombre de postes entre 2011 et 2014



Profil des agents de la CNIL

- **Âge moyen : 38,5 ans**
- **30 % de postes occupés par des juristes, 18 % par des assistants juridiques, 13 % par des ingénieurs / auditeurs**
- **50 % des agents travaillant à la CNIL sont arrivés entre 2010 et 2014**
- **70 % des agents occupent un poste de catégorie A**
- **63 % de femmes / 37 % d'hommes**
- **L'ancienneté moyenne est de 9 ans environ**

LES RESSOURCES FINANCIÈRES

En 2014, les crédits octroyés à la CNIL s'élèvent à 15 585 711 € en autorisations d'engagements et 17 434 431 € en crédits de paiement, répartis comme suit : 12 334 691 € pour le budget de personnel (titre 2) et 3 244 804 € en autorisations d'engagements et 5 150 114 € en crédits de paiement pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6 : soit le budget hors titre 2).

Ainsi, les crédits alloués au budget du personnel ont progressé de 5,5 % en raison des 7 créations de postes et le budget hors titre 2 (HT2) a diminué de 2,2 % en crédits de paiement en raison de l'effort budgétaire demandé aux institutions publiques.

En 2014, la CNIL a initié un schéma directeur des systèmes d'information (SDSI) qui doit s'achever à la fin de l'année 2015, autour de cinq axes de travail :

• Développer une réponse multicanal, avec notamment la mise en place d'une plate-forme de questions/réponses en ligne (pour mémoire, la permanence juridique de la CNIL reçoit actuellement 500 appels /jour) ;

• Améliorer l'accompagnement des usagers dans leurs démarches en ligne ;

• Disposer d'outils métiers pleinement adaptés aux missions de la Commission ;

• Refondre le site internet cnil.fr ;

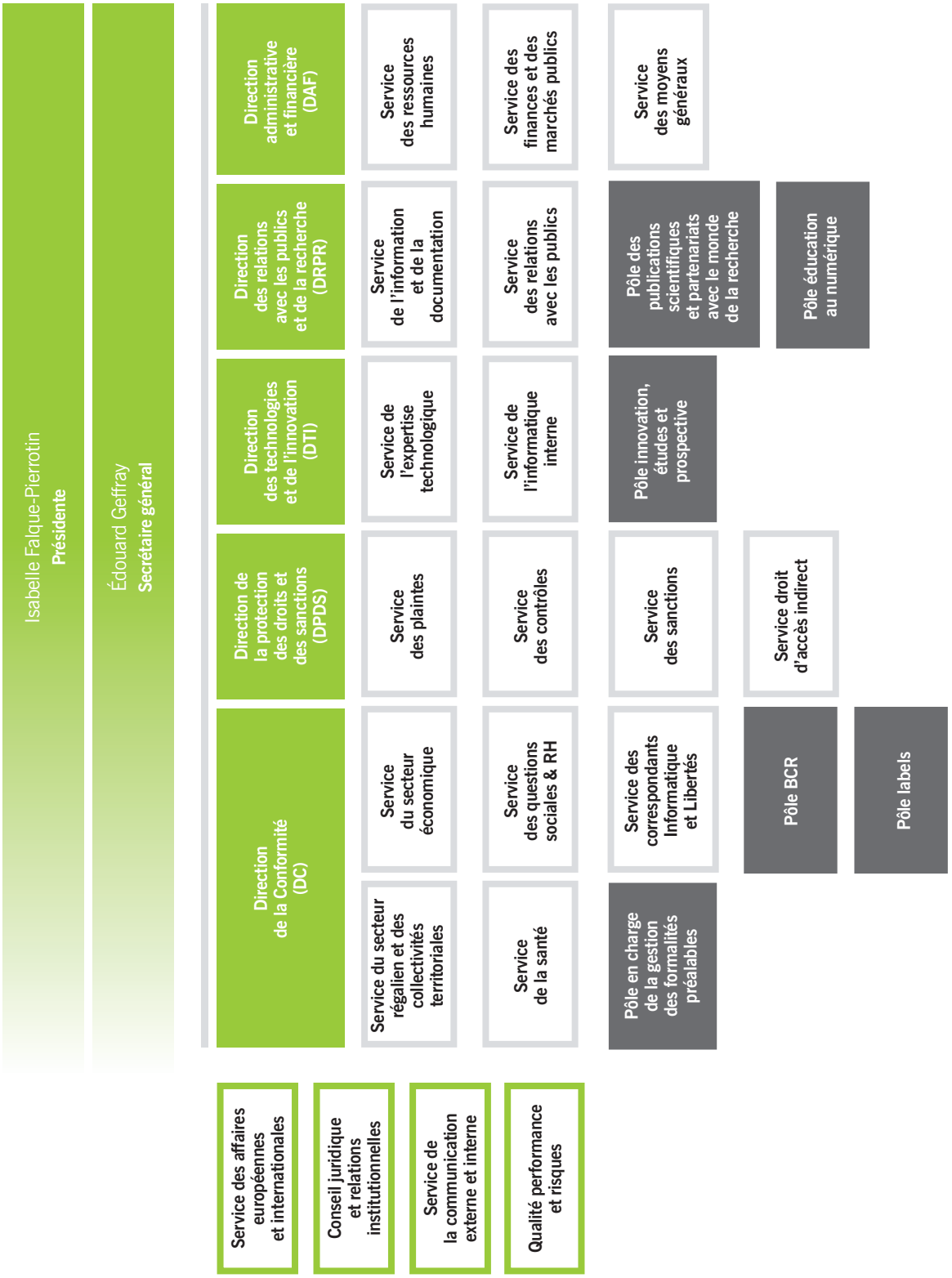
• Mettre en œuvre le projet d'Open data avec les données de la CNIL.

Dans ce cadre, un effort budgétaire a été réalisé par l'institution pour consacrer à cette action un montant de 236 495 € TTC en 2014.

Par ailleurs, la CNIL a poursuivi la mutualisation de ses achats avec les services du Premier ministre et le service des achats de l'Etat (SAE) afin de pouvoir dégager des économies pour des dépenses de fonctionnement courant et de réallouer ces sommes à des projets métiers.

CRÉDITS 2014	Autorisations d'engagement	Crédits de paiement
Budget disponible	**15 579 495 €**	**17 484 805 €**
Titre 2	12 334 691 €	**12 334 691** €
Hors Titre 2	3 244 804 €	**5 150 114** €

ORGANIGRAMME DES DIRECTIONS ET SERVICES



ANNEXES

Liste des organismes contrôlés en 2014

Lexique

LISTE DES ORGANISMES CONTRÔLÉS EN 2014

ASSURANCE

COURTANET

FÉDÉRATION DES MUTUELLES DE FRANCE

LA MUTUELLE DES ÉTUDIANTS

MAÏF

RHSP- MUTUELLE SANTÉ

SANTÉ MUTUELLE SERVICES

MUTUELLE ENTRAIN

FÉDÉRATION DES MUTUELLES DE FRANCE

BANQUES-FINANCE

BNP PARIBAS -MONTREUIL

BANQUE POPULAIRE OCCITANE

CA CONSUMER FINANCE

CAISSE D'ÉPARGNE ET DE PRÉVOYANCE DE BOURGOGNE FRANCHE-COMTÉ

CAISSE D'ÉPARGNE ET DE PRÉVOYANCE DE RHÔNE-ALPES

CARREFOUR BANQUE

CRÉDIT LYONNAIS

FORTUNEO

MINISTÈRE DES FINANCES ET DES COMPTES PUBLIQUES :

-SERVICE DES IMPÔTS DES PARTICULIER PARIS

ÉTABLISSEMENT DE SERVICE INFORMATIQUE NEVERS

ÉTABLISSEMENT DE SERVICE INFORMATIQUE BORDEAUX

ÉTABLISSEMENT DE SERVICE INFORMATIQUE CLERMONT - FERRAND

SECUVAD

COLLECTIVITÉS LOCALES

CENTRE COMMUNAL D'ACTION SOCIALE D'ARLES

CENTRE COMMUNAL D'ACTION SOCIALE DE BOULOGNE SUR MER

CENTRE COMMUNAL D'ACTION SOCIALE DE SAINT DENIS

COMMUNE D'ARLES

COMMUNE DE BOULOGNE SUR MER

COMMUNE DE CORBEIL ESSONNES

COMMUNE DE LA MADELEINE

COMMUNE DE LA PLAINE DES PALMISTES

COMMUNE DE MONTAUBAN

COMMUNE DE L'ISLE SUR LA SORGUE

COMMUNE DE RIS ORANGIS

COMMUNE DE SAINT PAUL

COMMUNE DE VENELLES

COMMUNE LE TAMPON

CONSEIL GÉNÉRAL DE SEINE-SAINT-DENIS

COMMERCE

A.C. CONSEILS & RECRUTEMENT

ADOPTEUNMEC

AGENCE FINANCIÈRE DE L'OR

ANKAMA ANIMATIONS

APPLICATION MOBILE NEARFACE - (ALLADIN TECHNOLOGIES)

ARAMIS

ARESLASER

ASSOCIATION CONTRIBUABLES ASSOCIÉS

ASSURLAND.COM

ATTRACTIVEWORLD

AVIS LOCATION DE VOITURES

AUCHAN FRANCE (VAL EUROPE)

AUCHAN FRANCE (VILLENEUVE D'ASCQ)

AUCHAN FRANCE – (FACHES THUMESNIL)

AUTOREFLEX.COM

BROTHER FRANCE

BIP & GO

BIO MINCEUR SAINT PAUL

BOOKING.COM

BOULANGERIE PAUL

BOUYGUES TÉLÉCOM - PREVENTEL

CARMIGNAC GESTION

CARREFOUR HYPERMARCHÉ

CARREFOUR HYPERMARCHÉ (COMPAGNIE IBM FRANCE)

CECOS

CELSIUS ONLINE

CERTEGY SNC

CLICHY DISTRIBUTION

COTTEL RÉSEAUX

CYBERSOURCE FRANCE SAS

DEKRA CERTIFICATION

DHL INTERNATIONAL EXPRESS FRANCE (TRAITEMENT DE DONNÉES AUX SITES DHL.FR ET DHL-FRANCE.COM)

DIET-AVENUE.COM DIET AVENUE (SITE MARCHAND) – AUDITION

DISTRIBUTION CASINO FRANCE (GÉANT CASINO MONTPELLIER)

DREAM CASH

EFFICIENCY NETWORK

EFFILIATION

ÉLYSÉES CONSULT

ENTREPÔT PÉTROLIER DE LYON

ÉTOILE ALSACE IMPRESSION

EXPÉDIA FRANCE

EUROPE RÉSEAUX

EUROPÉENNE DE TRAITEMENT DE L'INFORMATION

EURIWARE

EUROPE 1 TÉLÉCOMPAGNIE

FIPAC – AUDITION
GIE DU CENTRE COMMERCIAL ITALIE 2
GIE PREVENTEL ET SOPRA GROUP
GLEEDEN.COM
GRAND CASINO DE LYON
GROUPON FRANCE
HYPERCOSMOS
INTÉGRAL
JARDIN IMPORT
JF COM
JIVE SQUAD
LA POSTE - LA ROCHE SUR YON
LA POSTE AVIGNON
LE FROID VENDÉEN
LEROY MERLIN
LES ÉDITIONS NERESSIS
LEVANDIS
MGI-TWC SAS
MONOPRIX EXPLOITATION
MONSIEUR BONTE THIERRY - AUDITION
MONSIEUR MOURE JEAN-PIERRE - AUDITION
MEETIC.FR
MEKTOUBE.FR
MICROSOFT ADVERTISING
MORGANE
NESS INTERACTIVE (SITE FEUJWORLD)
ODYSSEY MESSAGING
OGONE
OPTICAL CENTER
PEOPLE AND TECH
PHOENIX CORP
PJMS
PRICEMINISTER
PRISMA MEDIA
RAY PRO MAILING
R2J COMPANY - AUDITION
RENTABILIWEB MARKETING
RPFFB
ROYALE DECO
SAPAM STRASBOURG
SARL FINANCIÈRE LAMPE
SARL MARLENE
SCHNEIDER ELECTRIC
SHOWROOPRIVE.COM
SMARTADSERVER
SOCIOMANTIC LABS SARL
SODIAM
SOLUTION SOUDURE
SEMS SA
STARS MUSIC TWEETER
STRASBOURG ÉVÉNEMENTS
SUPER JEAN NICOT
SUPER DOMINIQUE (G20)
SUPPLY CHAIN FRANCE - AUDITION
THEBLUEPILL
THESEIS
THIM NAUTIQUE SAINT GILLES LES BAINS
TOUCHVIBES
RUE DU COMMERCE
UNIC HÔTEL
VIADEO
VIDEDRESSING
UNIBAL MARKETING & MULTIMÉDIA
WILO SALMSON FRANCE
WWW.RENCONTRE-OBSESE.COM
WWW.EASYFLIRT.COM
WWW.DESTIDYLL.COM
WWW.FORCEGAY.COM
WWW.CHETIEN-RENCONTRE.COM
WWW.MARMITELOVE.COM
WWW.GAUCHE-RENCONTRE.COM
WWW.DROITE-RENCONTRE.COM
2L MULTIMÉDIA
3 H (HÔTEL ÉCOLE CENTRALE)
3M FRANCE

ÉDUCATION-CULTURE-SPORT

ASSOCIATION GESTION ÉCOLE CATHOLIQUE SACRE CŒUR
CENTRE D'INFORMATION ET D'ORIENTATION DE SAMBRE AVESNOIS
CHAMOIS NIORTAIS FOOTBALL CLUB NIORT
CIFA - AUXERRE
CLERMONT FOOT 63 - STADE GABRIEL-MONTPIED
FC NANTES
FC ROUEN
FOOTBALL CLUB DES GIRONDINS DE BORDEAUX
GFC AJACCIO
GROUPE EDH SAS
HARAS DE LA CENSE
LE MANS FOOTBALL CLUB
LYCÉE MARCELIN BERTHELOT
OLYMPIQUE DE MARSEILLE
PARIS SAINT-GERMAIN FOOTBALL - BOULOGNE-BILLANCOURT
PARIS SAINT-GERMAIN FOOTBALL - PARIS
RACING CLUB DE LENS -
RACING CLUB DE STRASBOURG ALSACE
RODEZ AVEYRON FOOTBALL
SASP ANGERS SCO FOOTBALL
SASP EVIAN THONON GAILLARD FOOTBALL CLUB
SASP FOOTBALL CLUB DE METZ
SASP TOULOUSE FOOTBALL CLUB
SASP VAFC - VALENCIENNES
STADE BRESTOIS 29
STADE MALHERBE CAEN-CALVADOS-BASSE NORMANDIE
STADE RENNAIS FOOTBALL CLUB
TOURS FOOTBALL CLUB ASSOCIATION
UNION SPORTIVE BOULOGNE COTE D'OPALE
UNIVERSITÉ PARIS 1 PANTHEON SORBONNE
UNIVERSITÉ PARIS DESCARTES
VANNES OLYMPIC CLUB
WWW.LEQUIPE.FR

IMMOBILIER

ADEME
GESTION ET TRANSACTIONS DE FRANCE

▸▸▸

POLICE-JUSTICE-SECURITÉ

MINISTÈRE DE LA JUSTICE - FIJAIS

MINISTÈRE DE LA JUSTICE

DIRECTION INTERRÉGIONALE DES SERVICES PÉNITENTIAIRES D'ILE-DE-FRANCE

MINISTÈRE DE LA JUSTICE MAISON CENTRALE DE POISSY

MINISTÈRE DE LA JUSTICE PRESTATAIRE THALES

MINISTÈRE DE LA JUSTICE (ADMINISTRATION PÉNITENTIAIRE CENTRE DE DÉTENTION DE MELUN)

MINISTÈRE DE LA JUSTICE

(ADMINISTRATION PÉNITENTIAIRE - CENTRE DE DÉTENTION DE RENNES)

MINISTÈRE DE LA JUSTICE (ADMINISTRATION PÉNITENTIAIRE - PARIS)

MINISTÈRE DE LA JUSTICE

(ADMINISTRATION PÉNITENTIAIRE - DIRECTION INTERRÉGIONALE DES SERVICES PÉNITENTIAIRES DE LILLE)

MINISTÈRE DE LA JUSTICE

(ADMINISTRATION PÉNITENTIAIRE) DIRECTION INTERRÉGIONALE DES SERVICES PÉNITENTIAIRES DE TOULOUSE)

MINISTÈRE DE LA JUSTICE

(ADMINISTRATION PÉNITENTIAIRE - MAISON CENTRALE DE ST MAUR)

MINISTÈRE DE LA JUSTICE (ADMINISTRATION PÉNITENTIAIRE - MAISON CENTRALE DE ST-MARTIN-DE-RÉ)

MINISTÈRE DE LA JUSTICE (ADMINISTRATION - PÉNITENTIAIRE) PRESTATAIRE SODEXO

MINISTÈRE DE LA JUSTICE (DIT)

MINISTÈRE DE LA JUSTICE (GEPSA)

MINISTÈRE DE LA JUSTICE (MAISON D'ARRÊT DE VALENCE)

MINISTÈRE DE LA JUSTICE (TELEM TÉLÉSURVEILLANCE)

MINISTÈRE DE LA JUSTICE DISP DE MARSEILLE (MAISON D'ARRÊT D'AIX-LUYNES)

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE L'INTÉRIEUR (DIRECTION INTERRÉGIONALE DE POLICE JUDICIAIRE – STRASBOURG)

MINISTÈRE DE L'INTÉRIEUR (SERVICE RÉGIONAL DE POLICE JUDICIAIRE – REIMS)

MINISTÈRE DE L'INTÉRIEUR ET DU MINISTÈRE DES AFFAIRES ÉTRANGÈRES (SOUS-DIRECTION DES VISAS – NANTES)

MINISTÈRE DE L'INTÉRIEUR POLICE DE L'AIR ET DES FRONTIÈRES - SAINTE-MARIE

SANTÉ – SOCIAL

AMNESTY INTERNATIONAL FRANCE

ASSISTANCE PUBLIQUE HÔPITAL EUROPÉEN GEORGES POMPIDOU

ASSISTANCE PUBLIQUE HÔPITAL ROBERT DEBRÉ

ASSOCIATION DES AMIS DE L'ACCUEIL DE NUIT DU PAYS CHAGNOTIN

CAISSE PRIMAIRE D'ASSURANCE MALADIE DE HAUTE-GARONNE

CENTRE HOSPITALIER DE BETHUNE

CENTRE HOSPITALIER DE LUNEVILLE

CENTRE HOSPITALIER ESQUIROL DE LIMOGES

CENTRE HOSPITALIER INTERCOMMUNAL ÉMILE DURKHEIM

CENTRE HOSPITALIER NATIONAL D'OPHTALMOLOGIE DES QUINZE-VINGTS

CHAIGNEAU DAMIEN

CONSEIL GÉNÉRAL DE L'HÉRAULT

CONSEIL NATIONAL DE L'ORDRE DES INFIRMIERS

E-SANTE

GESTION DE TÉLÉASSISTANCE ET DE SERVICES

LA POSTE

MEDICA CONTROL

MONDIAL ASSISTANCE FRANCE SAS

MONDOCTEUR

MUTUALITÉ FRANÇAISE NORD

POLE EMPLOI - NORD-PAS-DE-CALAIS AGENCE DE VILLENEUVE D'ASCQ

SANTÉ ASSISTANCE

SARL EMMANUEL HERE

SELARL PHARMACIE VALNESIS

SERVICE MÉDICAL PATRONAL

SIGEMS DATA CENTER

SOCIÉTÉ DE GESTION CLINIQUE SAINTE-CLOTHILDE

SYNDICAT NATIONAL DES INFIRMIÈRES ET DES INFIRMIERS LIBÉRAUX

VITALLIANCE

WORK 2000 MÉTALLURGIE

TÉLÉCOMMUNICATION

ORANGE

ORANGE - SOUS-TRAITANT GUTEMBERG NETWORKS

XL MARKETING

TRANSPORT

AUTOLIB'

DERET TRANSPORTEUR

IDTGV

RÉGIE COMMUNAUTAIRE D'EXPLOITATION DE PARCS DE STATIONNEMENT

S.A. GUY CASSET

SERVICE BAGAGES AÉROPORTUAIRE - ORLY SUD

SERVICE BAGAGES AÉROPORTUAIRE - ORLY OUEST

SOCIÉTÉ FRANÇAISE DU TUNNEL ROUTIER DU FRÉJUS

TRANSAT FRANCE

DISPOSITIFS DE VIDÉOPROTECTION/VIDÉOSURVEILLANCE

BANQUE

INSTITUT D'ÉMMISSION DES DÉPARTEMENTS D'OUTRE MER (IEDOM)

COLLECTIVITÉS LOCALES

COMMUNE D'ANTIBES
COMMUNE D'AUXERRE
COMMUNE D'AVILLY-SAINT-LÉONARD
COMMUNE DE BOURGES
COMMUNE DE CABOURG
COMMUNE DE CAVAILLON
COMMUNE DE CHAMBÉRY
COMMUNE DE CHANTILLY
COMMUNE DE CHÂTEAURENARD
COMMUNE DE CHÂTEAUROUX
COMMUNE DE COQUELLES
COMMUNE DE CORMEILLES-EN-PARISIS
COMMUNE DE CREST
COMMUNE DE CROISSY SUR SEINE
COMMUNE D'ÉPERNAY
COMMUNE DE DIJON
COMMUNE DE FEURS - POLICE MUNICIPALE
COMMUNE DE FRANCONVILLE
COMMUNE DE LA GARENNE COLOMBES
COMMUNE LE PECQ
COMMUNE DE MIGENNES
COMMUNE DE MONTEREAU-FAULT-YONNE
COMMUNE DE MONTPELLIER
COMMUNE DE LA MOTTE-SERVOLEX
COMMUNE DE MULHOUSE
COMMUNE D'ORLÉANS
COMMUNE DE RETHEL
COMMUNE DE ROUBAIX
COMMUNE DE SAINT-DENIS
COMMUNE DE SAINT-ÉTIENNE
COMMUNE DE SAINT-PRIEST
COMMUNE DE SAINT-QUAY-PORTRIEUX
COMMUNE DE SALON-DE-PROVENCE
COMMUNE DE TAIN L'HERMITAGE
COMMUNE DE THIERS
COMMUNE DE TOURCOING
COMMUNE DE TREVOU-TREGUIGNEC
COMMUNE DE TROUVILLE-SUR-MER
COMMUNE DE VALENCE
PRÉFECTURE DE SAINT-ÉTIENNE

COMMERCE

AARON OPTIC
APPLE – BORDEAUX
APPLE CARROUSEL DU LOUVRE – PARIS
APPLE OPÉRA – PARIS
APPLE – LE CHESNAY
APPLE – ROSNY SOUS BOIS
BOUCHERON
CARREFOUR – MONTIGNY LES CORMEILLES
CASINO LES QUATRE CHEMINS
CASTORAMA FRANCE
CB LINA CERRONE (3 contrôles)
CENTRE COMMERCIAL CARRE SENART
FUTUROSCOPE DE POITIERS
GAUMONT ANGERS MULTIPLEXE
HIPPODROME DE FEURS
HÔTEL DE L'ABEILLE
HÔTEL AIGLE NOIR
HÔTEL F1 DIJON SUD
HÔTEL MERCURE
HÔTEL MERCURE PARIS GARE DE LYON
LVMH
MR BRICOLAGE
NOVOTEL ORLÉANS LA SOURCE
PLANETE AUTO
RESTAURANT LE DIX-SEPTIÈME
SEPHORA - PARIS LA DÉFENSE
SMILE CLUB
SULTANE DE SABA
SWAROVSKI FRANCE

CULTURE

MUSÉE D'ORSAY ▸▸▸

ÉDUCATION

COLLÈGE SÉVIGNÉ
UNIVERSITÉ D'ORLÉANS
UNIVERSITÉ DE TECHNOLOGIE DE COMPIÈGNE

SANTÉ/SOCIAL

CENTRE HOSPITALIER DE CHÂTEAUROUX
CENTRE HOSPITALIER DÉPARTEMENTAL GEORGES DAUMEZON
CENTRE HOSPITALIER DE GRENOBLE
CENTRE HOSPITALIER PIERRE DEZARNAULDS
COMPAGNIE DE VICHY - ÉTABLISSEMENTS THERMAUX
EHPAD LES JARDINS DE SIDO - CHÂTILLON COLIGNY
EHPAD DU MARAIS
EHPAD SAINT JOSEPH - ORLÉANS
PÔLE EMPLOI - BESANÇON

TRANSPORT

ENTREPRISE MASSEY ET COMPAGNIE
NORBERT DENTRESSANGLE DISTRIBUTION
VOIES NAVIGABLES DE FRANCE SUBDIVISION DE PERONNE

CONTRÔLES EN LIGNE

ACCOR
APEC.FR
AUCHAN.FR
BOULANGER.FR
CHALLENGES.FR
CASSIS.FR
CENTERBLOG.NET
CLERMONT- FERRAND.FR
COLISSIMO.FR
COLOMBES.FR
COMMENTCAMARCHE.NET
COMPRENDRECHOISIR.COM
DARDILLY.FR
DIET-AVENUE.COM
EUROPE1.FR
FRESNES94.FR
HUFFINGTONPOST.FR
IUT-BV.UNIV-FCOMTE.FR
IUT.UNIV-AVIGNON.FR
LACHAINEMETEO.FR
LADEPECHE.FR
LAGARENNECOLOMBES.FR
LAROUSSE.FR
LEXPRESS.FR
LEFIGARO.FR
LE MONDE.FR
MARMITON.ORG
MAIRIE-ORLY.FR
MEGACINEMA.FR
MES-MEILLEURS-FILMS.COM
METEOFRANCE.COM
METRONEWS.FR
MUTUELLE ENTRAIN
NANCY.FR
NARBONNE.FR
NODARON
NOUVELOBS.COM
MAIRIE-AIX EN PROVENCE.FR
OUEST-FRANCE.FR
OVER-BLOG.COM
PARIS.FR
RESEAUX DE RENCONTRES (CELIBNORD ; CELIBEST ; CELIBOUEST ; CELIBPARIS ; CELIBLVON ; CELIBSUD)
ROCHE-LA-MOLIERE.FR
ROUTARD.COM
SLATE.FR
STRASBOURG.EU
VILLE-VICHY.FR
UNIV-ANGERS.FR
U-PEM.FR (UNIVERSITE PARIS EST MARNE LA VALLEE)
TOULOUSE.FR
U-BORDEAUX.FR
U-BORDEAUX-MONTAIGNE.FR
UNIV-MONTP2.FR
UNIV-PAU.FR
UNIV-TLSE3.FR
URSSAF.FR
VILLE-AUBIERRE.FR
VILLE-CHATEAUDUN.FR

LEXIQUE

INFORMATIQUE ET LIBERTÉS

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 sophistiqués offre aujourd'hui des possibilités inégalées d'exploitation des informations. Les ensembles de données traités correspondant à la définition du *big data* répondent à trois caractéristiques principales : volume, vélocité et variété.

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, etc.).

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.

Commission Nationale de l'Informatique et des Libertés (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 cinq 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. Il conseille le responsable de traitement dans l'organisation et la mise en œuvre de la conformité aux règles de la protection des données. Il bénéficie d'un service personnalisé spécialement proposé par la CNIL dédié pour l'accompagner dans l'exercice de ses missions. ▸▸▸

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 (article 8 de la loi « informatique et libertés »)
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 au déréférencement
Dans un arrêt du 13 mai 2014, la Cour de Justice de l'Union européenne a confirmé que les moteurs de recherche sont responsables de traitement. À ce titre, ils doivent respecter le droit européen à la protection des données personnelles. Désormais les personnes peuvent leur demander directement de désindexer une page web associée à leurs nom et prénom.
Ce déréférencement ne signifie pas l'effacement de l'information sur le site internet source. Le contenu original reste ainsi inchangé et est toujours accessible via les moteurs de recherche en utilisant d'autres mots-clés de recherche ou en allant directement sur le site à l'origine de la diffusion.

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.

Drone
Un drone est au sens strict un appareil sans pilote à bord. Il est généralement piloté à distance par un opérateur humain, mais peut avoir un degré plus ou moins important d'autonomie (par exemple pour éviter des collisions ou gérer les conditions aérologiques). Un drone est avant tout une plateforme de capteurs mobiles. C'est un engin d'observation, d'acquisition et de transmission de données géolocalisées.

FICOBA
FICOBA est le fichier national des comptes bancaires et assimilés. Il sert à recenser les comptes bancaires de toute nature (dépôt, épargne), et à fournir aux personnes habilitées des informations sur les comptes détenus par une personne ou une société.

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

Géolocalisation
Technologie permettant de déterminer la localisation d'un objet ou d'une personne avec une certaine précision. La technologie s'appuie généralement sur le système GPS ou sur les interfaces de communication d'un téléphone mobile. Les applications et finalités de la géolocalisation sont multiples : de l'assistance à la navigation, à la mise en relation des personnes, mais aussi à la gestion en temps réel des moyens en personnel et en véhicules des entreprises, etc.

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. La Présidence du G29 est actuellement assurée par la Présidente de la CNIL depuis février 2014, pour une durée de deux ans.

Mise en demeure
Une décision de la Présidente de la CNIL qui énumère les manquements reprochés à l'organisme mis en cause ainsi que les mesures qu'il doit prendre, pour se mettre en conformité dans un délai fixé. À ce stade, la procédure de sanction n'est pas encore engagée. En cas de conformité dans le délai fixé, la procédure est clôturée. À défaut, la Présidente de la CNIL peut désigner un rapporteur qui pourra proposer à la formation restreinte de prononcer une sanction. La mise en demeure peut être rendue publique par le bureau.

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.

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.

Responsable de traitement

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

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 0,05 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).

Sanction

Lorsque des manquements à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut prononcer à l'égard du responsable de traitement :

- Un avertissement, qui peut être rendu public ;
- Dans l'hypothèse où la Présidente de la CNIL a, au préalable, prononcé une mise en demeure, et que le responsable de traitement ne s'y est pas conformé, la formation restreinte peut prononcer, à l'issue d'une procédure contradictoire : Une sanction pécuniaire (sauf pour les traitements de l'État) d'un montant maximal de 150.000 euros, et, en cas de récidive, jusqu'à 300.000 euros. Cette sanction peut être rendue publique ; la formation restreinte peut également ordonner l'insertion de sa décision dans la presse, aux frais de l'organisme sanctionné.
Le montant des amendes est perçu par le Trésor Public et non par la CNIL ;
- Une injonction de cesser le traitement ;
- Un retrait de l'autorisation accordée par la CNIL en application de l'article 25 de la loi.

Séance plénière

C'est la formation qui réunit chaque semaine 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.

Smart city

La ville intelligente est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms) ; transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.) ; les e-services et e-administrations.

Traitement de données

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

Transfert de données

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

Vidéoprotection

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

Vidéosurveillance

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

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 et diffusion Direction de l'information légale et administrative
Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr
Illustrations de la couverture Geoffrey Dorne / **Crédit photo** Fotolia, istockphoto

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

www.cnil.fr

Diffusion
Direction de l'information légale et administrative

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

ISBN : 978-2-11-010024-5
DF : 5HC39710
Prix : 15 €

CNIL
Commission Nationale de l'Informatique et des Libertés