2016

Rapport d'activité

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Protéger les données personnelles,
Accompagner l'innovation,
Préserver les libertés individuelles

La documentation Française

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

2016

Rapport d'activité

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Protéger les données personnelles,
Accompagner l'innovation,
Préserver les libertés individuelles

Prévu par l'article 11 de loi du 6 janvier 1978, modifiée par la loi du 6 août 2004 et l'article 21 de la loi du 20 janvier 2017, portant statut général des autorités administratives indépendantes et loi organique relative aux autorités administratives indépendantes et autorités publiques indépendantes.

LES CHIFFRES CLÉS 2016

CONSEILLER & RÉGLEMENTER

3 078 DÉCISIONS ET DÉLIBÉRATIONS DONT :

190 AUTORISATIONS

145 AVIS

1 976 AUTORISATIONS DE TRANSFERT HORS UE (+83%)

697 AUTORISATIONS EN MATIÈRE DE SANTÉ (RECHERCHE ET ÉVALUATION)

ACCOMPAGNER LA CONFORMITÉ

316 AUTORISATIONS EN MATIÈRE DE BIOMÉTRIE DONT :

9 REFUS

97 LABELS DÉLIVRÉS

102 629 DOSSIERS DE FORMALITÉS REÇUS EN 2016 DONT :

54 000 FORMALITÉS SIMPLIFIÉES

14 734 DÉCLARATIONS POUR DES SYSTÈMES DE VIDÉOSURVEILLANCE

7 370 DÉCLARATIONS POUR DES DISPOSITIFS DE GÉOLOCALISATION

17 725 ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT, SOIT :

4 729 CIL

92 GROUPES ONT ADOPTÉ DES BCR

PROTÉGER

7 703 PLAINTES

410 **PLAINTES,** SUITE À DES REFUS DE DEMANDES DE DÉRÉFÉRENCEMENT AUPRÈS DES MOTEURS DE RECHERCHE

4 379 **DEMANDES DE DROIT D'ACCÈS INDIRECT** (fichiers de police, de gendarmerie, de renseignement, FICOBA, etc.)

7 909 **VÉRIFICATIONS RÉALISÉES**

INFORMER

166 565 APPELS

21 718 COURRIERS REÇUS

80 215 APPELS POUR LA PERMANENCE TÉLÉPHONIQUE

12 231 REQUÊTES REÇUES PAR VOIE ÉLECTRONIQUE

220 INTERVENTIONS LORS DE CONFÉRENCES, COLLOQUES, SALONS

CONTRÔLER & SANCTIONNER

430 **CONTRÔLES DONT :**

100 **CONTRÔLES EN LIGNE**

94 **CONTRÔLES VIDÉO**

82 **MISES EN DEMEURE**

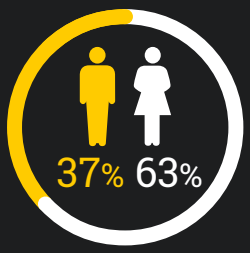
13 **SANCTIONS DONT :**

4 **SANCTIONS FINANCIÈRES ET PUBLIQUES**

9 **AVERTISSEMENTS**

RESSOURCES HUMAINES

195 emplois



41 ans Âge moyen

38% **DES POSTES OCCUPÉS PAR DES JURISTES**

22% **PAR DES ASSISTANTS**

12% **PAR DES INGÉNIEURS / AUDITEURS**

75% **DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A**

53% **DES AGENTS TRAVAILLANT À LA CNIL SONT ARRIVÉS ENTRE 2011 ET 2016**

9 ANS ANCIENNETÉ MOYENNE DES AGENTS DE LA CNIL

SOMMAIRE

Introduction

1 Analyses

2 Bilan d'activité

3 Sujets de réflexion

4 Ressources

LES TEMPS FORTS 2016

Février 2016

09/02
Mise en demeure publique à l'encontre de Facebook pour sa politique de confidentialité

Mars

24/03
Sanction de 100 000 € à l'encontre de Google qui ne procède pas au déréférencement sur l'intégralité des extensions du nom de domaine de son moteur de recherche

Avril

08/04
Publication de la position de la CNIL en matière de chiffrement

Mai

04/05
Parution au journal officiel de l'Union européenne du règlement européen sur la protection des données personnelles

Juin

15/06
Lancement de la consultation sur le règlement européen

Juillet

20/07
Mise en demeure à l'encontre de MICROSOFT concernant Windows 10

27/07
Les contrôles sur les cookies s'étendent au-delà des éditeurs de sites

29/07
Le G29 publie sa position sur le *Privacy shield*

Août

01/08
Entrée en vigueur du *Privacy Shield*

Septembre

26/09
Le premier label coffre-fort numérique est délivré

27/09
Un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail

Octobre

08/10
La loi pour une république numérique est publiée au Journal Officiel

14/10
GOSSIP, les potins anonymes : mise en demeure pour atteintes graves à la vie privée

19/10
CDISCOUNT : avertissement et mise en demeure pour de nombreux manquements

27/10
Avertissement public pour le parti socialiste en raison de failles de données sensibles en ligne

28/10
L'avis de la CNIL sur le fichier TES est publié

Novembre

08/11
La CNIL précise les règles que doivent respecter les candidats et partis quand ils utilisent des données issues des réseaux sociaux

Décembre

27/12
Publication des avis de la CNIL sur les décrets relatifs à l'utilisation des caméras piétons par les forces de l'ordre

29/12
Deux sites de rencontre sanctionnés pour défaut de consentement exprès

LES MEMBRES DE LA CNIL

© Jean-Lionel Dias / Picturetank

LE BUREAU

01

PRÉSIDENTE

Isabelle FALQUE-PIERROTIN

Conseiller d'État.
Membre de la CNIL depuis 2004 et vice-présidente de 2009 à 2011.
Isabelle Falque-Pierrotin est présidente de la CNIL depuis le 21 septembre 2011. Elle préside également le G29 (groupe des CNIL européennes) depuis février 2014.

02

VICE-PRÉSIDENTE 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.

03

VICE-PRÉSIDENT

Éric PERES

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

LES MEMBRES (COMMISSAIRES)

04

Valérie PEUGEOT

Chercheuse au sein d'Orange Labs.
Présidente de l'association Vecam
Secteurs : santé (assurances maladie/ recherche/e-santé).
Valérie Peugeot est membre de la CNIL depuis avril 2016.

05

Marie-Hélène MITJAVILE

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

06

Loïc HERVE

Sénateur de la Haute-Savoie.
Secteur : santé.
Loic Hervé est membre de la CNIL depuis septembre 2014.

07

Sylvie ROBERT

Sénatrice d'Ille-et-Vilaine.
Secteurs : justice et eurojust.
Sylvie ROBERT est membre de la CNIL depuis décembre 2016.

08

Marc DANDELOT

Conseiller d'État honoraire.
Président de la CADA (commission d'accès aux documents administratifs).
Marc Dandelot est membre de la CNIL depuis novembre 2016.

09

Philippe GOSSELIN

Député de la Manche.
Secteurs : collectivités territoriales, vidéoprotection et téléservices.
Philippe Gosselin est membre de la CNIL depuis février 2015.

10

Joëlle FARCHY

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

11

Maurice RONAI

Chercheur à l'École des Hautes Études en Sciences Sociales (EHESS).
Secteurs : NTIC, communications électroniques, innovation technologique.
Maurice Ronai est membre de la CNIL depuis février 2014.

12

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.

13

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.

14

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.

15

Philippe LEMOINE

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.

16

Édouard GEFFRAY

Secrétaire général

17

Alexandre LINDEN

Conseiller honoraire à la Cour de cassation.
Secteurs : santé (assurance maladie / recherche/ e-santé).
Alexandre Linden est membre de la CNIL depuis février 2014.

18

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.

19

Laurence DUMONT

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

LES MEMBRES ÉLUS DE LA FORMATION RESTREINTE

- Jean-François CARREZ (Président)
- Dominique CASTERA
- Philippe GOSSELIN
- Alexandre LINDEN
- Marie-Hélène MITJAVILE
- Maurice RONAI

COMMISSAIRE DU GOUVERNEMENT

- Nacima BELKACEM

AVANT-PROPOS DE LA PRÉSIDENTE

LE COMPTE À REBOURS A COMMENCÉ !

Isabelle FALQUE-PIERROTIN
Présidente de la CNIL

L'année 2016 s'est caractérisée pour la CNIL, une fois encore, par une activité intense et diversifiée, en France ou à l'international, dans un contexte d'évolutions majeures en matière réglementaire qui impactent de façon considérable son fonctionnement ou ses missions. Cela suppose tout à la fois de faire face aux flux des demandes des particuliers et des professionnels, tout en anticipant et en préparant l'entrée en application du règlement européen avec un compte à rebours qui nous rapproche chaque jour un peu plus du 25 mai 2018. Cela demande de faire preuve d'endurance, d'agilité et d'une bonne dose de ténacité.

2016, UNE ANNÉE D'ACTIVITÉ INTENSE ...

C'est indéniable, la protection des données n'a jamais été autant sur le devant de la scène qu'en 2016, et la CNIL est de plus en plus sollicitée, qu'il s'agisse des pouvoirs publics, des professionnels ou des particuliers. Au moment où de nouvelles missions lui sont confiées, elle doit aussi continuer à mener à bien ses missions « traditionnelles ».

C'est d'abord **une CNIL au service des citoyens** qui les aide, dans leur vie quotidienne, à exercer leurs droits. On le constate chaque année, ils souhaitent mieux maîtriser leur vie en ligne, ce à quoi la loi pour une République numérique et le règlement européen font écho en renforçant cette autonomie individuelle. Dans ces deux textes en effet, l'individu est placé au centre de la régulation numérique et le rapport de force avec les plateformes est en train de se rééquilibrer. L'engouement du droit au déréférencement en France illustre bien cette nouvelle posture responsable et active qui permet de limiter dans le temps l'effet d'un contenu et aménager sa vie en ligne en fonction de ses propres attentes. Ce droit européen, auquel s'intéressent aujourd'hui d'autres pays, devrait d'ailleurs pouvoir être porté comme standard international.

C'est aussi **une CNIL qui conseille davantage les pouvoirs publics** dans l'élaboration de textes réglementaires ou législatifs. Parmi les 3 000 décisions de l'année 2016, elle a ainsi rendu 145 avis, répondant très souvent à des saisines en urgence, sans dégrader la qualité de l'analyse produite. L'avis que la Commission a rendu sur la création du fichier TES a par exemple particulièrement compté dans le débat qui a suivi la publication du décret et a donné lieu à de nombreuses auditions.

C'est enfin **une CNIL qui accompagne les entreprises et les organismes publics** dans leur conformité à droit constant, tout en les préparant au nouveau cadre juridique européen. Dès 2012, la CNIL a anticipé le règlement en développant des outils de

conformité tels que le Correspondant Informatique et Libertés, les labels, les analyses d'impact vie privée ou les packs de conformité qui sont aujourd'hui consacrés. Les entreprises françaises ayant déjà intégré ces outils pourront aborder le règlement de façon plus sereine puisqu'elles ont déjà fait une bonne partie du chemin vers l'*accountability*, clé de voûte de la conformité à l'heure du règlement.

… MARQUÉE PAR L'ADOPTION DE TROIS TEXTES MAJEURS POUR LA PROTECTION DES DONNÉES EN FRANCE ET DANS LE MONDE

L'année 2016, c'est aussi l'aboutissement de trois textes majeurs pour la protection des données en France et dans le monde, auxquels la CNIL et ses homologues européens ont très activement participé.

La loi pour une République numérique du 7 octobre 2016 constitue incontestablement une avancée pour la protection des droits des personnes. Elle complète l'article 1er de la loi Informatique et Libertés et prévoit que : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. » Elle réaffirme, qu'à l'ère numérique, la personne est le centre de gravité de la législation sur la protection des données. En effet, la loi reconnait aux personnes un droit à « l'autodétermination informationnelle » y compris la possibilité de prévoir le sort de ses données après sa mort. Un droit à l'oubli pour les mineurs est consacré et les modalités d'information sont renforcées.

Au-delà des pouvoirs de sanction renforcés, la CNIL s'est aussi vue confier de nouvelles missions. Sans attendre, elle s'est emparée de certaines d'entre elles, comme « la conduite d'une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ». Le 23 janvier, la CNIL a donc initié une démarche originale consistant à lancer un cycle de débats, réflexions et événements divers sur le thème des algorithmes. En effet, ceux-ci sont présents dans tous les compartiments de nos vies et véhiculent une puissance présumée considérable. L'algorithme fait une promesse et la question est de savoir s'il tient cette promesse. Dans le même temps c'est une véritable machine à fantasmes. Pour toutes ces raisons, il nous semblait utile de prendre un peu de distance et d'adopter une approche raisonnée pour permettre, in fine, de dessiner les contours d'un pacte social partagé. Une vingtaine d'organismes partenaires se sont engagés à nos côtés, prêts à organiser des événements grands publics, professionnels ou sectoriels autour de l'utilisation des algorithmes dans leurs champs de compétences. La CNIL coordonne ces initiatives en vue de restituer une cartographie de l'état du débat public et, le cas échéant, de proposer aux pouvoirs publics des pistes pour accompagner le développement des algorithmes dans un cadre éthique.

L'autre grand texte de l'année est le ***Privacy Shield*, accord signé entre l'Europe et les États-Unis en juillet** et remplaçant le *Safe Harbor* invalidé par la Cour de Justice de l'Union Européenne en octobre 2015. C'est un véritable bras de fer qui s'est joué ente la Commission européenne et les autorités américaines pendant plusieurs mois, rythmé par le G29 qui avait fixé une date butoir à la conclusion de ces négociations. Le G29, avec la CNIL en première ligne, puisqu'elle assure la présidence du groupe des autorités européennes, a su tenir ferme la barre et naviguer dans un environnement d'une extrême complexité mêlant enjeux économiques, politiques et diplomatiques. Après de nombreux rebondissements, l'accord a finalement été conclu fin juillet. Cet accord est majeur car il fait entrer la problématique de la surveillance par les services de renseignement au sein des accords commerciaux et démontre ainsi que, nonobstant la valeur économique des données, la protection des données reste centrale.

Depuis cette date, de nombreuses actions ont été engagées pour assurer la mise en œuvre concrète du bouclier vie privée. La prochaine étape sera la première revue annuelle de l'accord qui doit se tenir en septembre 2017. Cette évaluation sera décisive puisqu'elle sera l'occasion d'évaluer concrètement la robustesse et l'effectivité des garanties prévues par l'accord en juillet dernier, et ce, alors que les équipes en place à l'époque ont toutes quitté leur fonction et ne sont pas encore renouvelées, à l'heure où j'écris ces lignes. Le G29 vient d'ailleurs d'adresser un courrier aux autorités américaines leur demandant de clarifier leur position quant aux engagements pris, au regard notamment de la tonalité non favorable au non-américains exprimée dans certains décrets présidentiels publiés récemment.

J'en viens maintenant bien sûr au **règlement européen sur la protection des données** qui a été adopté en 2016 et qui entrera en application le 25 mai 2018. Texte fondamental qui rénove profondément la régulation européenne des données et qui offre incontestablement à l'Europe la possibilité de récupérer sa souveraineté numérique : une souveraineté individuelle car les individus gagnent de la maîtrise, une souveraineté collective car les autorités parleront d'une seule voix et enfin une souveraineté territoriale dans la mesure où il remet les acteurs européens à égalité de concurrence avec les acteurs mondiaux qui seront soumis au droit européen dès lors qu'ils offrent un produit ou un service à un citoyen européen. La complexité du règlement avec ses 99 articles et ses 200 considérants ne doit pas masquer pour autant l'essence du texte qui consiste à renforcer la place centrale de l'individu dans l'univers des données.

« La personne est le centre de gravité de la législation sur la protection des données. »

« Le règlement offre incontestablement à l'Europe la possibilité de récupérer sa souveraineté numérique. »

UNE PRIORITÉ ABSOLUE EN 2017, PRÉPARER LE PASSAGE AU RÈGLEMENT

Après quatre années de négociations intenses, l'adoption du règlement est donc un aboutissement mais aussi un point de départ. Après avoir manié pendant plusieurs années de nombreux concepts, il va falloir leur donner corps. Je pense notamment à l'*accountability*, au guichet unique, à la portabilité, à la certification ou au *privacy by design*. Notre tâche essentielle consiste maintenant à décliner à partir du texte du règlement une boîte à outils opérationnelle et claire pour les acteurs, avant mai 2018. Ce sera donc notre priorité absolue pour 2017. Nous sommes très attendus par les professionnels qui demandent avant tout un cadre lisible leur permettant de garantir la sécurité juridique de leurs traitements et leur développement économique.

Pour parvenir à cet objectif, **le G29 a adopté un plan d'action ambitieux qui s'articule autour de deux axes principaux :**

- Le premier concerne la publication de lignes directrices sur les sujets prioritaires. Il s'agit de rendre le règlement le plus opérationnel possible pour les responsables de traitement et de limiter tout risque de « dés-harmonisation », voire le *forum shopping*. Ce travail a été engagé dès 2016 et trois lignes directrices sont en phase d'adoption finale. De nouvelles lignes directrices sont en cours de finalisation ou d'élaboration. Au cours de ce processus, le G29 a souhaité proposer aux acteurs concernés de co-construire la boîte à outils, forts de leur expérience terrain. Des concertations sont donc mises en place, soit au niveau national, comme les consultations en ligne proposées par la CNIL, soit par le biais d'ateliers participatifs organisés à Bruxelles avec les différentes parties prenantes. C'est une démarche tout à fait originale pour le G29 qui permet de s'assurer que les lignes directrices ne sont pas élaborées « hors-sol » mais intègrent bien les préoccupations ou les bonnes pratiques des professionnels eux-mêmes.

- Le second axe s'attache à construire le nouveau modèle de gouvernance des autorités. En effet, le règlement impose une intégration des autorités de protection beaucoup plus importante dans la mesure où elles sont amenées à prendre des sanctions communes pour le compte des 28 sur la base d'une doctrine partagée. Cette avancée considérable nécessite que toutes les procédures de coopération entourant les sanctions, la désignation de l'autorité chef de file dans le cas des traitements transnationaux soient imaginées et écrites. Elle nécessite également de rendre opérationnel le Comité Européen à la protection des données (CEPD) qui bénéficiera d'une institutionnalisation européenne renforcée par rapport au G29. L'enjeu de cette nouvelle gouvernance est énorme : opérationnel naturellement car sinon le règlement restera lettre morte ; politique aussi car il s'agit de montrer que l'Europe peut accoucher d'un modèle nouveau, moins centralisé à Bruxelles mais plus participatif et distribué.

La CNIL participe bien sûr très activement à ces travaux au niveau européen parallèlement à un plan d'action national qui s'articule principalement autour de l'accompagnement des professionnels, la transformation de nos outils de conformité en standards européens et la conduite du changement au sein de la CNIL.

Nous abordons ces changements avec méthode et par étapes. Ce nouveau cadre nous donne aussi l'occasion de repenser nos pratiques et renouveler nos modes d'intervention. Comme je l'évoquais plus haut, certains principes du règlement ont été éprouvés et anticipés par la CNIL depuis plusieurs années. Il n'en demeure pas moins que le chantier est considérable et que les services de la CNIL sont de fait soumis à de très fortes pressions qui peuvent parfois aller jusqu'au sentiment de vertige.

Nous sommes comme les éléments d'une cordée qui progresse lentement vers le sommet, qui regarde parfois vers le bas et qui voit à la fois le chemin parcouru et le sommet qui reste à gravir.

Dans les instants de doutes, et il en existe, je me tourne vers les collaborateurs de la CNIL, vers mes collègues européens, vers les entreprises et les acteurs publics que nous rencontrons tous les jours et je sais que collectivement, nous pouvons réussir. Je sais surtout que ce texte offrira assurément aux citoyens européens des droits renforcés et que c'est pour eux que nous œuvrons.

À l'aube de ses 40 ans, c'est une véritable cure de jouvence à laquelle la CNIL se prépare. Pourtant, même si elle évolue et se renouvelle, nous gardons à l'esprit que le principe qui guide notre action et nous anime chaque jour, c'est que le numérique et les technologies demeurent au service de l'individu. L'année 2016 l'a réaffirmé et renforcé par les textes, veillons à ce que 2017 et 2018 lui donnent tout son sens.

MOT DU SECRÉTAIRE GÉNÉRAL

UNE CNIL À 360° AU SERVICE DES CITOYENS

Edouard GEFFRAY
Secrétaire général

Alors que le règlement européen entre en vigueur dans un an, la CNIL a, en 2016, arrêté et mis en œuvre son nouveau plan stratégique pour les années 2016-2018. Les principaux objectifs de ce plan stratégique sont de conduire la transition vers le règlement européen, d'accompagner la transition numérique des acteurs publics et privés et de fournir un service de haut niveau aux personnes pour assurer une protection effective de leurs droits et libertés à l'ère numérique.

Un an plus tard, la CNIL a considérablement avancé sur le chemin ainsi tracé, dans un contexte de croissance toujours soutenue. L'année à venir sera l'occasion de renforcer l'accompagnement des acteurs et des citoyens dans une double logique : promouvoir une culture de la donnée et assurer une sécurisation juridique optimale pour les acteurs.

L'année écoulée a, sans aucun doute, donné lieu à une première prise de conscience de la part des entreprises de la nécessité de se préparer au règlement européen. Tous les outils de la conformité sont désormais mobilisés par les entreprises pour développer cette nouvelle culture, caractérisée par une responsabilisation, non seulement des entreprises et administrations en tant que donneuses d'ordre, mais également de leurs sous-traitants.

Pour tous, le premier vecteur de cette préparation est bien sûr le Correspondant Informatique et Libertés, le CIL. Non seulement il permet de se préparer à l'évolution du cadre applicable par l'internalisation de cette compétence et d'une organisation respectueuse de la protection des données, mais son successeur, le délégué à la protection des données, sera obligatoire à compter du 25 mai 2018 dans toutes les administrations et dans de très nombreuses entreprises. Or, la France est sur ce terrain en avance : ce sont en effet plus de 17 700 entités qui sont d'ores et déjà dotées d'un CIL. Il y en aura probablement 80 à 100 000 dans un an. De même, à titre indicatif, 92 groupes se sont dotés de « BCR », ces règles d'entreprises contraignantes qui permettent de créer une bulle juridique protectrice pour la circulation des données à l'intérieur d'un même groupe.

Pourtant, nombreux sont les acteurs qui ne sont pas - ou ne se sentent pas - prêts pour le règlement. C'est pourquoi la CNIL

« La CNIL accompagne les professionnels pour leur apporter le maximum de sécurité juridique. »

et ses services se mobilisent pour les accompagner dans cette transition, qui correspond aussi, souvent, à l'évolution de leurs métiers.

Concrètement, la CNIL densifie progressivement la rubrique de son site dédié au règlement européen pour permettre à chacun de s'approprier le texte. Outre les textes fondamentaux, les entreprises peuvent ainsi y trouver les lignes directrices du G29, une présentation générale du texte, la méthodologie pour réaliser les études d'impact sur la vie privée, ou encore des questions/réponses, régulièrement alimentées, pour répondre à leurs principales interrogations.

Au-delà, la CNIL souhaite accompagner les professionnels pour leur apporter le maximum de sécurité juridique. Elle peut notamment s'appuyer sur son organisation sectorielle, qui offre à chaque entité un « guichet unique », sa longue expérience des cadres de références en matière de simplification (dispenses de déclaration, normes simplifiées, autorisations uniques), pour construire les référentiels de demain et les promouvoir au niveau européen. De même, les packs de conformité préfigurent les relations entre les secteurs économiques et le régulateur dans le champ de la conformité. Enfin, grâce à son expérience en matière de labels, la CNIL est également préparée à la nouvelle activité de certification prévue par le règlement.

C'est ainsi que, depuis plusieurs années et en avance de phase sur le règlement, la CNIL a développé une série d'outils qui seront, demain, au cœur de la conformité. L'adoption de codes de bonne conduite, tout comme le recours obligatoire, dans certains cas, aux études d'impact, permettra à la CNIL de disposer d'une large gamme d'outils. En d'autres termes, d'être un régulateur complet.

L'enjeu est de concilier protection des droits fondamentaux des personnes et innovation. Or, cet équilibre est non seulement nécessaire, mais il est fécond : administrations comme entreprises ont compris, ces dernières années, à quel point la protection des données était au cœur des nouveaux modèles de développement numériques. La diversité des activités de la CNIL, relatée dans ce rapport, en témoigne : au titre de sa mission d'information, la CNIL a répondu à plus de 160 000 appels et poursuivi ses travaux en matière d'éducation au numérique. S'agissant de son activité réglementaire et de conseil, elle a adopté plus de 3 000 autorisations, dont 145 avis au Gouvernement. Elle a également été conviée à près d'une trentaine d'auditions parlementaires. Au titre de sa mission de contrôle, elle a procédé à plus de 400 contrôles, traité près de 8000 plaintes et plus de 4000 demandes de droit d'accès indirect. Mais au-delà de ces aspects quantitatifs, la CNIL a aussi approfondi ses réflexions sur des enjeux majeurs, comme la biométrie, ou engagé de nouvelles réflexions prospectives, avec le concours du Comité de la prospective, notamment sur les villes intelligentes. La loi du 7 octobre 2016 a complété cette gamme en confiant à la CNIL le soin de conduire la réflexion sur les conséquences éthiques et les questions de société soulevées par le numérique. La CNIL a ainsi lancé un grand débat public, multi partenarial, en 2017, sur le thème « Ethique et algorithmes ».

La CNIL est donc un régulateur complet, une CNIL à 360°, qui, protège les personnes, accompagne la transition numérique des administrations et entreprises, et prépare le passage au règlement européen. Tout ceci n'est possible que grâce à ce qui fait la force de la CNIL : ses valeurs, auxquelles sont profondément attachés tous les agents qui travaillent au service de la Commission. C'est cette boussole qui permet, en cette période de transition, d'aller de l'avant et de construire une régulation sereine.

« Un régulateur complet. »

Analyses

Règlement européen : de l'adoption à la mise en œuvre

Le règlement européen, dit règlement général sur la protection des données (RGDP) a été adopté le 14 avril 2016 après plus de quatre ans de négociations. Applicable à compter du 25 mai 2018, il constitue une évolution majeure du cadre juridique de la protection des données et permet de construire une régulation commune sur l'ensemble du territoire de l'Union. Il implique cependant, d'une part, une adaptation de la législation nationale dans ce même délai ; d'autre part, que l'ensemble des acteurs s'emparent des nouveaux droits et obligations pour être prêts le 25 mai 2018. Dans ce contexte, la CNIL accompagne la mise en conformité des acteurs, leur propose des instruments de sécurisation juridique et travaille avec ses homologues à l'élaboration de lignes directrices.

UNE ÉVOLUTION SUBSTANTIELLE DU CADRE JURIDIQUE

La protection des données est actuellement régie par la directive 95/46/CE du 24 octobre 1995 et la loi du 6 janvier 1978. Si cette législation a fait la preuve de la solidité et de la pertinence de ses principes (principe de finalité, proportionnalité, légitimité du traitement, droits des personnes), elle nécessitait plusieurs adaptations à l'univers numérique. C'est le sens du règlement européen adopté en 2016.

De manière générale, le règlement européen comporte plusieurs avancées :

- **En termes de cohérence juridique**, le règlement constitue un texte unique, directement applicable dans l'ensemble de l'Union, ce qui devrait apporter une plus grande sécurité juridique aux entreprises. La directive de 1995 avait en effet fait l'objet de transpositions diverses dans les États membres.

- **En termes de champ d'application territorial :** la directive de 1995 est applicable aux « responsables de traitement » disposant d'un établissement ou de moyens de collecte dans l'Union européenne. Son application territoriale dépend donc de l'implantation des organismes qui traitent des données.

Le règlement s'appliquera dès lors que le responsable de traitement ou le sous-traitant sera établi sur le territoire de l'Union européenne (même critère) ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler ». En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet. La territorialité du droit européen se construit donc désormais autour de la personne.

- **En termes de champ d'application des responsabilités** la directive s'applique essentiellement – sauf sur certains aspects de sécurité informatique – aux « responsables de traitements », c'est-à-dire aux donneurs d'ordre, et non aux sous-traitants, qui ont, de fait, souvent la main sur le service et ses modalités. A la différence de la directive, le règlement « égalise » les obligations applicables aux sous-traitants et aux responsables de traitement, qui verront leur responsabilité engagée en cas de manquement.

Le règlement renforce les droits des personnes et les adapte à l'ère numérique. Il conforte la place de l'individu au cœur du système juridique, technique et éthique de la protection des données en Europe.

L'expression du consentement est également définie et renforcée : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

Le corollaire de cette évolution est **l'amélioration de l'information**, qui doit en tout état de cause être claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

Le règlement crée en outre un nouveau droit : le droit à la portabilité des données. Ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

La protection des enfants est renforcée : l'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

L'ensemble de ces éléments concourt à un même objectif : donner à la personne les moyens de mieux maîtriser le devenir de ses données (cf. l'analyse relative au droit à l'autodétermination informationnelle en page 40).

« Le droit européen s'appliquera chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet. La territorialité de ce droit se construit autour de la personne. »

FOCUS

LE DROIT À LA PORTABILITÉ
un droit effectif avec le règlement européen

Si le droit à l'autodétermination inscrit dans la loi française donne son sens aux droits issus de la loi Informatique et Libertés à l'ère numérique, le règlement européen sur la protection des données personnelles, qui entrera en application en mai 2018, conforte lui aussi le caractère central de la personne.

En premier lieu, le règlement européen repose sur un champ d'application territorial substantiellement différent de celui de la directive de 1995 actuellement applicable. Alors que la législation Informatique et Libertés ne s'appliquait jusqu'à présent qu'aux entités établies dans l'Union européenne – en France pour la loi française –, le règlement européen s'appliquera désormais dès lors qu'un résident européen sera substantiellement affecté par un traitement de données. Ce critère, dit du « ciblage », constitue une évolution profonde : désormais, la territorialité du droit européen de la protection des données se construit autour de la personne, et non plus seulement autour de l'acteur économique qui traite ses données.

En second lieu, le règlement introduit un nouveau droit qui participe de la volonté de redonner à l'individu la maîtrise de ses données : le droit à la portabilité. Toute personne pourra ainsi demander, pour de nombreux traitements et notamment tous ceux reposant sur un contrat ou sur le consentement de la personne, à récupérer les données qu'elle aura fournies à une entreprise, par exemple, sous un format lisible par une machine et aisément réutilisable, et pourra décider de les transmettre à une autre entité, sans limitations ni contraintes vis-à-vis du responsable de traitement initial.

L'objectif est double : du point de vue de la personne, à partir du moment où la donnée évolue dans un univers fluide, de *Big data*, l'enjeu n'est plus seulement d'accéder à ses données, mais de récupérer la main sur ses données. La portabilité est le corollaire de la mobilité numérique. D'un point de vue économique, redonner à l'individu la maîtrise de ses données, c'est rendre possible la réduction, à l'échelle individuelle, de l'asymétrie.

Cette approche, déjà mise en place pour les télécoms, est nouvelle en matière de données personnelles, et particulièrement adaptée à l'univers numérique : au lieu de reposer sur une correction prescriptive par le régulateur, elle repose sur les moyens d'action accordés à chaque individu.

L'effectivité de ce nouveau droit est essentielle : c'est ce qui explique que le G29 a retenu la portabilité parmi ses thèmes d'action prioritaires en 2016. Il a publié des lignes directrices en décembre 2016 sur le sujet, afin que les professionnels puissent garantir que ce droit sera effectivement effectif à compter du 25 mai 2018.

La CNIL suit et accompagne également les projets innovants permettant à l'individu de récupérer la maîtrise de ses données, et de décider par lui-même de les mettre à disposition de tiers. Ces initiatives, regroupées sous le terme de « *self-data* », connaissent un important développement.

« La portabilité est le corollaire de la mobilité numérique. »

Le règlement repose sur une logique de responsabilisation des organismes qui traitent des données, qu'ils soient responsables de traitements ou sous-traitants.

Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose prioritairement sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur (en France, la CNIL).

Cette notion de responsabilisation (*accountability*) se traduit tout d'abord par l'affirmation de deux principes : la prise en compte de la protection des données dès la conception du service ou du produit et par défaut (souvent connues sous leur nom anglais de *privacy by design* et by default). Concrètement, cela signifie qu'à la fois en termes d'organisation interne, de configuration des services ou des produits et de nature et volume de données traitées, les responsables de traitements devront mettre en place des processus et mesures permettant de garantir *ab initio* une protection optimale des données et une minimisation de la collecte.

Elle se traduit ensuite par la structuration interne de l'entité et la mise en place d'outils destinés à permettre, opérationnellement, le respect du règlement et la protection des données.

Les entités qui traitent des données devront ainsi :

- **Se doter, dans un certain nombre de cas, d'un délégué à la protection des données**, véritable chef d'orchestre de la conformité en interne, qui exercera une mission de conseil et de contrôle interne en la matière. Les administrations devront obligatoirement en désigner un ; de très nombreuses entreprises également. On relèvera que le délégué est le successeur, aux prérogatives et missions renforcées, du Correspondant Informatique et Libertés (le CIL) dont plus de 17 700 organismes sont d'ores et déjà dotés en France (contre 8000 il y a cinq ans) ;

> « Les responsables de traitement devront mettre en place des processus et mesures pour garantir une protection optimale des données et une minimisation de la collecte. »

- **Tenir un registre** des traitements mis en œuvre avec une documentation complète, facilitant ainsi l'information des personnes et l'éventuel contrôle par la CNIL ;

- **Mener des études d'impact sur la vie privée (EIVP)** pour les traitements à risque, sous le contrôle du régulateur Pour tous les traitements à risques, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et des traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

- **Notifier les failles** de sécurité (aux autorités et personnes concernées)

Ils pourront également adhérer à des **codes de bonne conduite** approuvés par les CNIL, et faire certifier leurs traitements par des tiers certificateurs, ou encore bénéficier de labels.

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

Le règlement adapte la régulation en instaurant une nouvelle gouvernance de la régulation de la protection des données.

Afin d'apporter une plus grande sécurité juridique à l'échelle du continent, le règlement instaure une nouvelle gouvernance européenne de la protection des données, qui repose sur l'étroite coopération entre les autorités nationales. Concrètement, la plupart des missions du régulateur qu'est la CNIL interviendront donc dans un environnement fortement européanisé.

Un contrôle a priori sensiblement simplifié

Les responsables de traitements n'auront plus à effectuer de déclarations (100 000 déclarations par an à la CNIL, mobilisant moins de deux postes) ; les traitements les plus sensibles devront faire l'objet d'une étude d'impact sur la vie privée par le responsables de traitements, avant d'être soumis, dans certaines conditions, à la CNIL pour qu'elle puisse, le cas échéant, s'opposer au traitement ou demander des garanties supplémentaires. Enfin, pourront demeurer certains cas d'autorisations, qui devront être déterminés par la loi.

Une partie des procédures européanisée

Dès lors qu'un traitement sera transnational, l'ensemble des décisions et outils de conformité devra être approuvé conjointement par les autorités concernées : il en ira ainsi des suites données

aux études d'impact sur la vie privée, de l'approbation des codes de bonne conduite, de la certification ou de la délivrance de labels.

Un mécanisme « plaintes-contrôles sanctions » maintenu en aval, mais renforcé et européanisé

- **Renforcé**, puisque les sanctions pourront s'élever, pour les manquements les plus graves, à 4% du chiffre d'affaires mondial, contre 3 millions d'euros depuis la loi pour une République numérique (150 000 auparavant). Le montant des sanctions doit être apprécié à l'aune de cette assiette territoriale : c'est le montant maximum pour une sanction unique applicable sur l'ensemble du territoire de l'Union. Ce montant tient compte en outre de l'évolution du poids économique des données personnelles, véritable actif financier dans l'économie numérique.

- **Européanisé**, puisque pour l'ensemble des traitements transnationaux, les autorités de protection des données « codécideront » de la conformité ou au contraire de la sanction de l'organisme contrôlé ou mis en cause. Plus que le montant, c'est en effet l'européanisation des procédures et des décisions qui change considérablement les conditions d'intervention de la CNIL en matière répressive.

Concrètement, dès qu'un traitement sera transnational – donc qu'il concernera les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernés seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre. Toutefois, afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, le règlement européen

> « Les entreprises devront désigner leur autorité chef de file, qui sera leur interlocuteur unique mais qui coopérera avec les autres autorités de protection. »

prévoit un mécanisme de « **guichet unique » (one-stop-shop).** En pratique, les entreprises devront désigner, pour leurs différents traitements, un ou plusieurs « établissements principaux ». Ceux-ci auront alors pour interlocuteur la « CNIL » de leur pays d'établissement, qui sera leur unique interlocuteur, au nom de l'ensemble des CNIL des pays concernés, pour le ou les traitements en question.

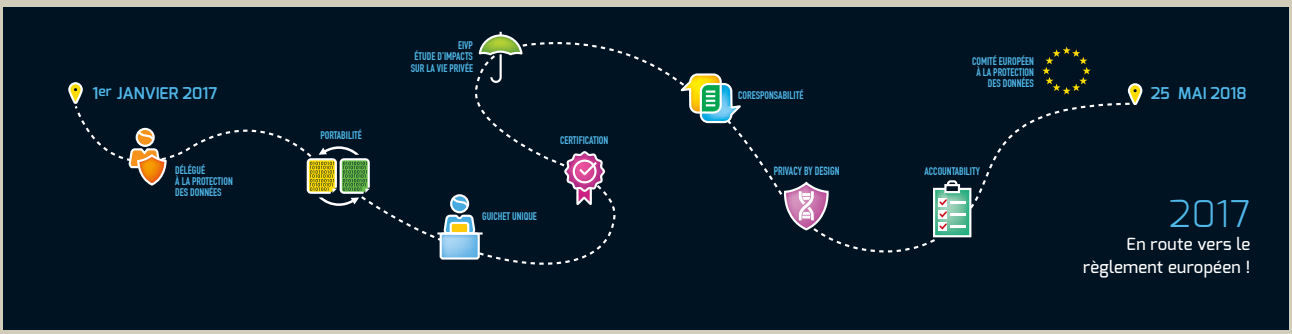
Cette autorité dite « chef de file » ne décidera cependant pas seule : si elle est l'interlocuteur de référence de l'entreprise, elle devra toutefois coopérer avec les autres autorités de protection des données concernées. L'autorité « chef de file » propose ainsi les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD (comité européen de la protection des données), le groupe des « CNIL » européennes, qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ». L'autorité chef de file doit alors prendre une mesure conforme à cet avis et la notifier à l'entreprise concernée.

508

millions
c'est le nombre de personnes habitant au sein de l'Union Européenne qui vont voir leurs droits renforcés en 2018.

L'accompagnement de la mise en conformité

Corollaire de la responsabilisation des organismes, la CNIL développe l'accompagnement de la conformité notamment en répondant à de très nombreuses demandes de conseils. Cette dimension de l'activité a connu une forte progression ces dernières années, et correspond plus aux mutations de l'univers numérique. Face à des technologies très évolutives, mais aussi aux enjeux de cybersécurité, les entreprises sont de plus en plus amenées à solliciter la CNIL 'au fil de l'eau', et à lui adresser des demandes de conseils. D'ores et déjà, la CNIL reçoit plusieurs milliers de demandes de conseils par an, et sa permanence téléphonique traite 160 000 appels par an de particuliers ou de professionnels. .



VERS UNE « NOUVELLE LOI INFORMATIQUE ET LIBERTÉS »

Le règlement européen comporte 57 mentions ou renvois au « droit des États membres », donc au droit national. En outre, parallèlement au règlement, a été adoptée une directive applicable aux fichiers en matière de sécurité publique et de recherche et répression des infractions pénales (dite « police-justice). Il est donc indispensable que le Législateur, en France, procède à une adaptation profonde de la loi Informatique et Libertés pour tenir compte de cette évolution et parachever l'environnement réglementaire, et transposer la directive « police-justice »

C'est pour cette raison que le Gouvernement a engagé un travail de refonte de la loi Informatique et Libertés, piloté par le ministère de la Justice dans le cadre de groupes de travail auxquels participe la CNIL.

La future loi Informatique et Libertés devra donc contenir des dispositions générales (principes, règles, fonctionnement, pouvoirs de la Commission, procédures ; des dispositions spécifiques pour les matières pour lesquelles le règlement, applicable, renvoie le soin aux États membres de prendre des mesures spécifiques ou complémentaires ; des dispositions dérogatoires pour les fichiers de sécurité publique, qui devraient être quasi-conformes aux dispositions actuelles qui permettent de satisfaire les obligations posées par la directive.

Concrètement, la loi devrait comporter plusieurs types de dispositions : abrogation, nouvelles procédures, renvoi au droit des États membres

La loi devrait tout d'abord **abroger une série d'articles** dont la substance est reprise par le règlement ou qui ne peuvent pas coexister avec celui-ci. Tel est notamment le cas de la plupart des articles relatifs aux définitions, règles, principes et conditions de licéité – à l'exception notable de l'article 1er de la loi Informatique et Libertés qui conserve sa pertinence et une forte valeur principielle et symbolique – ainsi que de la plupart des dispositions relatives aux droits des personnes et aux obligations des entreprises.

La loi devrait ensuite **redéfinir les procédures applicables à la CNIL impactées par le règlement, notamment en matière répressive, afin de prévoir l'européanisation des procédures.**

Le Législateur se prononcera également sur les règles applicables dans les matières pour lesquelles le règlement renvoie au droit des États membres.

Le règlement fixe le cadre général applicable à l'ensemble des traitements de données à caractère personnel. Toutefois, compte tenu des spécificités de certaines données, ou de l'imbrication entre le droit de la protection des données et d'autres pans du droit (santé, etc.), le règlement européen renvoie, dans plusieurs hypothèses, au droit national.

Les renvois du règlement au droit national sont assez divers, rendant complexe une présentation synoptique. Le chapitre IX a pour objet d'énumérer des champs d'intervention dans lesquels les États membres peuvent préciser ou déroger au règlement : traitements journalistiques, traitements et accès du public aux documents officiels, traitement du NIR, traitement des données au travail, traitement des données à des fins de recherche historique, scientifique ou statistique, obligations de secret. Mais il existe aussi des dispositions disséminées, qui renvoie le soin aux États membres de fixer les mesures et garanties appropriées ou de compléter les règles existantes.

Les principales dispositions figurent :

- à l'article 9, relatif aux données sensibles : « Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé » ;
- à l'article 10, relatif aux données relatives aux infractions ou condamnations pénales ;
- à l'article 36, sur les pouvoirs des autorités de contrôles sur les fichiers d'intérêt public ;

La loi devra enfin conserver un chapitre relatif à la composition, au fonctionnement et aux missions de la CNIL, qui vont d'ailleurs au-delà du champ du règlement européen.

« Un projet de loi devra être déposé au Parlement au plus tard en juin 2017 pour garantir à la France une application du règlement en mai 2018. »

LA MISE EN ŒUVRE DU RÈGLEMENT EUROPÉEN PAR LES RÉGULATEURS : L'ACTION DE LA CNIL ET DU G29

La CNIL a, dès 2012, anticipé la mise en œuvre du règlement européen, en développant son activité d'accompagnement de la mise en conformité. Au-delà de l'accompagnement des CIL, elle est ainsi la première en Europe à avoir développé une activité de labellisation et des packs de conformité.

Par ailleurs, la CNIL diffuse également une information large sur le règlement afin de répondre aux questions des professionnels : outre une présentation générale du règlement sur son site et un dispositif dédié d'accompagnement des délégués à la protection des données, elle va publier, de février 2017 à mai 2018 au moins, des réponses aux questions les plus fréquemment posées sur le règlement européen afin d'assurer une sécurité juridique maximale aux entreprises et administrations qui dialoguent avec elle.

L'action de la CNIL s'insère également dans le cadre plus général de celui du G29, qu'elle préside.

Les lignes directrices, une boussole pour les professionnels

Le G29, futur « comité européen de la protection des données », a en effet adopté un plan d'action ambitieux autour de trois axes :

- La publication de lignes directrices destinées à unifier et clarifier l'interprétation de dispositions essentielles du règlement européen ;
- La mise en place du nouveau modèle de gouvernance et de coopération entre autorités de protection.
- La création de l'organisme communautaire (CEPD) succédant au G29.

En 2016, quatre sujets avaient été identifiés comme prioritaires : le droit à la portabilité, le délégué à la protection des données, les analyses d'impact et la certification.

Les deux premiers thèmes ont fait l'objet de lignes directrices publiées fin 2016. Le G29 a lancé un appel à commentaires en décembre 2016 destiné à enrichir ces documents et publiera leur version définitive au printemps 2017.

Par ailleurs, les prochaines lignes directrices en cours d'élaboration portent sur le consentement, le profilage et les notifications de failles de sécurité. L'ensemble de ces lignes directrices devrait être publié courant 2017.

Les lignes directrices sont élaborées au terme d'une large concertation. C'est ainsi que la CNIL a systématiquement ouvert une consultation publique sur les différents thèmes abordés, afin de recueillir les questions concrètes ou propositions de bonnes pratiques des

professionnels. Les premiers thèmes soumis à consultation à l'automne 2016 ont ainsi suscité plus de 500 contributions particulièrement fournies.

Cette première phase de consultation publique est également suivie d'ateliers opérationnels avec des professionnels.

Le 26 juillet 2016, le G29 a ainsi organisé à Bruxelles un FabLab intitulé : *GPDR : from concepts to operational toolbox, DIY!* Cette journée a réuni des représentants de la société civile, des fédérations professionnelles, des universitaires et des personnels des autorités de protection des données européennes au sein d'ateliers collaboratifs. Les 4 thèmes prioritaires du plan d'action 2016 ont orienté les interventions.

L'objectif de cette journée collaborative était de co-construire avec les acteurs de terrain la fameuse « boîte à outils ». Les échanges et propositions de cette journée ont permis au G29 d'alimenter les différents groupes de travail en charge de ces 4 thèmes et de décliner les principes du Règlement en mesures opérationnelles correspondant aux besoins et attentes des principaux acteurs concernés par la mise en œuvre du Règlement.

Ce sont près de 100 participants qui ont participé au FabLab en 2016, ont alimenté les travaux et enrichi les débats. Face au succès rencontré une seconde édition a été prévue au printemps 2017 sur les nouveaux thèmes retenus.

Du G29 au comité européen de la protection des données

A compter du 25 mai 2018, les autorités devront se prononcer conjointement dans les cas de traitements transfrontières. Elles ont donc défini, au cours de l'année 2016, les modalités de leur future coopération autour des nouveaux mécanismes d'assistance mutuelle, de contrôles conjoints, d'autorité chef de file et de guichet unique. Des lignes directrices sur ce sujet ont été publiées fin 2016 et sont ouvertes à commentaires jusqu'en début 2017. La CNIL a également été très impliquée sur ces outils essentiels pour l'efficacité de la régulation et la sécurité juridique des acteurs.

Quant au G29, il sera remplacé par le Comité européen de la protection des données (ou « CEPD »). Ce nouvel organisme aura des missions élargies par rapport à celles confiées au G29 par la directive de 1995. Il sera en effet en charge du contrôle de la cohérence. Cette mission nouvelle et centrale dans le règlement vise à assurer une application uniforme des droits et obligations prévus par le texte. Le CEPD sera le régulateur européen et produira la doctrine européenne sur tout sujet relatif à la protection des données. Dans le cadre du règlement des litiges, le CEPD aura le pouvoir de prendre des décisions contraignantes en cas de conflits entre autorités.

Le règlement au-delà des frontières de l'UE

L'adaptation à ce nouveau cadre demande à la fois de la souplesse, de la créativité et une ouverture sur les systèmes qui existent en dehors de l'Union Européenne. En effet, le Règlement européen aura également un impact important pour les États tiers à l'Union européenne puisque les entreprises établies en dehors de nos frontières mais qui ciblent le marché européen devront respecter l'ensemble des principes du Règlement.

Le G29 a en ce sens créé de nouveaux liens avec la région Asie Pacifique en mettant en place un lien permanent entre le G29 et l'APPA (réseau des autorités de protection de données de l'Asie Pacifique).

Les entreprises établies en dehors de l'Union Européenne qui ciblent le marché européen devront respecter le Règlement.

À SUIVRE

Les 3 nouvelles thématiques inscrites au plan d'action 2017 du G29 pour le premier semestre seront ouvertes à la consultation publique en mars 2017.

Une consultation en ligne sur le site de la CNIL de février à mars portera sur le profilage, le consentement et la notification des failles de sécurité. Un atelier sera organisé à Bruxelles à la suite de cette consultation.

La CNIL a participé en 2016

- **Aux 9 groupes de travail réunissant des experts des autorités de protection des données**
- **À la réflexion portant sur les 11 sujets identifiés comme prioritaires pour se préparer au Règlement en 2016**
- **À la rédaction des 3 lignes directrices publiées en fin d'année**

Biométrie : la CNIL précise sa doctrine

L'année 2016 a été l'occasion pour la CNIL de préciser son approche en matière de traitements biométriques. Elle a ainsi procédé à une refonte de sa doctrine en matière de contrôle d'accès biométrique et précisé sa position quant aux dispositifs biométriques utilisés par les particuliers dans un cadre privé. Elle a enfin contribué au débat public sur la mise en œuvre du fichier TES relatif aux cartes d'identité et aux passeports biométriques. Toutes ces actions et positions répondent à un double objectif : permettre aux personnes de mieux maîtriser leurs données et les enjeux des systèmes biométriques ; anticiper l'application du règlement européen, qui obligera les responsables de traitement à mettre en œuvre de nouvelles mesures de protection concernant ces fichiers.

LES DONNÉES BIOMÉTRIQUES DOIVENT FAIRE L'OBJET D'UNE VIGILANCE PARTICULIÈRE

5 754
ENGAGEMENTS

1 372
engagements AU-007 biométrie : contour de la main sur lieu de travail

1 899
engagements AU-008 biométrie : empreinte digitale sur lieu de travail

1 038
engagements AU-009 biométrie : accès aux cantines scolaires

1 182
engagements AU-019 réseaux veineux de la main sur lieu de travail

174
engagements AU-027 contrôles d'accès aux ordinateurs portables

62
engagements AU-052 contrôles d'accès lieu de travail avec maîtrise de la personne sur son gabarit

27
engagements AU-053 contrôles d'accès lieu de travail avec maîtrise de la personne en base

Comme la CNIL le rappelle régulièrement dans ses délibérations, les données biométriques ne sont pas des données à caractère personnel comme les autres. Elles résultent d'un traitement technique bien particulier des caractéristiques physiques, physiologiques ou comportementales des personnes et permettent de reconnaître celles-ci automatiquement.

Utilisée initialement aux seules fins d'identification judiciaire, la biométrie est aujourd'hui intégrée à de nombreux actes de la vie quotidienne nécessitant une authentification préalable des personnes. Il peut s'agir du contrôle d'accès à des locaux professionnels, à des ordinateurs, à des services en ligne, mais aussi du contrôle usuel d'identité lors du passage aux frontières ou encore, dans certains pays, d'un moyen de reconnaître les utilisateurs de télévisions connectées, de remplacer les clés, de sécuriser les paiements électroniques ou de sécuriser la circulation des données médicales.

La biométrie est souvent présentée comme une alternative ergonomique et efficace à l'usage de mots de passe trop nombreux et trop longs à retenir. Pour autant, les données biométriques permettent à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir. Leur traitement génère donc des risques importants pour les droits et libertés des personnes concernées.

En effet, à la différence d'un mot de passe, il n'est pas possible de se défaire d'une caractéristique biométrique ou de la modifier. Le détournement de données biométriques (par exemple, en reproduisant une empreinte digitale et en la réutilisant à l'insu de la personne concernée) a dès lors des conséquences immédiates et définitives pour la personne concernée : elle ne pourra plus utiliser la caractéristique biométrique compromise pour s'identifier de manière fiable et la donnée biométrique ainsi récupérée pourra être utilisée pour usurper son identité.

Les traitements biométriques ne sont donc pas des traitements anodins et nécessitent un encadrement strict. C'est pourquoi le Législateur a prévu, dès 2004, un contrôle renforcé de la CNIL sur ces traitements qui doivent faire l'objet d'une autorisation préalable de la CNIL s'agissant du secteur privé et d'un décret en Conseil d'État, pris après avis motivé et publié de la CNIL, pour les traitements mis en œuvre pour le compte de l'État.

Le règlement européen, applicable à compter de mai 2018, a consacré le caractère particulier de ces données en les qualifiant de données « sensibles », au même titre que les données concernant la santé, les opinions politiques ou les convictions religieuses, dont le traitement est par principe interdit sauf dans certains cas limitativement énumérés.

« Des données pas comme les autres, qualifiées désormais de sensibles dans le règlement européen. »

UN NOUVEL ENCADREMENT DES DISPOSITIFS BIOMÉTRIQUES

Depuis 2004, la CNIL a adopté plusieurs autorisations uniques et de nombreuses autorisations ou avis spécifiques en matière de traitements biométriques. Historiquement, elle a fondé sa doctrine en la matière sur la distinction entre les biométries dites « à trace » et les biométries dites « sans trace ».

Certaines caractéristiques physiques laissent en effet des traces (par exemple, une empreinte digitale laissée sur un verre) qui peuvent être facilement récupérées à l'insu des personnes concernées. Le traitement biométrique de ces données présente donc des risques élevés pour les personnes. Partant de ce constat, la Commission a systématiquement privilégié les dispositifs permettant aux personnes de garder le contrôle sur leurs données biométriques, qui devaient dès lors être conservées sur un support individuel (badge, clé USB, etc.) détenu par la seule personne concernée. La centralisation de tous les gabarits biométriques dans des serveurs gérés par le responsable du traitement biométrique, n'était admise qu'exceptionnellement en présence d'un « fort impératif de sécurité ».

A l'inverse, les biométries ne laissant pas de trace, par exemple le réseau veineux de la main, étaient considérées comme moins risquées et les données pouvaient donc être centralisées dans une base de données.

Toutefois, depuis plusieurs années, de nombreux outils se sont développés pour permettre de capter et de reproduire les caractéristiques physiques des personnes, aisément et à bas coût. Par exemple, s'agissant de la reconnaissance faciale, le développement des caméras de vidéosurveillance et de vidéoprotection, ainsi que l'exposition grandissante de photographies sur différents sites internet génèrent de nombreuses « traces numériques » du visage des personnes. Un constat identique peut être fait s'agissant de la reconnaissance vocale et du développement des dispositifs d'enregistrement de la voix, ou encore s'agissant de la reconnaissance du réseau veineux et des possibilités de captation de ces caractéristiques par caméra infrarouge.

La CNIL a donc décidé d'adapter ses lignes directrices, en partant du constat que, désormais, toutes les caractéristiques biométriques peuvent être considérées comme laissant des traces. A ce titre, toutes les biométries présentent des risques élevés pour les personnes concernées.

Deux nouvelles autorisations uniques fixant la position de la CNIL

Le 30 juin 2016, la CNIL a adopté deux autorisations uniques[1], abrogeant et remplaçant les décisions précédemment adoptées en matière de contrôle d'accès sur les lieux de travail[2]. Ces décisions rappellent à titre général que le contrôle d'accès biométrique ne doit pas devenir courant et se substituer, sans justification, à d'autres dispositifs standards moins intrusifs pour les personnes (badge, clé, gardiennage, etc.). Elles ne se basent plus sur des distinctions entre les biométries utilisées, ni non plus, à titre principal, entre stockage en base et stockage sur un support individuel : elles favorisent les dispositifs garantissant le contrôle des individus sur leurs données biométriques et conformes au principe de minimisation des données.

L'autorisation n° 52 vise deux possibilités pratiques permettant de respecter ces principes. En premier lieu, la personne concernée peut se voir confier un support de stockage de son gabarit biométrique, afin de réduire les risques de détournement et l'impact d'une usurpation si le support est subtilisé : en cas de perte ou de vol du support individuel, seule la donnée concernée est compromise et non les gabarits de l'ensemble des personnes soumises au contrôle d'accès.

En second lieu, et si la détention d'un support dédié au seul stockage du gabarit n'est pas adaptée à l'architecture et au contexte d'exploitation du dispositif, le gabarit peut être conservé dans les serveurs de la société sous une forme le rendant inexploitable en l'absence d'intervention de la personne concernée. En pratique, le gabarit doit être protégé par un secret ou un élément que la personne concernée est seule à détenir et qu'elle peut utiliser lors de son authentification.

« Les nouvelles autorisations favorisent les dispositifs garantissant le contrôle des individus sur leurs données biométriques. »

1 Délibération n° 2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052) et Délibération n° 2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)

2 Délibération n° 2006-101 du 27 avril 2006 portant autorisation unique (007) pour la reconnaissance du contour de la main ; délibération n° 2006-102 du 27 avril 2006 portant autorisation unique (008) pour la reconnaissance de l'empreinte digitale ; délibération n° 2009-316 du 7 mai 2009 portant autorisation unique (019) pour la reconnaissance du réseau veineux de la main ; délibération n° 2011-074 du 10 mars 2011 portant autorisation unique (027) pour la reconnaissance de l'empreinte digitale permettant d'accéder à des ordinateurs portables

L'autorisation n° 53 couvre quant à elle les cas dans lesquels il n'est pas possible de mettre en place les préconisations de l'autorisation n° 52. A titre d'exemple, une centrale nucléaire peut nécessiter, pour des questions de sécurité et de capacité à réagir en situation d'urgence, de centraliser les gabarits des personnes habilitées à accéder aux locaux.

Dans ces cas, la société devra démontrer que son besoin ne peut être raisonnablement satisfait, d'une part, sans traitement biométrique et, d'autre part, sans le coupler à un stockage en base des gabarits. Après avoir documenté la pertinence de son choix, le responsable du traitement devra également respecter un niveau d'exigence élevé en adoptant des mesures permettant de limiter au maximum les risques posés par le traitement en matière de vie privée.

Les dispositifs biométriques offerts aux particuliers

La révision de ses lignes directrices en matière de biométrie imposait également que la CNIL précise sa position quant aux dispositifs biométriques utilisés par les particuliers dans un cadre privé. Le contrôle d'accès par biométrie rencontre en effet un succès croissant auprès des particuliers désireux de simplifier notamment le déverrouillage des smartphones, l'accès aux applications mobiles, l'usage des moyens de paiement, etc. Ce phénomène s'est notamment accéléré avec l'introduction de la fonctionnalité d'authentification par empreinte digitale, en complément du code d'accès, dans les derniers modèles des principaux fabricants de téléphones.

À RETENIR

Les responsables du traitement voulant se conformer à ces autorisations devront donc démontrer, au moyen d'une documentation étayée, que le contexte de mise en œuvre du contrôle d'accès justifie le recours à un traitement biométrique et que toutes les mesures sont prises, notamment du point de vue technique, pour limiter les risques soulevés par l'utilisation de ces données.

La CNIL a dès lors clarifié le cadre juridique applicable à ces dispositifs et a fixé les conditions de mise en œuvre des traitements biométriques configurés et mis en œuvre par des professionnels respectueuses de la protection des données.

1ER CAS : La CNIL considère que les traitements mis en œuvre à l'initiative et sous le seul contrôle de la personne concernée sont couverts par l'exception dite « domestique » prévue à l'article 2 de la loi Informatique et Libertés.

Ainsi, les organismes utilisant une reconnaissance biométrique intégrée à leurs appareils n'ont pas besoin de demander une autorisation à la CNIL, si les dispositifs concernés répondent à l'ensemble des critères suivants :

- **L'utilisateur utilise ce dispositif à titre privé,** grâce à ses propres données biométriques, pour déverrouiller son téléphone ou accéder aux applications qu'il a téléchargées de son propre chef ;
- **L'utilisateur décide seul d'utiliser l'authentification biométrique intégrée dans son appareil :** cela exclut toute authentification biométrique imposée par son employeur, si l'appareil lui a été fourni dans le cadre de ses activités professionnelles ; cela suppose en outre que les fournisseurs d'application proposent un mode d'authentification alternatif à la biométrie (par exemple, la saisie d'un code), sans contrainte additionnelle.
- **Le gabarit biométrique est stocké dans l'appareil,** dans un environnement cloisonné et n'est pas accessible ou transmis à l'extérieur : cela exclut les dispositifs biométriques envoyant le gabarit dans une base de données distante, ainsi que toute possibilité d'intervention d'un organisme extérieur (fournisseur de l'appareil ou d'une application par exemple) sur les données biométriques ;
- **Le gabarit biométrique est stocké de manière chiffrée,** à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art.

Les dispositifs fonctionnant dans ces conditions intègrent par défaut des mécanismes protecteurs de la vie privée. En effet, la donnée biométrique ne risque pas d'être récupérée et détournée par un organisme extérieur si elle reste dans un « compartiment » fermé, à l'intérieur de l'appareil, et si cet appareil reste sous le contrôle de son utilisateur. De plus, le choix de recourir à l'authentification biométrique appartient au principal intéressé et n'est pas lié à une contrainte extérieure. Cette limitation au seul usage domestique permet d'exclure l'application de la loi Informatique et Libertés.

Dans ce cas, le fournisseur d'une application ou d'un service recourant à ce type de dispositif n'est pas responsable du traitement de données biométriques correspondant, mais il reste toutefois responsable de la sécurité de son application. À ce titre, il doit s'assurer de la fiabilité de la solution d'authentification biométrique avec laquelle son application peut échanger, en vérifiant notamment :

- que les taux de faux positifs et de faux négatifs propres à la solution biométrique utilisée sont adaptés au niveau de sécurisation du contrôle d'accès souhaité (par exemple, une application ou un service sensible, pour lequel un contrôle d'accès strict est nécessaire, nécessitera un taux de faux positifs très faible) ;
- que la solution biométrique utilisée repose sur un capteur résistant aux attaques considérées comme triviales en l'état de l'art (telles que, à l'heure actuelle, l'utilisation d'une photographie pour duper la reconnaissance faciale ou l'utilisation d'une empreinte imprimée à plat pour la reconnaissance d'empreinte digitale, la détection de faux doigts) ;
- que le nombre d'essais d'authentification est limité.

2ÈME CAS : Si l'ensemble de ces conditions ne sont pas respectées, en particulier si la reconnaissance biométrique proposée à la personne sur son appareil fonctionne en interaction avec des serveurs distants maîtrisés par un organisme tiers, l'organisme en question (fournisseur de l'application, de l'appareil, etc.) doit effectuer une demande d'autorisation auprès de la CNIL.

Dans ce cas, les lignes directrices formulées dans les autorisations uniques précitées ont vocation à s'appliquer bien qu'il ne s'agisse pas de contrôle d'accès sur les lieux de travail : les responsables de ces traitements proposés aux particuliers doivent prendre les mesures techniques nécessaires à la protection de la confidentialité des gabarits et privilégier les systèmes permettant de préserver la maîtrise de l'utilisateur sur son gabarit.

EXEMPLE

La CNIL a autorisé la mise en place d'un traitement de reconnaissance vocale par La Banque Postale permettant de déclencher le pré-remplissage de formulaire de paiement en ligne. La voix est en effet stockée dans les serveurs de la Banque Postale sous une forme chiffrée au moyen d'une clé ou d'un secret placé sous le seul contrôle de la personne concernée. Dans ces conditions, cette donnée est inexploitable sans l'accord de la personne, que ce soit par La Banque Postale ou par des tiers[3].

La CNIL a autorisé la mise en place d'un service d'authentification biométrique par l'association Natural Security Alliance en juillet dernier, accessible depuis une application à télécharger sur les smartphones. Le gabarit du doigt des personnes est stocké sous forme chiffrée, chaînée et révocable dans l'application et peut être ensuite comparé, via une communication sans contact, avec le doigt apposé sur des lecteurs biométriques distribués par l'association à différents opérateurs souhaitant utiliser ce type d'authentification. Ici encore, l'ensemble du dispositif a été conçu pour préserver le contrôle de l'utilisateur sur ses données biométriques, respecter sa liberté de choix et limiter au minimum les risques pour sa vie privée[4].

La prise en compte anticipée du règlement européen

Pour rappel, tous les organismes devront avoir mis en conformité leurs traitements avec le règlement européen d'ici mai 2018. A cette date, ils ne seront plus tenus d'obtenir l'autorisation préalable de la CNIL pour opérer des traitements biométriques. Ils devront en revanche documenter les différentes caractéristiques de leurs traitements et être en mesure de démontrer leur proportionnalité ainsi que le respect des principes de protection des données par défaut et dès la conception. Ils devront également réaliser une analyse d'impact relative à la protection des données, si leur traitement biométrique est réalisé à grande échelle.

La logique de contrôle a priori liée au système d'autorisation préalable valable aujourd'hui s'inverse donc pour passer à un système de contrôle a posteriori, le responsable du traitement étant notamment tenu :

- de documenter son traitement et les mesures de mise en conformité adoptées ;
- dans certains cas, de mener une analyse d'impact conforme à l'article 35 du règlement ;
- et de tenir l'ensemble de cette documentation à disposition de la CNIL, notamment en cas de contrôle a posteriori de ces traitements.

C'est également dans cette optique qu'ont été élaborées les nouvelles lignes directrices de la CNIL concernant les traitements biométriques mis en œuvre aux fins du contrôle d'accès. Ces exigences sont en effet intégrées dans les autorisations uniques n° 52 et n° 53 et se traduisent par :

- des modalités de stockage du gabarit et des mesures techniques applicables à la donnée biométrique, tout au long de son cycle de vie, limitant les risques pour la vie privée, en accord avec le principe de respect de la vie privée dès la conception ;
- l'obligation du responsable du traitement de décrire son traitement et de documenter son évaluation de la nécessité et de la proportionnalité de sa mise en place, des risques générés pour les droits et libertés des personnes concernées, ainsi que les mesures envisagées pour traiter ces risques et se conformer au règlement, sur le modèle des études d'impact sur les données personnelles imposées par le règlement.

Afin de guider les responsables du traitement, les autorisations uniques détaillent les mesures permettant de limiter les impacts au regard des risques identifiés par la CNIL au cours des dernières années. Ainsi, par le biais de ces autorisations, la CNIL met à disposition des responsables de traitement peu familiers de l'exercice un premier exemple d'analyse d'impact, réunissant les conditions inscrites dans le règlement européen. La même approche devra guider l'offre aux particuliers de dispositifs d'authentification biométrique.

Le cas des traitements biométriques mis en œuvre par l'État

La même approche guide la CNIL lorsqu'elle se prononce sur des projets de traitements biométriques mis en œuvre pour le compte de l'État. Ces dernières années, elle s'est ainsi prononcée à plusieurs reprises sur des dispositifs biométriques de contrôle d'accès aux lieux de travail mis en œuvre dans le secteur public. Dès lors que ces traitements permettaient la maîtrise de leurs données par les employés concernés, comme par exemple la conservation d'éléments biométriques sur un support individuel, et étaient justifiés par la nécessité d'un contrôle d'accès renforcé, la CNIL a émis des avis globalement favorables sur les projets de décret en Conseil d'État dont elle était saisie[5].
De même, en matière de contrôle d'accès, non des employés mais des usagers, la CNIL a utilisé la même grille de lecture que celle appliquée au secteur privé. Concernant le traitement PARAFE par exemple, elle a estimé que le dispositif

3 Pour plus d'information, se référer à la Délibération n° 2016-037 du 18 février 2016 autorisant La Banque Postale à mettre en œuvre un système d'authentification des titulaires de cartes bancaires par reconnaissance vocale.

4 Pour plus d'information, se référer à la Délibération n° 2016-212 du 7 juillet 2016 autorisant l'association Natural Security Alliance à mettre en œuvre un système d'authentification biométrique basé sur la détention d'un ordiphone ou d'un support individuel contenant une application, placé sous le contrôle des personnes concernées, aux fins d'accès à des services.

mis en œuvre par le ministère de l'intérieur était conforme à la protection des données, qu'il s'agisse de l'utilisation des empreintes digitales des voyageurs[6] puis de leur photographie aux fins de reconnaissance faciale de ces derniers[7], dès lors que le système repose sur le volontariat des personnes concernées et s'appuie sur la conservation de ces éléments biométriques dans un support dont elles ont l'usage exclusif.

Le consentement des personnes concernées peut néanmoins, à l'évidence, être écarté dans le cadre de certaines finalités poursuivies par des traitements biométriques, de même que la nécessité de conserver les identifiants biométriques sous le contrôle des personnes concernées. Les fichiers de police technique et scientifique, tels que le Fichier Automatisé des Empreintes Digitales (FAED), dont un des buts est précisément d'identifier des personnes dont l'identité n'est pas connue, constitue l'exemple typique d'une telle utilisation de données biométriques. De ce point de vue, l'approche retenue par la CNIL est également la même dans le secteur public et dans le secteur privé : certaines finalités et certains contextes nécessitent, par nature, une conservation en base des éléments biométriques mais des mesures compensatoires, en termes de sécurité technique en particulier, doivent être mises en œuvre afin d'atténuer les risques soulevés par l'utilisation de ces données.

C'est également la même approche qui a conduit la CNIL à adopter son avis sur le fichier TES[8].

Les traitements relatifs aux passeports biométriques et aux cartes d'identité biométriques ont fait l'objet de nombreuses délibérations de la CNIL[9], ainsi que de décisions du Conseil constitutionnel, du Conseil d'État et de la Cour de justice de l'Union européenne qui ont clairement délimité les possibilités d'usage de tels fichiers. Le système TES créé par décret du 28 octobre 2016[10], traitement commun aux passeports et aux cartes nationales d'identité ayant vocation à regrouper l'ensemble des documents numérisés et données personnelles collectées dans le cadre de la procédure d'établissement et de délivrance de ces titres, et notamment l'image numérisée du visage et les empreintes digitales des demandeurs, en a d'ailleurs tenu compte en interdisant, juridiquement (par une mention expresse dans le décret) et techniquement (l'accès aux empreintes n'est théoriquement possible que sur la base d'éléments d'identité, et non l'inverse), l'identification biométrique des demandeurs de titres.

Néanmoins, la CNIL a estimé dans son avis que le système projeté n'était pas, en l'état des éléments dont elle disposait et au vu de ses exigences traditionnelles en matière de traitements biométriques, entouré de garanties suffisantes permettant d' assurer un haut niveau de protection des données.

En effet, la fusion en une base unique de l'ensemble de ces éléments conduit à un changement d'ampleur et de nature considérables : ce traitement a vocation à comporter les données biométriques de la quasi-totalité de la population française, ce qui constitue une situation inédite. Or, les alternatives à la constitution d'une telle base de données n'ont pas été suffisamment étudiées et expertisées, contrairement aux exigences posées par la CNIL pour les traitements biométriques mis en œuvre par le secteur privé. Ainsi, aucune étude d'impact sur la vie privée n'a été communiquée à la CNIL et aucune justification particulière n'a été avancée pour écarter la conservation des données biométriques sur un support individuel exclusivement détenu par la personne concernée.

De même, certaines mesures de sécurité que la CNIL exige s'agissant du secteur privé n'ont pas été prévues pour le système TES. La conservation de données biométriques brutes soulevant des risques que l'utilisation de gabarits permettrait de prévenir, la Commission a recommandé que ces données soient remplacées par des gabarits ou tout autre dispositif technique permettant de renforcer la protection et la sécurité du système.

Enfin, la CNIL a estimé que les risques de mésusage des données n'étaient pas suffisamment pris en compte, qu'il s'agisse de l'utilisation du système à des fins de reconnaissance faciale, qui n'est pas interdite en l'état du texte, ou encore du risque de consultation massive des données enregistrées dans le traitement dans le cadre de réquisitions judiciaires.

La CNIL a utilisé les mêmes critères d'appréciation pour ce traitement que ceux fixés s'agissant de traitements biométriques plus courants, en tenant dûment compte des spécificités dues à l'ampleur du fichier TES. Ces critères seront d'ailleurs directement applicables à ce traitement dès mai 2018 dans le cadre de la refonte du cadre juridique européen en matière de protection des données.

Néanmoins, les questions soulevées par le traitement TES dépassent les seuls enjeux juridiques de conformité à la législation applicable.

C'est pourquoi la CNIL a également, dans son avis précité, recommandé l'intervention du Législateur, alors même que cette saisine n'était pas juridiquement obligatoire. Cette recommandation s'est appuyée sur un double constat : d'une part, l'ampleur et la sensibilité du traitement, susceptible de comporter des données particulièrement sensibles concernant l'ensemble de la population française et, d'autre part, le choix de société induit par la mise en œuvre d'un tel traitement. Le Parlement s'est saisi de la question, en organisant plusieurs auditions, tandis que le Gouvernement, s'agissant des mesures techniques, demandait à l'ANSSI et la DINSIC de procéder à l'évaluation technique du dispositif.

5 Cf. par exemple Délibération n° 2013-239 du 12 septembre 2013 portant avis sur un projet de décret portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « contrôle d'accès et système biométrique ».

6 Délibération n° 2010-105 du 15 avril 2010 portant avis sur un projet de décret modifiant le décret n° 2007-1182 du 3 août 2007 portant création d'un traitement automatisé de données à caractère personnel relatives à des passagers des aéroports français franchissant les frontières extérieures des Etats parties à la convention signée à Schengen le 19 juin 1990

7 Délibération n° 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE

8 Délibération n° 2016-292 du 29 septembre 2016 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité

9 Cf. rapport annuel 2011 pour un rapide historique sur ces questions

10 Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité

Open data : la protection des données comme vecteur de confiance

Si l'*open data* ne concerne pas initialement la protection des données à caractère personnel, le nouveau contexte numérique implique de mieux prendre en compte, au niveau de la mise à disposition des données comme de leur réutilisation, la protection de la vie privée. Le nouveau cadre juridique relatif à l'*open data* permet cette conciliation. Pour accompagner le développement d'un *open data* respectueux des droits des personnes, la CNIL souhaite élaborer un pack de conformité dédié à l'ouverture et à la réutilisation des données publiques.

« Penser l'administration comme une plateforme. »

LES ENJEUX POSÉS PAR L'OPEN DATA DU POINT DE VUE DE LA PROTECTION DES DONNÉES

20 000

jeux de données disponibles sur data.gouv.fr

Depuis plusieurs années, de nombreux Etats se sont inscrits dans un mouvement d'ouverture en ligne des informations détenues par leurs administrations publiques *(open data)*. En France, l'Etat et les collectivités territoriales sont particulièrement actifs en matière de mise à disposition gratuite et accessible des données publiques.

Sans bénéficier d'une définition partagée par tous les acteurs, l'*open data* répond à **trois objectifs majeurs :**

1 renforcer la transparence de l'action publique et de la vie démocratique,

2 communiquer au public une image détaillée du territoire et de son fonctionnement actuel,

3 développer le marché de l'information publique en permettant d'identifier des leviers d'amélioration de l'organisation publique et de susciter l'innovation économique.

La philosophie de ce mouvement est de « penser l'administration comme une plateforme » pour confier aux développeurs et aux administrés les propositions d'amélioration du service public ou encore la création de services innovants constitués à partir de jeux de données ouvertes.

Littéralement traduit de l'anglais « données ouvertes », l'*open data* se concrétise par la mise à disposition de tout internaute des informations du secteur public, sous leur forme la moins interprétée (donnée brute) et la plus facilement utilisable (donnée directement exploitable par une machine). En pratique, un portail en *open data* propose sur Internet une plate-forme de téléchargement permettant de récupérer des jeux de données, sans autre filtre, le plus souvent, que l'acceptation d'une licence ou de conditions générales d'utilisation.

En France, ce mouvement a d'abord été initié par les collectivités territoriales. L'État a ensuite mis en œuvre une politique fortement incitative en matière d'*open data*, qui s'est notamment traduite par la mise en ligne de la plateforme data.gouv.fr, où plus de 20 000 jeux de données sont aujourd'hui disponibles, faisant de la France un des Etats les plus en pointe du mouvement d'ouverture des données publiques. Elle s'est également traduite par la création de nouvelles structures administratives incitant les différents acteurs publics à mettre en ligne les informations dont ils disposent et les accompagnent dans leurs projets « *open data* ».

À titre général, l'*open data* ne concerne pas directement la protection des données à caractère personnel : **la majorité des informations du secteur public mises à disposition des internautes ne comportent aucune donnée personnelle.** Il peut s'agir par exemple de données liées au fonctionnement budgétaire et quotidien d'un service public, de statistiques, de cartographies et de localisation, de données liées à l'organisation d'évènements culturels et sportifs, d'informations touristiques, de mesures sur la qualité environnementale, etc.

Néanmoins, les organismes publics produisent ou détiennent une très grande variété de données susceptibles, dans le cadre de l'*open data*, d'être mises à disposition sur Internet. En outre, **l'essor sans précédent du numérique implique des possibilités croissantes de ré-identification des personnes initialement concernées par ces données et, par voie de conséquence, l'applicabilité de la loi Informatique et Libertés auxdits jeux de données.**

La CNIL publie des « jeux de données » dans 9 domaines intéressant ses activités :

- Délibérations
- Organismes ayant désigné un correspondant Informatique et Libertés
- Protection des données personnelles dans le monde (données par pays)
- Plaintes reçues
- Droit d'accès indirect
- Contrôles réalisés
- Budget
- Effectifs
- Marchés publics

Ces jeux de données sont accessibles gratuitement sur cnil.fr (rubrique Open CNIL) ou directement sur data.gouv.fr, et disponibles aux formats csv ou xls. Une large réutilisation de ces données est possible (Licence ouverte / Open licence).

Il existe deux hypothèses dans lesquelles l'*open data* implique, directement ou indirectement, la prise en compte de la protection des données personnelles.

1ÈRE HYPOTHÈSE

Les informations publiques peuvent tout d'abord, sans même contenir initialement de données identifiantes, permettre, par recoupement avec d'autres informations publiques mises à disposition et plus généralement avec d'autres données disponibles sur Internet, l'identification ou la réidentification de personnes physiques. Dans ce cas, plus que sa qualité intrinsèque, c'est bien l'usage fait de la donnée initiale qui lui confère son caractère personnel.

Cette hypothèse ne doit pas être négligée. Tous les travaux de recherche sur ces questions démontrent qu'il devient de plus en plus facile, du fait de la multiplicité des données disponibles et de leur degré de précision, de réidentifier directement des personnes sur la base d'informations dépersonnalisées comme, par exemple, les données de géolocalisation de téléphones portables, les données de fréquentation d'établissements de soin ou encore les données agrégées de notation de films par les utilisateurs des plateformes numériques audiovisuelles.

Exemple : *Le chercheur du MIT Yves-Alexandre de Montjoye a démontré en 2015, à partir de l'étude des données de cartes bancaires, produites sur trois mois par 1,1 million de personnes, que seuls quatre points «spatio-temporels» (coordonnées géographiques, date et heure) suffisent pour retrouver l'identité de 90% des individus. Connaître le tarif des transactions permet d'augmenter encore le risque de ré-identification de 22%. Déjà, en 1997, la doctorante du MIT Latanya Sweeney, avait retrouvé les données de santé du gouverneur de l'État au sein des données anonymes publiques en utilisant d'autres données ouvertes (lui permettant de définir son âge, code postal et sexe).*

2ÈME HYPOTHÈSE

La protection de la vie privée des personnes doit impérativement être prise en compte lorsque les jeux de données mis à disposition en *open data* comportent directement des données personnelles.

L'*open data*, au sens large, est en effet susceptible de concerner de très nombreuses catégories d'informations. Certaines données nominatives ou directement identifiantes sont ainsi publiées sur Internet en application d'obligations légales, afin de produire les effets juridiques attachés aux décisions administratives (arrêtés de nomination d'agents publics, résultats d'examen, etc.) ou afin de favoriser la transparence à l'égard du public (par exemple, publication des déclarations de situation patrimoniale et d'intérêts de certains élus, publication des avantages consentis par les entreprises pharmaceutiques aux professionnels de santé, etc.).

D'autres dispositions légales encadrent en outre la communication et la réutilisation de certaines données personnelles qui, sans être nécessairement publiées sur Internet, participent de ce mouvement de l'*open data*, telles que, par exemple, les relevés de propriété, les avis d'imposition, la liste électorale, les actes de l'état civil, les archives publiques, etc.

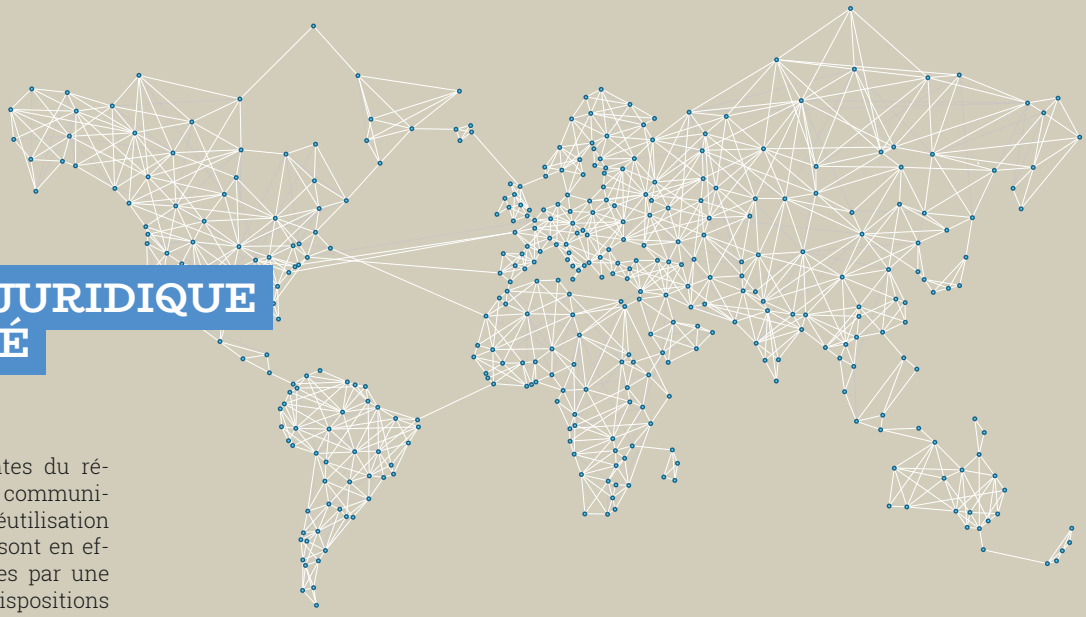
Enfin, si certaines expressions sont improprement employées, la logique de l'*open data* concerne de plus en plus de secteurs et les demandes sociales ou économiques « d'ouverture » de données se font de plus en plus diverses : on parle ainsi d'*open data* des décisions de justice, d'*open data* des données de santé, d'*open data* en matière d'énergie, d'immobilier, etc. Ces quelques exemples montrent que **des données de plus en plus sensibles et relatives aux activités relevant de la vie privée des personnes sont concernées par la dynamique de l'*open data*.**

Le développement de ce mouvement soulève donc la question de l'équilibre entre le droit d'accès à l'information publique, c'est-à-dire la transparence administrative, et la nécessaire protection des données à caractère personnel. Plus que l'*open data* lui-même, c'est davantage le contexte dans lequel il s'inscrit qui doit appeler à la vigilance : informatisation de la société, des administrations comme des acteurs privés ; diffusion spontanée de données personnelles par les internautes ; indexation de données nominatives par de puissants moteurs de recherche ; développement du *Big Data*...

Les autorités publiques n'ont pas toujours intégré spontanément cette dimension essentielle. L'*open data* est en effet porté par des objectifs de transparence administrative et démocratique, ainsi que par des objectifs de création de valeur économique, les entreprises du numérique voyant dans l'exploitation des données publiques une source de création de valeur, auxquels la protection des données personnelles peut sembler s'opposer.

Pour la CNIL, il n'en est rien : les objectifs parfaitement légitimes poursuivis par la politique d'ouverture des données publiques sont pleinement conciliables avec la protection de la vie privée. Plus encore, la prise en compte de cet impératif permettra de favoriser la confiance des différentes parties prenantes de ce mouvement (autorités publiques, citoyens, entreprises), qui constitue une condition essentielle de la réussite de toute politique publique.
La CNIL a donc, très tôt, appelé l'attention des pouvoirs publics sur la nécessité de mieux concilier ces impératifs. Cette conciliation est d'autant plus réalisable en pratique qu'un cadre juridique existe depuis la fin des années 70 visant précisément à articuler les objectifs de transparence administrative et de protection des données personnelles. Ce cadre juridique a été largement renouvelé par la loi du 7 octobre 2016 pour une République numérique.

« Le développement de l'*open data* soulève la question de l'équilibre entre la transparence administrative et la nécessaire protection des données personnelles. Pour la CNIL, ces objectifs sont non seulement conciliables mais complémentaires. »



UN CADRE JURIDIQUE RENOUVELÉ

Des modifications importantes du régime juridique relatif à la communication, la publication et la réutilisation des informations publiques sont en effet intervenues, matérialisées par une refonte substantielle des dispositions du Code des relations entre le public et l'administration. La CNIL s'est assurée, dans le cadre de cette refonte, de la prise en compte de la protection des données personnelles.

Les dispositions générales

La loi du 7 octobre 2016 pour une République numérique **fixe ainsi le cadre juridique relatif à l'*open data***, en modifiant les dispositions créées dès la fin des années 70 (loi dite « CADA » du 17 juillet 1978 modifiée). Pour rappel, la loi CADA comportait plusieurs dispositions visant à concilier transparence administrative et protection des données à caractère personnel : elle prévoyait que les informations publiques contenues dans des documents administratifs dont la communication porterait atteinte à la protection de la vie privée ne sont ni communicables (sauf aux personnes intéressées), ni réutilisables, et que de telles informations sont dès lors exclues de tout mise à disposition en *open data* par une autorité administrative. Elle prévoyait en outre que les informations publiques ne portant pas directement atteinte à la vie privée mais comportant néanmoins des données personnelles sont réutilisables, dans trois hypothèses (consentement, anonymisation ou disposition légale expresse) et dans certaines conditions (respect des dispositions de la loi Informatique et Libertés). Elle distinguait enfin trois étapes, soumises chacune à des conditions différentes : la communication, la publication et la réutilisation d'informations publiques.

Dans ce contexte, la loi pour une République numérique vise à favoriser l'*open data* en modifiant le cadre juridique de la diffusion en ligne des informations publiques. Ainsi, les conditions applicables à la communication et à la publication des documents administratifs sont uniformisées : par principe, tout document communicable est donc publiable sur Internet. En cas de demande de communication d'informations publiques, les demandeurs peuvent en outre exiger de l'administration saisie que les documents requis soient publiés en ligne.

Les documents portant atteinte à la vie privée des personnes concernées ne peuvent en revanche pas être publiés. De même, un sort particulier est réservé à la publication de documents comportant des données à caractère personnel.

Trois conditions alternatives sont prévues pour en permettre la publication de documents comportant des données personnelles :

1. l'existence de dispositions législatives expresses,
2. l'accord des personnes concernées,
3. la mise en œuvre d'un traitement permettant de rendre impossible l'identification de ces personnes (anonymisation).

Il est également fait obligation aux administrations, sous les réserves précitées, de publier en ligne certaines informations qu'elles produisent ou détiennent. Pour ces informations, définies dans la loi, il s'agit donc de passer d'une logique de demande d'accès par les personnes privées à une logique d'offre par les administrations.

En outre, des dispositions visent à **favoriser et à faciliter la réutilisation de documents administratifs.** Elles dessinent la logique générale sous-jacente à l'ensemble des modifications apportées au cadre juridique de l'*open data* : **la contraction des trois phases que constituaient auparavant la communication, la publication et la réutilisation des informations publiques.** L'objectif général est en effet de permettre que tout document communicable puisse faire l'objet, non seulement d'une publication, mais également d'une libre réutilisation, en uniformisant les conditions applicables à ces trois régimes juridiques. Il n'est dès lors plus prévu de conditions particulières d'exercice de ce droit de réutilisation en cas d'informations comportant des données à caractère personnel, à l'exception du respect de la loi Informatique et Libertés.

> « Avec la loi pour une République numérique, par principe, tout document communicable est donc publiable sur Internet. »

La réutilisation d'informations est ainsi appréhendée comme la suite logique du droit d'accès aux documents administratifs, conformément à la logique de l'*open data* : toute mise à disposition, sous forme électronique, de documents - c'est-à-dire toute communication ou publication - « se fait dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé ».

Au total, le cadre juridique relatif à l'*open data* est plus prescriptif et mieux adapté à la pratique en la matière. En revanche, il ne remet pas en cause les fondements de l'équilibre trouvé par la « loi CADA » entre transparence administrative, d'une part, et protection de la vie privée et des données personnelles, d'autre part. En effet, le triple filtre prévu (interdiction de publication de documents portant atteinte à la vie privée ; publication sous condition de documents comportant des données personnelles ; réutilisation de telles données dans le respect de la loi Informatique et Libertés) **permet de garantir la protection des données des personnes concernées par les informations publiques.**

Les dispositions sectorielles

Deux autres points méritent d'être soulignés. Au-delà de ces dispositions générales sur l'*open data*, la loi du 7 octobre 2016 comporte de nombreuses dispositions sectorielles permettant la mise à disposition, à des fins d'intérêt général, de données publiques particulières ou de données détenues par des opérateurs privés, ainsi que des dispositions visant à favoriser la circulation de ces données dans la société par l'obligation de les mettre à disposition dans des standards ouverts et réutilisables.

D'autres dispositions sectorielles sont également prévues pour l'immobilier (ouverture aux professionnels du secteur des données foncières détenues par l'administration fiscale), en matière de sécurité routière (création d'une base de données nationale des vitesses maximales autorisées) ou encore en matière d'environnement.

Elles s'ajoutent aux nombreuses dispositions spéciales déjà existantes, par exemple en matière de santé : depuis la loi du 26 janvier 2016 de modernisation de notre système de santé, les données du système national des données de santé (SNDS) font l'objet d'une mise à la disposition du public sous la forme de statistiques agrégées ou de données individuelles dans des conditions telles que l'identification, directe ou in-

INFOSPLUS

La loi pour une République numérique prévoit que les données suivantes doivent être diffusées en *open data* :

- données détenues par les délégataires de service public ;
- données essentielles des conventions de subvention par une autorité administrative ;
- données détaillées de consommation et de production d'électricité et de gaz naturel, « sous une forme agrégée garantissant leur caractère anonyme » ;
- ensemble des décisions rendues par les juridictions administratives et les juridictions judiciaires « dans le respect de la vie privée des personnes concernées », et notamment après avoir procédé à une analyse du risque de ré-identification des personnes.

directe, des personnes concernées est impossible. La loi prévoit que la réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées.

Des missions renforcées pour la CNIL et la CADA

La loi pour une République numérique a renforcé les missions des autorités administratives indépendantes chargées de veiller à l'application de ce régime juridique renouvelé, à savoir la CADA et la CNIL. La CNIL a par exemple été dotée d'un pouvoir de certification et d'homologation de processus d'anonymisation des données. Dans la mesure où cette anonymisation constitue une des conditions présidant à la mise en *open data* de données publiques, elle pourra ainsi contrôler et assurer le développement de projets *open data* respectueux de la protection des données personnelles.

Le rapprochement de ces deux autorités a également été poursuivi : le président de la CADA devient membre de droit de la CNIL et, réciproquement, le président de la CNIL devient membre à part entière de la CADA, tous deux pouvant désigner un représentant. En outre, il est rendu possible pour les deux autorités, lorsqu'un sujet d'intérêt commun le justifie et sur l'initiative conjointe de leurs présidents, de se réunir dans un collège unique.

L'ensemble de ces dispositions dessinent un nouveau paysage juridique en matière d'*open data*, qui vise notamment à consolider l'équilibre nécessaire entre transparence administrative et protection de la vie privée et des données à caractère personnel. Si toutes les difficultés pratiques liées à l'application de la loi ne sont pas résolues, les conditions juridiques sont dorénavant établies pour permettre un développement de l'*open data* favorisant l'innovation tout en respectant les libertés individuelles.

VERS UN « PACK DE CONFORMITÉ » DÉDIÉ À L'OPEN DATA

La mise en œuvre de ce nouveau dispositif juridique, complexe et composite, n'est pas sans susciter des interrogations de la part de l'ensemble des autorités publiques, nationales ou locales, soumises à ces obligations. De même, les responsabilités exactes des réutilisateurs des informations publiques ainsi mises en *open data* ne sont pas nécessairement et clairement appréhendées lorsque ces jeux de données comportent des données à caractère personnel.

Ainsi, l'étendue exacte des secrets protégés par la loi en matière de publication de données, les modalités de recueil du consentement des personnes concernées par celles-ci ou le caractère anonyme ou non des informations diffusées constituent des points d'interrogations récurrents de la part des différentes parties prenantes du mouvement de l'*open data*.

Dans ce contexte, la CNIL souhaite améliorer l'accompagnement de ces acteurs en élaborant un « pack de conformité » dédié à l'ouverture des données publiques.

Un tel référentiel permettra de mieux encadrer, du point de vue de la protection des données personnelles, les modalités d'action des administrations, établissements publics et collectivités territoriales, tout particulièrement en matière de diffusion en ligne de données publiques, ainsi que de répondre à leurs questions récurrentes en la matière. Il permettra également de faciliter la réutilisation de données à caractère personnel, dans des conditions conformes aux droits des personnes concernées par ces données.
Il devra nécessairement être élaboré dans une démarche de co-régulation avec les autres autorités concernées par cette thématique, et en particulier avec la CADA, conformément à la loi pour une République numérique, ainsi qu'avec les autorités publiques en charge des politiques nationales et locales d'ouverture des données. Producteurs et réutilisateurs d'informations publiques pourront ainsi s'appuyer sur des outils juridiquement et technologiquement approuvés par le régulateur dans le cadre de leurs projets d'*open data*.

Cette démarche se distingue néanmoins des précédents packs de conformité élaborés par la CNIL, axés sur un secteur d'activité particulier, voire sur une catégorie de traitements particuliers (les assurances, le logement social, les compteurs intelligents). La diversité des jeux de données en cause, les possibilités infinies de réutilisation de ces données, la variété des conditions juridiques présidant à leur diffusion ou à leur réutilisation et le caractère fortement évolutif des projets *open data* ne permettront pas d'établir, de manière ferme et définitive, l'ensemble des conditions de mise en œuvre de tout projet de mise à disposition ou de réutilisation de données.

Il s'agit donc bien plutôt de mettre en œuvre des actions concrètes qui permettent de clarifier et de consolider le cadre juridique applicable à l'ouverture des données publiques en cas de présence de données personnelles et de faciliter la mise en œuvre pratique de ce cadre, pour les producteurs comme pour les réutilisateurs. Ces actions seront développées sur la base de projets sectoriels et spécifiques, et en particulier dans les domaines expressément visés par la loi pour une République numérique.

L'*open data* des décisions de justice

La CNIL s'est investie très tôt dans la régulation de la diffusion des données de jurisprudence en édictant, dès 2001, **une recommandation en matière de diffusion sur internet des décisions de justice,** aujourd'hui largement appliquée par les juridictions concernées et les diffuseurs de ces décisions. Afin de faciliter l'accès au droit tout en protégeant la vie privée des personnes concernées par ces décisions, la CNIL avait recommandé d'occulter, préalablement à la diffusion sur internet, les données les plus directement identifiantes (noms, prénoms et adresses des parties et des témoins). Ces données ne sont donc pas « anonymisées » au sens strict, mais plutôt pseudonymisées.

La loi pour une République numérique marque l'aboutissement de ce processus de mise à disposition des données de jurisprudence. Elle prévoit en effet que l'ensemble des jugements des juridictions administratives et judiciaires « sont mis à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées » et que cette mise à disposition « est précédée d'une analyse du risque de ré-identification des personnes ».

La mise en œuvre de ces nouvelles dispositions permettra à la CNIL de mieux accompagner les juridictions dans leurs projets de mise à disposition de leurs décisions. Le décret en Conseil d'Etat qui doit déterminer les conditions d'application de ces nouvelles obligations devra en effet déterminer les modalités d'analyse de risque de réidentification des personnes et la CNIL pourra ainsi apporter toute son expertise sur ce sujet, dans le cadre de son avis sur ce décret, ainsi que son concours dans la réalisation de ces études d'impact sur la vie privée. Le changement d'échelle opéré par la loi du 7 octobre 2016 devra également s'accompagner d'une nouvelle clarification des obligations des réutilisateurs de ces données, dans la même lignée que celle opérée par le caveat. La pseudonymisation en amont de ces données par la puissance publique et le contrôle de la CNIL sur leur réutilisation, en particulier sur l'absence de réidentification des personnes et sur le caractère effectif et continu du respect des droits des personnes concernées (rectification et opposition notamment), permettra ainsi de maintenir le délicat équilibre entre accès au droit et protection de la vie privée.

FOCUS

Le caveat accompagnant la consultation ou le téléchargement des jeux de décisions de justice

Les informations figurant dans la licence ouverte proposée par la DILA n'étaient en effet pas assez précises pour permettre aux réutilisateurs de connaître les limites d'usage à respecter en cas de traitement de ces données. Il a ainsi été reconnu nécessaire de délivrer une information plus précise à tout internaute accédant aux jurisprudences contenant des données à caractère personnel, dans le souci de rappeler le cadre juridique et les limites d'usages à respecter en cas de réutilisation.

Ce caveat rappelle dès lors plus précisément le cadre juridique applicable à la réutilisation de ces données et en particulier que, lorsque les données personnelles contenues dans ces informations ont préalablement à leur diffusion fait l'objet d'une anonymisation totale ou partielle, conformément à des dispositions légales ou aux recommandations de la Commission nationale de l'informatique et des libertés (CNIL), cette réutilisation ne peut avoir pour objet ou pour effet de réidentifier les personnes concernées. Il rappelle également que les réutilisateurs doivent respecter les principes essentiels de la loi Informatique et Libertés.

Il s'agit donc d'une mention formulée en vocabulaire courant, qui apparaît au frontispice du cadre conventionnel conclu entre le diffuseur des données et les réutilisateurs. Il permet une balance des intérêts, qui part du principe que, si la puissance publique – en l'occurrence, les juridictions suprêmes – anonymise (au sens large) les décisions de justice, ce n'est pas pour que cette anonymisation soit ensuite contournée, ni a fortiori pour que ces éléments permettent de réidentifier les personnes en enrichissant d'autres jeux de données à disposition des réutilisateurs.

Ces travaux communs avec la CADA, la DILA et Etalab ont ainsi participé de la mise en œuvre d'une politique d'ouverture des données responsable, respectueuse de la vie privée et des droits des personnes.

L'*open data* en matière d'énergie

Depuis 2015, la CNIL participe aux travaux gouvernementaux portant sur l'anonymisation de données énergétiques. La loi pour une République numérique a prévu dans ce cadre de nouvelles dispositions, selon lesquelles les gestionnaires des réseaux de transport et de distribution d'électricité et de gaz naturel mettent à disposition du public les données détaillées de consommation et de production issues de leurs systèmes de comptage d'énergie, dans l'objectif de favoriser notamment le développement d'offres d'énergie, d'usages et de services énergétiques, « sous une forme agrégée garantissant leur caractère anonyme ».

Dans le cadre du décret d'application de ces dispositions, **la CNIL devra donc énoncer les critères d'anonymisation des données énergétiques.** Ce cas particulier permettra dès lors à la CNIL d'actionner les nouveaux pouvoirs qui lui ont été conférés par la loi du 7 octobre 2016 en matière de certification et d'homologation de processus d'anonymisation des données.

Une même démarche opérationnelle sera suivie par la CNIL dans les autres domaines d'application de ce pack de conformité, comme en matière de santé par exemple, où l'accès et la mise à disposition des données issues du SNDS doivent intervenir dans des conditions variables selon la qualité des « réutilisateurs ». Pour le public en particulier, cette mise à disposition doit intervenir dans des conditions rendant impossible la réidentification des personnes et la CNIL devra dès lors fixer les opérations techniques permettant l'anonymisation de ces données particulièrement sensibles.

Au total, il s'agira de clarifier les obligations générales ou sectorielles des producteurs de données mises à disposition en *open data* et des réutilisateurs de ces jeux de données. Ce pack permettra également, sur la base de projets *open data* aboutis, de définir et de promouvoir les bonnes pratiques opérationnelles ou techniques. En un mot, de participer à l'accompagnement de l'innovation dans le respect des droits des personnes.

La loi pour une République numérique : une avancée pour la protection des droits, en anticipation du règlement européen

La loi pour une République numérique du 7 octobre 2016 crée de nouveaux droits Informatique et Libertés et permet ainsi aux individus de mieux maîtriser leurs données personnelles. Elle renforce les pouvoirs de sanctions de la CNIL et lui confie de nouvelles missions. Elle contribue également à une meilleure ouverture des données publiques.
Certaines dispositions anticipent le règlement européen sur la protection des données personnelles applicable en mai 2018. La loi introduit de nombreuses dispositions directement applicables, d'autres doivent attendre la publication de décrets d'application.
La CNIL s'est déjà prononcée sur certains d'entre eux.

QUELS CHANGEMENTS POUR LA PROTECTION DES DONNÉES PERSONNELLES ?

De nouveaux droits pour les personnes

- **L'affirmation du principe de la maîtrise par l'individu de ses données.** Le droit à l'autodétermination informationnelle s'inspire d'un droit similaire dégagé par la juridiction constitutionnelle allemande. Il renforce positivement les principes énoncés à l'article 1er de la loi Informatique et Libertés en affirmant la nécessaire maîtrise de l'individu sur ses données.

- **Le droit à l'oubli pour les mineurs.** L'article 40 de la loi Informatique et libertés prévoit désormais un « droit à l'oubli » spécifique aux mineurs et une procédure accélérée pour l'exercice de ce droit. Lorsque la personne concernée était mineure au moment de la collecte des données, elle peut obtenir auprès des plateformes l'effacement des données problématiques « dans les meilleurs délais ». En l'absence de réponse ou de réponse négative de la plateforme dans un délai d'un mois, la personne peut saisir la CNIL qui dispose alors d'un délai de 3 semaines pour y répondre.

- **La possibilité d'organiser le sort de ses données personnelles après la mort.** Le nouvel article 40-1 de la loi Informatique et libertés permet aux personnes de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès. Une personne peut être désignée pour exécuter ces directives. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés.

  Ces directives sont :

- générales, lorsqu'elles portent sur l'ensemble des données concernant une personne ;

- ou particulières, lorsque ces directives ne concernent que certains traitements de données spécifiques.

Lorsque ces directives sont générales et portent sur l'ensemble des données du défunt, elles peuvent être confiées à un tiers de confiance certifié par la CNIL.

Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement (réseaux sociaux, messagerie en ligne) en cas de décès. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.

En l'absence de directives données de son vivant par la personne, les héritiers auront la possibilité d'exercer certains droits, en particulier :

- **le droit d'accès,** s'il est nécessaire pour le règlement de la succession du défunt ;

- **le droit d'opposition** pour procéder à la clôture des comptes utilisateurs du défunt et s'opposer au traitement de leurs données.

- **La possibilité d'exercer ses droits par voie électronique.** Le nouvel article 43 bis de la loi Informatique et Libertés impose, «lorsque cela est possible», de permettre à toute personne l'exercice des droits d'accès, de rectification ou d'opposition par voie électronique, si le responsable du traitement des données les a collectées par ce vecteur.

Plus d'information et de transparence sur le traitement des données

- **L'information des personnes sur la durée de conservation de leurs données.** L'obligation d'information prévue par l'article 32 de la loi Informatique et Libertés est renforcée. Les responsables de traitements de données doivent désormais informer les personnes de la durée de conservation des données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

Les compétences de la CNIL confortées et élargies

- **Un pouvoir de sanction renforcé.** Le plafond maximal des sanctions de la CNIL passe de 150.000€ à 3 millions € (anticipation sur l'augmentation du plafond du montant des sanctions par le règlement européen qui sera applicable le 25 mai 2018 et prévoit un plafond pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial). La formation restreinte de la CNIL peut désormais ordonner que les organismes sanctionnés informent individuellement de cette sanction et à leur frais, chacune des personnes concernées. Elle pourra également prononcer des sanctions financières sans mise en demeure préalable des organismes lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité.

- **Une consultation plus systématique de la CNIL.** La CNIL sera saisie pour avis sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Cette rédaction permettra à la CNIL d'apporter son expertise aux pouvoirs publics de manière plus systématique, alors que les textes actuels ne prévoient sa saisine que sur les dispositions relatives à la « protection » des données personnelles.

- **La publicité automatique des avis de la CNIL sur les projets de loi.** Cette disposition renforce la transparence sur les avis de la CNIL.

De nouvelles missions

- **L'affirmation de sa mission de promotion de l'utilisation des technologies protectrices de la vie privée,** notamment les technologies de chiffrement des données.

- **La certification de la conformité des processus d'anonymisation** des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation. L'anonymisation des bases de données est une condition essentielle à leur ouverture ou à leur partage : elle permet de prémunir les personnes des risques de ré-identification, et les acteurs (administrations émettrices de données,

FOCUS

Le droit à « l'autodétermination informationnelle », clé de lecture de la loi Informatique et Libertés

La loi Informatique et Libertés reconnait déjà les droits d'accès, d'opposition ou d'effacement, et prévoit également une information des personnes, traduction d'un principe de transparence à l'égard de l'individu. Mais si ces droits permettent un regard par la personne sur l'utilisation de ses données, ou une opposition au traitement de celles-ci, ils ne traduisent pas explicitement une réelle maîtrise. C'est pourquoi le Législateur a décidé, par la loi pour une République numérique, d'inscrire au frontispice de la loi Informatique et Libertés le principe de « l'autodétermination informationnelle ». L'article 1er de la loi prévoit ainsi désormais : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

L'affirmation de ce principe – et le fait qu'il ouvre la loi Informatique et Libertés - signifie qu'il s'agit, en quelque sorte, d'une clé de lecture de cette législation. A l'ère numérique, il signifie que la personne humaine doit pouvoir maîtriser le devenir de ces données, et que l'ensemble des droits qui lui sont ouverts, comme des obligations qui pèsent sur les entités qui traitent ces données, concourent à cet équilibre.

Ce principe, dit « d'autodétermination informationnelle », n'est pas inédit. Il a été défini par la Cour constitutionnelle fédérale d'Allemagne (Bundesverfassungsgerichtshof) à l'occasion d'un arrêt du 15 décembre 1983, relatif à une loi sur le recensement. Cet arrêt est souvent présenté comme une jurisprudence fondatrice de la protection des données personnelles en Allemagne et de sa constitutionnalisation. La Cour de Karlsruhe a ainsi posé que la Loi fondamentale allemande garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel. Ce droit à l'autodétermination en matière informationnelle découle en effet des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale.

Ce double fondement juridique est particulièrement éclairant : la dignité – qui associe donc la donnée à l'essence même de la personne – et l'autonomie – qui est au cœur de la figure du citoyen – sont les deux valeurs placées au sommet de la Loi fondamentale allemande. La Cour de Karlsruhe relève d'ailleurs que cette autodétermination est une condition première pour permettre au citoyen d'interagir dans une société démocratique.

L'inscription de ce droit dans le droit interne français a donc été décidée dans le cadre de la loi pour une République numérique du 7 octobre 2016. Elle traduit un principe implicite, et réaffirme ainsi que la personne humaine est le centre de gravité de la législation sur la protection des données. Cela ne signifie bien sûr pas que ce droit soit illimité : il doit être concilié, dans les conditions prévues par la loi, avec l'intérêt légitime, notamment, des entreprises ou administrations qui traitent les données, ou avec l'intérêt général, par exemple en matière de sécurité publique ou en matière fiscale. Mais après des débats qui ont conduit à des interrogations sur une éventuelle « patrimonialisation » des données, il permet d'inscrire avec force que le citoyen français et européen est titulaire de droits à l'égard de ses données, quel que soit le détenteur de celle-ci, ou leur éventuel transfert. C'est parce que la donnée porte sur l'individu que celui-ci peut exercer ses droits, droits qui ne peuvent pas être cédés à un tiers ou monnayés. C'est d'ailleurs ce qui avait conduit le Conseil d'Etat, dans son rapport annuel 2014 consacré au numérique et aux droits fondamentaux, à recommander l'inscription de ce droit à la loi Informatique et Libertés, en précisant que « ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès...), mais comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette finalité ».

> « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »
>
> Complément apporté à l'article 1er de la loi Informatique et Libertés.

ré-utilisateurs, entreprises privées qui réalisent des recherches notamment statistiques), de la mise en cause de leur responsabilité en la matière. La certification ou l'homologation de méthodologies d'anonymisation ainsi que la publication de référentiels ou de méthodologies générales par la CNIL sera ainsi un gage de protection des personnes et de sécurité juridique pour les acteurs.

- **La conduite par la CNIL d'une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.** Même si la loi Informatique et Libertés a toujours comporté une dimension éthique fondamentale, comme en témoignent tant ses conditions de création et son article 1er, que la composition de la Commission, la révolution numérique implique une réflexion élargie sur sa dimension éthique.

L'ouverture des données publiques étendue

La loi pour une république numérique ne remet pas en cause l'équilibre entre transparence administrative et protection de la vie privée et des données personnelles. En effet, les critères de communicabilité n'ont pas changé, et la publication – donc la réutilisation – est subordonnée au caractère librement communicable du document.
Pour autant, en passant d'une logique de la demande d'un accès à une logique de l'offre de données publiques, la loi vise clairement à ouvrir très largement les données publiques. La CNIL va accompagner cette ouverture, notamment en répondant aux demandes de conseil des collectivités publiques ou des réutilisateurs, puisque toute réutilisation de données personnelles est soumise au « droit commun » Informatique et Libertés. La possibilité pour la CNIL d'homologuer des méthodologies d'anonymisation constituera un élément important de cette régulation.

En matière de gouvernance de la donnée, la loi prévoit un rapprochement entre la CNIL et la CADA, à travers, notamment, une participation croisée dans les deux collèges.

Les décrets d'application

Depuis la publication de la loi, la CNIL s'est déjà prononcée pour avis sur 6 décrets d'application et doit encore se prononcer sur 9 décrets.

Principaux décrets d'application prévus par la loi numérique dont la CNIL a déjà été saisie	Saisine de la CNIL	Passage en séance plénière
Décret fixant les conditions de mise en œuvre de la carte « mobilité inclusion »	1er août 2016	Délibération du 13 octobre 2016 n°2016-318
Décret relatif à la substitution d'un code statistique non signifiant au numéro d'inscription des personnes au répertoire national d'identification des personnes physique dans le champ de la statistique publique de la recherche	Le 10 octobre 2016	Délibération du 1er décembre 2016 n°2016-372
Décret fixant les conditions de mise en œuvre de l'information des usagers sur les algorithmes utilisés dans les décisions administratives	Le 17 octobre 2016	Deliberation du 16 février 2017 n°2017-023
Décret relatif à la mise à disposition du public des données détaillées de consommation et de production issues du système de comptage d'énergie (électricité de gaz) – *open data* énergie	Le 24 octobre 2016	Délibération du 16 février 2017 n°2017-024
Décret fixant la périodicité de renouvellement de consentement en cas de traitements de la correspondance privée en ligne	18 novembre 2016	Délibération du 12 janvier 2017 n°2017-001
Décret fixant les catégories de documents administratifs pouvant être rendus publics sans anonymisation	17 janvier 2017	Passage en séance plénière prévu en mars 2017
Décret relatif à l'information des utilisateurs sur les modalités de publication et de traitement des avis mis en ligne	10 février 2017	Délibération du 23 février 2017 n°2017-046
Au 1er mars 2017, les décrets suivants n'avaient pas encore fait l'objet d'une saisine de la CNIL.		
Décret fixant les conditions de mise à disposition de la jurisprudence judiciaire		
Décret fixant les conditions de mise à disposition de la jurisprudence administrative		
Décret fixant les documents pouvant être exigés lors de l'enregistrement auprès de commune constituant déclaration de location pour de courtes durées		
Décret portant registre unique d'enregistrement des références des directives générales de traitement des données personnelles après décès		
Décret fixant un cahier des charges permettant de déterminer la fiabilité d'un moyen d'identification électronique (+probablement, arrêté)		
Décret encadrant la possibilité, offerte par un service de coffre-fort numérique, de récupérer les documents et les données stockées		
Décret fixant les modalités de mise en œuvre du service de coffre-fort numérique et de sa certification par l'État		
Décret fixant la liste des pièces justificative que les particuliers n'ont plus à produire, lorsqu'une administration détient déjà ces informations		

Le chiffrement : un élément vital de la sécurité des données

La question de l'équilibre entre protection des données personnelles, innovation technologique et surveillance est au centre de nombreuses préoccupations, dans un contexte marqué par des cyberattaques de grande envergure comme par les révélations d'Edward Snowden sur la surveillance de masse. Or, le chiffrement contribue à la résilience de nos sociétés numériques et de notre patrimoine informationnel. Alors que la loi pour une République numérique a confié à la CNIL le soin d'assurer la promotion des technologies de chiffrement, la CNIL a pris position sur les enjeux du chiffrement et d'éventuelles « portes dérobées ». La mise en place de tels dispositifs ou de clés maîtres fragiliserait l'avenir de l'écosystème du numérique et la protection des données personnelles des individus, alors même que les autorités disposent par ailleurs de nombreux autres moyens permettant d'accéder aux données nécessaires aux enquêtes relatives aux faits graves, et de les analyser.

QU'EST-CE QUE LE CHIFFREMENT ?

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός). Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).

La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'authenticité d'un message (qui a envoyé ce message ?) ou encore assurer son intégrité (ce message a-t-il été modifié ?).

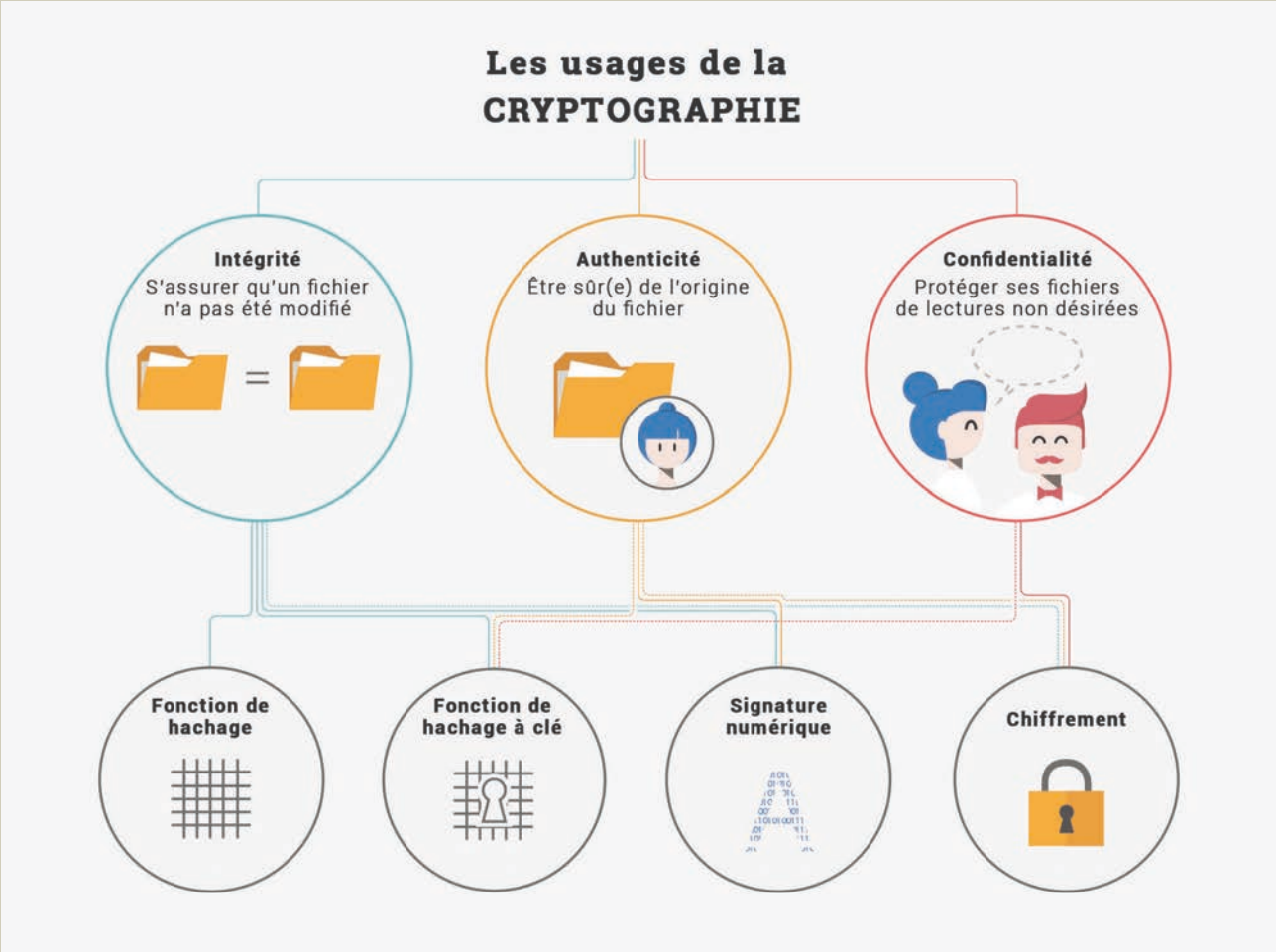
Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement

Le chiffrement (parfois improprement appelé « cryptage ») est la partie de la cryptologie qui a pour objectif de **rendre impossible la compréhension d'un message à toute personne n'ayant pas la clé de déchiffrement.** Ce principe permet ainsi d'assurer la confidentialité du message mais, par défaut, il n'assure ni son authenticité ni son intégrité.

Ainsi, le chiffrement d'un message permet de garantir que seuls l'émetteur et les destinataires légitimes d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré et sans détenir une clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

Plus précisément, il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Le chiffrement symétrique permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit alors être choisi avec précaution, afin que la clé ne puisse être récupérée par des tiers, ce qui n'assurerait plus la confidentialité du message.

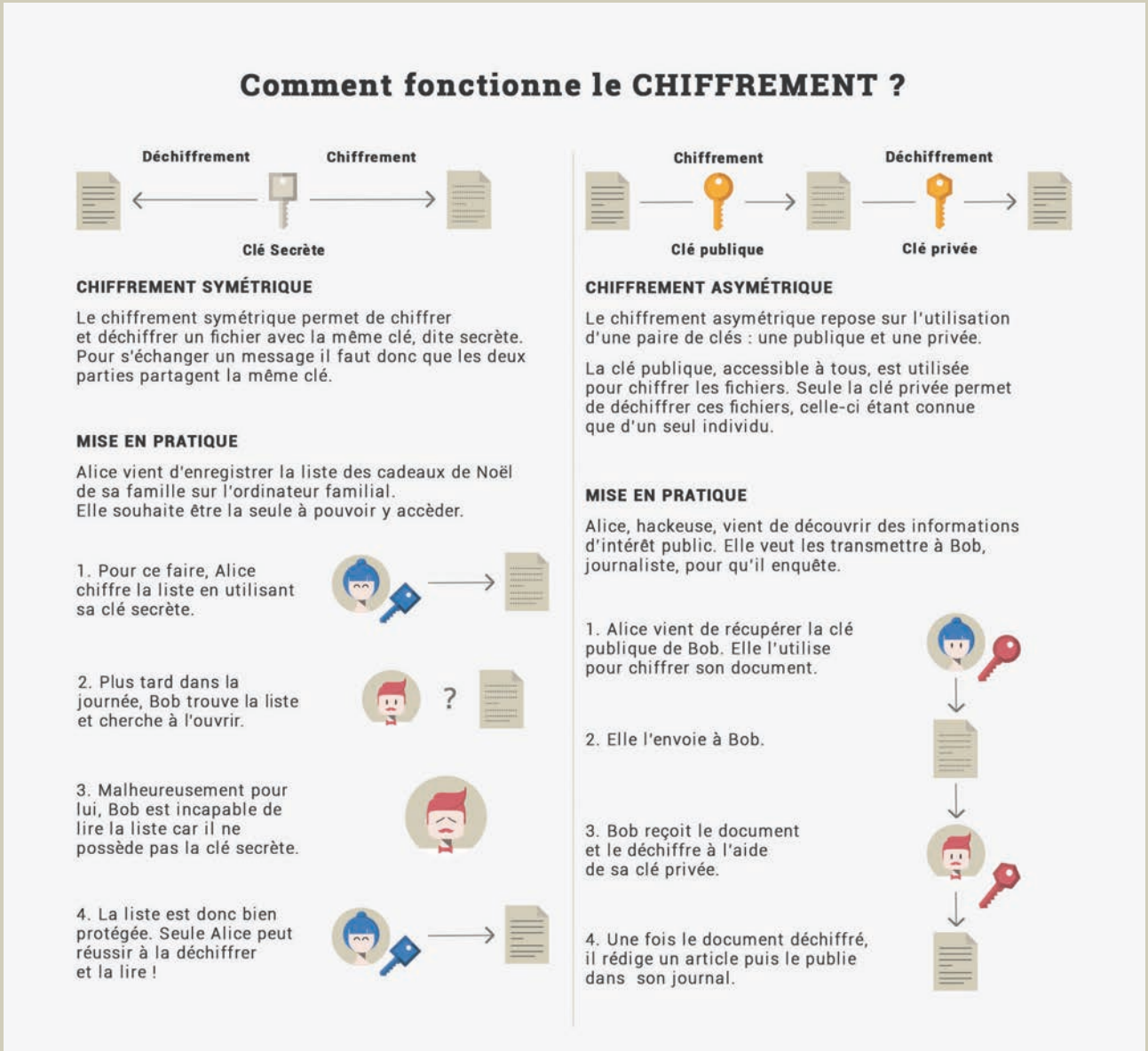


Le chiffrement asymétrique suppose que le (futur) destinataire soit muni d'une paire de clés (clé privée, clé publique) et qu'il ait fait en sorte que les émetteurs potentiels aient préalablement accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message, tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi les avantages de cette option :

- la clé publique peut être connue de tous et publiée : mais il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire ;
- plus besoin de partager une même clé secrète : le chiffrement asymétrique permet de s'en dispenser.

Ce mode de chiffrement est en revanche plus lent que le chiffrement symétrique. C'est pourquoi est dans certains cas mise en œuvre une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de **« chiffrement hybride ».**
Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque l'on visite un site dont l'adresse débute par « https ».



L'ESSOR DU CHIFFREMENT

Jusque dans les années 70, les moyens de cryptographie faisaient l'objet d'un quasi-monopole des organismes gouvernementaux. Mais la cryptologie est par la suite devenue un sujet d'étude universitaire et plus uniquement militaire, faisant ainsi l'objet de publications dans des revues académiques. Les organismes non gouvernementaux ont ainsi eu accès à un niveau de chiffrement pouvant résister aux agences gouvernementales et des controverses et conflits, connus par la suite sous le nom de Crypto War (« guerre de la cryptographie »), ont alors émergé, en particulier sur l'introduction de « portes dérobées » dans les logiciels et sur les restrictions d'exportation de la cryptographie.

À l'issue de ces débats, l'utilisation des moyens de cryptologie a été largement libéralisée dans les États occidentaux. En France, si ces moyens ont été considérés, jusqu'en 1996, comme des armes de guerre de deuxième catégorie, la législation s'est ensuite assouplie et a autorisé le chiffrement avec des clés jusqu'à 128 bits.

La loi du 21 juin 2004 modifiée pour la confiance dans l'économie numérique (LCEN) encadre dorénavant les moyens de cryptologie et prévoit notamment que « l'utilisation d'un moyen de cryptologie est libre ». Elle prévoit néanmoins des modalités de contrôle spécifique de ces outils :

- la fourniture, l'importation, le transfert intracommunautaire et l'exportation d'un moyen de cryptologie font l'objet d'un contrôle : ils sont soumis, sauf exception, à une déclaration ou à une demande d'autorisation par le fournisseur du moyen de cryptologie auprès de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) ;

- le régime applicable (déclaration ou demande d'autorisation) dépend des fonctionnalités techniques du moyen (fonctions exclusives d'authentification ou de contrôle d'intégrité ou, par exemple, prestations à des fins de confidentialité comme le chiffrement) et de l'opération commerciale projetée (fourniture, importation...) ;

- certains moyens de cryptologie sont en outre classés « matériels de guerre » : dans ce cas spécifique, les opérations relatives à ces moyens de cryptologie sont uniquement règlementées par le régime des matériels de guerre, au niveau domestique et à l'exportation ; les autorités compétentes sont alors la Direction générale de l'armement (DGA) et la Direction générale des douanes et des droits indirects (DGDDI) ;

- des sanctions administratives et pénales sont prévues en cas de non-respect, par les fournisseurs de moyens de cryptologie, de leurs obligations.

Ce cadre juridique a permis un développement sans précédent du chiffrement dans le contexte de l'utilisation massive d'Internet. Internet est en effet devenu le support principal de nos communications, privées ou professionnelles : de très nombreuses informations circulent ainsi par ce réseau ouvert et public, et non par des liens dédiés. Les solutions de chiffrement permettent ainsi de faire transiter de façon sécurisée de nombreux flux techniques ou d'informations via Internet.

INFOSPLUS

La Crypto War

Cette guerre a connu de nombreux épisodes marquants, et en particulier l'introduction des « *clipper chips* » dans les téléphones américains dans les années 90 ainsi que la création et la distribution d'un système de chiffrement à clé publique, encore utilisé aujourd'hui, dénommé Pretty Good Privacy (PGP).

Les « *clipper chips* » introduites dans les téléphones permettaient aux utilisateurs de chiffrer leurs conversations mais sur la base d'une clé maître à disposition du Gouvernement américain. Du fait de la publication des vulnérabilités de ces puces électroniques, de l'absence de marché pour les produits de chiffrement à clé maitre détenue par les Etats-Unis et d'une opposition massive du grand public, ces puces ont finalement été retirées dans les années 90.

Par ailleurs, en 1991, un militant pour les libertés individuelles, Phil Zimmermann, se sentant menacé par une législation alors en cours d'examen par le gouvernement américain qui exigerait l'inclusion de portes dérobées dans tous les produits cryptographiques développés aux États-Unis, a développé, puis distribué gratuitement Pretty Good Privacy (PGP), un système de chiffrement à clé publique. Son système a été distribué dans le monde entier peu de temps après sa distribution aux États-Unis, parfois sous la forme de logiciel mais surtout sous la forme d'un livre contenant le code source du logiciel afin de contourner les législations sur les logiciels de cryptographie.

Le département de la Justice des États-Unis a mené une longue enquête criminelle sur Phil Zimmermann pour violation alléguée de restrictions à l'exportation. Mais le département de la Justice a finalement abandonné son enquête en 1996 et la distribution gratuite de PGP a continué dans le monde entier.

Pour la littérature spécialisée, ces deux évènements ont marqué la victoire de la première « *Crypto war* » et ont grandement contribué à la libéralisation de la cryptologie.

Les données, quels que soient leur nature et leur usage (paiement, santé, police, propriété intellectuelle, etc.), la régulation de certaines infrastructures, le pilotage de certaines industries, ou encore les informations émises par les objets connectés sont autant d'éléments qui ne fonctionnent aujourd'hui que grâce à la seule mise en œuvre de solutions sécurisées à l'aide du chiffrement. Ces solutions permettent non seulement de préserver la confidentialité des données transmises mais également d'en assurer l'intégrité, dans un contexte de cybercriminalité qui vise tout autant à accéder à des informations confidentielles ou sensibles qu'à les modifier, les copier ou les supprimer.

Suite aux révélations d'Edward Snowden sur la surveillance de masse, la question de l'équilibre entre protection des données personnelles, innovation et surveillance s'est en outre placée au centre des préoccupations des entreprises et du grand public.

Ce contexte a mené à un nouvel essor du chiffrement des données. Ainsi, de plus en plus d'entreprises ont mis en œuvre des mécanismes de chiffrement, sur les flux entre leurs clients et leurs infrastructures ou entre leurs infrastructures. HTTPS est même devenu un critère dans le classement des résultats sur certains moteurs de recherche. De même, les services proposés au public en matière de télécommunications, qu'il s'agisse de services de messagerie ou de fabrication de smartphones, mettent en œuvre le chiffrement sur une part de plus en plus importante des infrastructures concernées.

> « Le chiffrement est devenu une mesure essentielle de protection de la vie privée et de sécurité des données. »

Les solutions de messageries sécurisées plébiscitées par le grand public, et notamment par les adolescents, proposent ainsi de chiffrer les données « de bout en bout », c'est-à-dire d'un utilisateur à l'autre, sans accès aux données par le fournisseur de service (par exemple, via les applications WhatsApp, Telegram, Chatsecure, etc.). Les deux principaux systèmes d'exploitation sur smartphone, ceux d'Apple et de Google, proposent également de chiffrer les données stockées sur les téléphones qu'ils produisent par des clés auxquelles ils n'ont pas accès : on parle alors de chiffrement « à la main de l'utilisateur », activé ou non par défaut selon les fabricants.

Dans ce contexte, le chiffrement est devenu une mesure essentielle de protection de la vie privée et de sécurité des données.

Le règlement général sur la protection des données mentionne ainsi expressément le chiffrement comme une des mesures techniques de nature à garantir un niveau de sécurité élevé du traitement de donnée à caractère personnel, et notamment une réduction des risques en cas de violation de données. De même, la loi Informatique et Libertés a récemment été modifiée par la loi du 7 octobre 2016 pour une République numérique, afin de mentionner le chiffrement comme une des « technologies protectrices de la vie privée » et de doter la CNIL d'une nouvelle mission de promotion de telles technologies.

L'ACCÈS DES AUTORITÉS PUBLIQUES AUX DONNÉES CHIFFRÉES : DES DISPOSITIONS NOMBREUSES

La question de l'articulation entre ces objectifs de protection de la vie privée et de sécurité du patrimoine informationnel, d'une part, et la nécessité pour les autorités publiques d'accéder aux informations qui leur sont nécessaires, d'autre part, s'est posée avec une acuité particulière ces dernières années. Le principe de l'accès, par les autorités judiciaires, aux documents, informations et données « intéressant l'enquête », « utiles à la manifestation de la vérité » ou qui peuvent servir de preuve à l'élucidation d'une infraction, est en effet au cœur des dispositions du code de procédure pénale. L'accès à des données informatiques fait ainsi l'objet de nombreuses dispositions spécifiques.

Sont ainsi prévues **les réquisitions de données**, y compris celles issues d'un système informatique ou d'un traitement de données personnelles, qui permettent d'exiger de toute personne la communication de toute donnée informatique, quel que soit son support.

Les perquisitions et les saisies de données sont encadrées par des dispositions distinctes, qui permettent de prendre connaissance, au domicile des personnes concernées, des données informatiques nécessaires à la manifestation de la vérité et de saisir le support physique de ces données ou d'en faire copie. Les autorités judiciaires peuvent dans ce cadre accéder aux données stockées dans le système informatique implanté dans le lieu où se déroule la perquisition, ainsi que dans tout autre système accessible ou disponible par l'intermédiaire du système initial. Elles peuvent également, dans les conditions de la perquisition, accéder, par un système informatique implanté dans les locaux d'un service de police judiciaire, à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial.

En pratique, ces dispositions permettent donc d'accéder, de copier ou de saisir des données informatiques, quel que soit leur support (logiciel, fichier, traitement, cloud, etc.), dans les conditions prévues par le code de procédure pénale. Dès lors que des données chiffrées ont été synchronisées de manière non chiffrée dans un autre espace de stockage, par exemple dans les serveurs d'une messagerie électronique ou dans le cloud, les autorités judiciaires peuvent ainsi accéder auxdites données.

L'accès aux données informatiques chiffrées fait également l'objet de dispositions spécifiques. La fourniture des clés de déchiffrement ou des informations déchiffrées aux autorités judiciaires, par les personnes concernées ou par des tiers, est prévue dans l'ordre juridique national : le code pénal permet de punir la personne qui, ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre une infraction, refuse de la remettre ; des peines aggravées sont prévues lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit, mais ne sont pas applicables aux personnes qui remettent aux autorités la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.

Dans le cas particulier des perquisitions, les autorités judiciaires peuvent requérir de toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition ou de leur remettre les informations permettant d'accéder à ces données. Ces dispositions, introduites en 2014, permettent ainsi aux enquêteurs de **demander à des tiers, détenteurs des codes d'accès verrouillant l'accès au contenu informatique, de les leur remettre**, afin de parer à l'absence du détenteur d'un contenu informatique ou à son refus de fournir ces codes.

Le recours à des experts techniques est également prévu. Au-delà des dispositions générales en matière de recours à des personnes qualifiées, le code de procédure pénale permet aux autorités judiciaires, aux fins de « mettre au clair des données chiffrées », de recourir à une **expertise « externe** » pour effectuer les opérations techniques permettant l'accès à des données chiffrées, leur version en clair ou la convention secrète de déchiffrement. En pratique, il s'agit donc de faire appel à un « expert en chiffrement » afin de « déchiffrer » des informations en leur disposition.

Les autorités judiciaires peuvent également faire appel à une **expertise « interne » aux services de l'État :** au-delà d'un certain seuil infractionnel, elles peuvent prescrire le recours aux moyens de l'État soumis au secret de la défense nationale, c'est-à-dire au centre technique d'assistance, rattaché au directeur général de la sécurité intérieure (DGSI) et qui dispose de puissants moyens informatiques de déchiffrement. Les organismes de police judiciaire disposent également de moyens techniques importants en matière de déchiffrement.

Enfin, au-delà des possibilités offertes aux autorités judiciaires s'agissant de l'accès aux données informatiques et en particulier aux données chiffrées, **il existe également des moyens légaux de contourner les difficultés liées à l'utilisation de solutions de chiffrement.** Si l'accès à des données chiffrées à la main de l'utilisateur peut se heurter à certaines difficultés, d'autres outils techniques permettent d'accéder aux données nécessaires à la prévention ou à la répression d'infractions graves, comme les actes de terrorisme en particulier. Des moyens spécifiques sont ainsi mis à la disposition des autorités judiciaires dans le cadre de la lutte contre la délinquance et la criminalité organisées, ainsi qu'aux services de renseignement dans le cadre de lutte anti-terroriste.

Ces autorités peuvent en effet mettre en œuvre, dans certaines conditions, de nombreuses techniques d'enquête leur permettant d'accéder aux données informatiques nécessaires à l'exercice de leurs missions de police judiciaire ou administrative. Sans être nécessairement exhaustif, on peut notamment rappeler qu'elles disposent des moyens suivants :

- **Accès aux données de connexion** des utilisateurs de services de communications électroniques, également appelées « méta-données » et dont l'exploitation est susceptible de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.

- **Interceptions de correspondances émises par la voie des télécommunications** (en matière de police judiciaire) ou interceptions de sécurité (en matière de renseignement) : initialement circonscrites aux écoutes téléphoniques, ces interceptions peuvent également concerner tout échange de correspondance par voie électronique (mail, messagerie instantanée, etc.). S'il s'agit principalement d'écoutes « en flux », c'est-à-dire d'interceptions directes de télécommunications, le code de procédure pénale permet également, en matière de criminalité organisée, l'accès aux correspondances stockées dans des messageries électroniques.

- **Enregistrements audio-visuels :** des dispositifs techniques peuvent être utilisés aux fins de capter, à l'insu des personnes concernées, des paroles ou des images dans des lieux privés.

- **IMSI-catchers :** les services de renseignement comme les autorités judiciaires peuvent utiliser des appareils permettant de capter à distance les données de connexion comme les correspondances échangées ; il s'agit en pratique de fausses antennes relais, installées à proximité (de l'ordre d'une centaine de mètres, dans l'état actuel des techniques) de la personne dont on souhaite intercepter les échanges électroniques, afin de capter l'ensemble des données transmises entre le périphérique électronique et la véritable antenne relais.

- **Captation de données informatiques :** les autorités peuvent mettre en œuvre des dispositifs techniques ayant pour objet, sans le consentement des intéressés, d'accéder et d'enregistrer des données informatiques « telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ».

Ces derniers outils ont précisément pour objet de contourner certaines mesures de chiffrement, en « interceptant » les données informatiques produites ou reçues par une personne sur son terminal électronique avant ou après toute mesure de chiffrement, c'est-à-dire avant d'être adressées par Internet par le biais d'une communication chiffrée ou une fois déchiffrées sur l'écran de l'ordinateur du récepteur.

Ces outils, qui ne peuvent être mis en œuvre que dans certaines conditions précisément établies par le code de procédure pénale ou le code de la sécurité intérieure, forment un arsenal juridique solide et relativement complet. Le cadre juridique de ces différents outils est en outre régulièrement modifié afin de mieux les adapter à l'état des différentes technologies.

Malgré ce contexte, un débat s'est fait jour, dans le monde anglo-saxon en particulier, sur l'opportunité d'obliger les fournisseurs de services de communication et les fabricants de technologies à installer des « portes dérobées » dans les systèmes de chiffrement.

LES RISQUES LIÉS À LA REMISE EN CAUSE DU CHIFFREMENT

À la suite d'attentats intervenus en 2015 et 2016, plusieurs autorités publiques ont affiché des positions défavorables au chiffrement. Confrontées à des matériels chiffrés à la main de l'utilisateur, selon des technologies de pointe, des autorités judiciaires ont en effet eu des difficultés substantielles à accéder à des informations pourtant nécessaires à leurs enquêtes, portant sur des faits particulièrement graves.

Plusieurs acteurs ont ainsi demandé à ce que soient prévues des obligations juridiques de mise en place de « *Backdoors* » dans les systèmes de chiffrement ou de mise en œuvre de « clés maitres », qui soulèvent des questions similaires aux portes dérobées, ou encore de mettre fin à la possibilité pour le grand public d'utiliser des techniques de chiffrement des données à la main des utilisateurs.
Ces options mettent néanmoins en péril le principe même de fonctionnement des technologies actuelles de chiffrement, qui reposent précisément sur l'interdiction d'accès, par des tiers, aux données ainsi protégées.

Or, un défaut de chiffrement fait peser plusieurs risques substantiels sur la cybersécurité, qui est vecteur de confiance pour les utilisateurs, particuliers ou professionnels, et d'innovation pour les industriels.

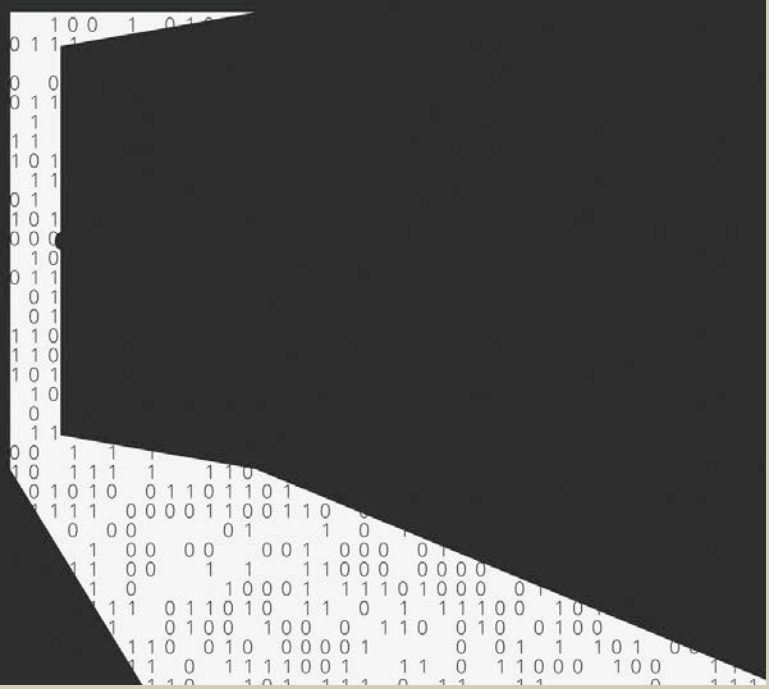
Un défaut de chiffrement peut en effet mettre en péril la sécurité des individus. On peut citer notamment l'expérience malheureuse d'une autorité publique américaine, l'OPM (Office of Personal Management), qui s'est vue dérober 22 millions de fiches concernant les employés fédéraux américains. Parmi ces fiches, les formulaires SF86 comportaient les données privées des personnes relevant de la sécurité nationale.

Il ne s'agit là que d'un exemple parmi d'autres. Dans un contexte de cybercriminalité grandissante, qui touche tous les secteurs d'activité, tous les publics (entreprises, autorités) et tous les domaines de la vie quotidienne des particuliers (données bancaires, données de santé, téléphonie, etc.), il ne peut être envisagé d'affaiblir la sécurité des solutions informatiques aujourd'hui déployées, sans que cela

DÉFINITION

BACKDOOR
ou porte dérobée

Le principe de la mise en œuvre d'une « *Backdoor* » ou porte dérobée correspond à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel.
Le principe de la mise en œuvre d'une « *Master Key* » ou « clé maître » correspond à prévoir ouvertement un tel accès, mis en œuvre via cette clé, aux données chiffrées contenues dans un logiciel ou sur un matériel.



devienne préjudiciable au patrimoine informationnel des entreprises et à la protection de la vie privée des individus. Les « *Backdoors* » créeraient ainsi un **risque collectif tendant à affaiblir le niveau de sécurité des personnes physiques comme morales face à l'ampleur du phénomène cybercriminel,** alors même que la protection des systèmes d'information des entreprises et des États devient de plus en plus impérieuse, au vu des graves préjudices que peuvent causer les atteintes à ces systèmes, du point de vue économique, politique ou de la sécurité publique.

Face aux attaques des États ou du crime organisé, les « *Backdoors* » et « *Master Keys* » seraient en outre peu robustes dans le temps, d'autant plus qu'il serait nécessaire d'échanger au niveau international le secret ou les clés concernés, les autorités publiques étant en effet confrontées aux mêmes menaces, notamment terroristes. Ces solutions seraient également très **complexes à mettre en œuvre de manière sûre :** dans le cas où une clé maître serait corrompue (obtenue par un groupe ou un État non habilités), il serait en effet très difficile de la renouveler et d'assurer la confidentialité des données qu'elle protégeait. Enfin, **même sur le court terme, leur efficacité pourrait s'avérer douteuse,** dans la mesure où les applications en cause sont majoritairement d'origine étrangère et mondialisées et où les personnes visées par ces mesures pourront toujours continuer à utiliser des solutions échappant à ces obligations.

> « Dans un contexte de numérisation croissante de nos sociétés et d'accroissement exponentiel des cybermenaces, le chiffrement est en effet un élément vital de notre sécurité. »

Pour toutes ces raisons, la CNIL comme la plupart des autorités nationales compétentes en matière de cybersécurité, à l'image de l'ANSSI par exemple, ne pense pas souhaitable une telle obligation.

DERNIÈRE MINUTE

À vos marques, prêts, chiffrez !

La loi pour une République numérique affirme une nouvelle mission pour la CNIL de promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

La CNIL a publié en mars une série de tutoriels pour sensibiliser aux technologies de chiffrement des données. En se rendant sur cnil.fr, les professionnels exposés aux risques (avocats, journalistes, médecins) mais aussi les néophytes peuvent d'ores et déjà comprendre l'intérêt du chiffrement et s'initier à des outils libres et gratuits pour protéger la confidentialité d'un poste de travail, d'un document, d'une clé USB ou d'un courrier électronique.

Une sensibilisation de premier niveau qui permettra peut-être à ces personnes d'aller plus loin dans la mise en place de procédures pour mieux protéger leurs données personnelles ou les documents confidentiels qu'elles hébergent ou qu'elles transmettent au quotidien.

Bilan d'activité

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, mène des actions de communication et s'investit particulièrement en matière d'éducation au numérique. La protection des données personnelles repose en effet sur les obligations des responsables de traitements, mais aussi sur les comportements individuels et l'exercice effectif des droits par les personnes concernées. La CNIL est également 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 d'information et de sensibilisation, la CNIL participe aussi à des colloques, des salons ou des conférences pour informer et s'informer.

Sandrine
Téléconseillère au service des relations avec les publics

Le service des relations avec les publics est le point d'entrée des appels et courriers adressés par les particuliers et les professionnels à la CNIL. Il a été créé en 2006. En tant que téléconseillère, j'ai pour mission de conseiller juridiquement les usagers, en leur prodiguant toute recommandation utile et en leur indiquant notamment les démarches à suivre ou les procédures à mettre en œuvre. Je les guide notamment à l'aide du site internet.

Les lundis, mardis, jeudis et vendredis, je réponds au téléphone de 10h à 12h et de 14h à 16h. En 2016, avec mes 6 collègues téléconseillers, nous avons reçu plus de 80 000 appels.

En dehors des permanences téléphoniques, je traite les demandes d'information adressées par voie postale ou électronique via le service Besoin d'aide. En 2016, nous avons répondu à plus de 12 000 requêtes.

Ce que j'aime dans mon métier, c'est la diversité des sujets traités. Nous sommes interrogés sur la mise en place de fichiers dans tout secteur, en particulier le monde du travail qui voit se développer les dispositifs de vidéosurveillance et de géolocalisation des salariés. Nous devons pouvoir réagir dès qu'une actualité concerne l'application de la loi Informatique et Libertés. Je considère que je suis en formation continue depuis 10 ans et c'est très enrichissant !

2 600 000
visiteurs sur cnil.fr

35
actualités

41
communiqués

LA CNIL INFORME AU QUOTIDIEN

Le nouveau site cnil.fr

En février 2016 la CNIL a mis en ligne une nouvelle version de son site internet. Plus clair, plus pédagogique, mieux adapté à la consultation sur mobile et tablette. Le nouveau site de la CNIL a été pensé pour répondre aux besoins des particuliers et des professionnels en proposant une offre éditoriale différenciée.
La CNIL a enrichi son offre éditoriale afin de conseiller les internautes sur les paramétrages protecteurs de la vie privée des réseaux sociaux, (Twitter, Snapchat), des smartphones (Pokemon Go, Bloctel).

Cnil.fr a pour ambition de se positionner comme un site de référence pour contrôler l'exposition de la vie privée en ligne ou gérer les problèmes d'e-réputation.

Un espace dédié aux professionnels propose un premier niveau de nouveaux contenus simples et illustrés pour mieux comprendre les bases des obligations Informatique et Libertés, tout en poursuivant le développement des formats à destination des professionnels plus experts.
La refonte de cnil.fr a permis d'augmenter l'audience du site de 4% par rapport à l'année 2015 avec 2 600 000 visiteurs.

Quelques chiffres sur les statistiques du site cnil.fr :

Le top 3 des actualités les plus consultées à destination des professionnels en 2016 :

« Ce que change la loi pour une république numérique pour la protection des données personnelles »
7 965 consultations

« Consultation sur le règlement européen : aidez-nous à construire le mode d'emploi opérationnel »
5 196 consultations

« Autorisation unique n°46 : procédure simplifiée pour les traitements de gestion de contentieux »
4 262 consultations

Le top 3 des actualités les plus consultées à destination des particuliers en 2016 :

« Bloctel - un nouveau site pour vous opposer au démarchage téléphonique »
59 319 consultations

« Snapchat : 5 paramètres à régler pour maîtriser ses données »
16 309 consultations

« Prenez 1 heure pour adopter de meilleurs réflexes pour votre vie privée numérique »
10 403 consultations

Le top 3 des communiqués les plus consultés en 2016 :

« Adoption du règlement européen par le parlement européen : un grand pas pour la protection des données en Europe »
19 430 consultations

« CDISCOUNT : avertissement et mise en demeure pour de nombreux manquements »
10 251 consultations

« La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi Informatique et Libertés »
7 865 consultations

FOCUS

Educnum

Educnum a connu un gros succès grâce à l'article « 5 arguments pour rappeler que la mise en ligne d'une photo de votre enfant n'est pas un acte anodin »

86 573
consultations

LINC

« Cookieviz, une dataviz en temps réel du tracking de votre navigation » est toujours autant apprécié des internautes

11 525
consultations

Une consultation des professionnels sur le mode d'emploi du règlement européen

Le 16 juin 2016 la CNIL a lancé une consultation sur le règlement européen sur la protection des données pour recueillir les questions concrètes des professionnels, leurs éventuelles difficultés d'interprétation, leurs exemples de bonnes pratiques. La consultation en ligne a porté sur les quatre thèmes inscrits au plan d'action 2016 du G29 :

- le délégué à la protection des données (DPO-Data Protection Officer),
- le droit à la portabilité,
- les études d'impact sur la vie privée (EIVP),
- la certification.

Tous ces éléments ont permis de clarifier et de rendre pleinement opératoires les nouvelles règles européennes et ont nourri les lignes directrices du G29.

225
contributeurs ont posté

540
contributions et soumis

994
votes

1 248
visiteurs ont téléchargé la synthèse de la consultation

Les réseaux sociaux : un point de contact précieux avec les usagers

Ce sont désormais 65 000 followers, 25 000 fans, et 10 000 professionnels sur LinkedIN qui portent la voix de l'institution sur les réseaux sociaux et font connaître les conseils de la CNIL en matière de vie privée et de sécurité informatique ! Les internautes n'hésitent pas à solliciter la CNIL publiquement ou en messagerie privée pour exercer leurs droits, obtenir des conseils de 1er niveau, ou signaler d'éventuels manquements. Les comptes sociaux permettent de répondre aux messages pertinents, transmettre si nécessaire aux services concernés ou réorienter l'internaute vers des institutions plus compétentes. Le temps de réponse moyen est généralement inférieur à 4 jours ouvrés*.

La CNIL, vue par les citoyens

Plus des deux tiers des Français (67%) connaissent la CNIL ne serait-ce que de nom. Ceci explique sans doute que la CNIL soit de plus en plus sollicitée, y compris pour des questions plus larges que la protection des données personnelles. La CNIL est identifiée comme protégeant les citoyens et particulièrement les internautes et défendant leurs libertés individuelles.

53% des personnes qui connaissent la CNIL déclarent voir précisément de quoi il s'agit. Ces mêmes connaisseurs de la CNIL sont 85% à affirmer qu'elle leur inspire confiance et qu'elle aide les personnes à défendre leurs droits dans l'univers numérique.

65 000
followers

25 000
fans

10 000
professionnels sur LinkedIN

* Statistique Facebook Insight réalisée sur 180 jours

LES RÉPONSES AUX PUBLICS

Le service des relations avec les publics (SRP) accueille et informe les particuliers et les professionnels désireux d'obtenir un renseignement juridique général, une aide à l'accomplissement des démarches auprès de la CNIL. Il peut être saisi via différents canaux : par courrier postal, par téléphone lors des permanences téléphoniques assurées les lundis, mardis, jeudis et vendredis, ou encore en ligne en utilisant le service « Besoin d'aide » disponible sur le site www.cnil.fr.

En 2016, les particuliers ont principalement utilisé le service « Besoin d'aide » pour solliciter la CNIL. Cet outil disponible en ligne propose 462 questions/réponses qui ont été consultées 191 860 fois en 2016. Lorsque les personnes ne trouvent pas la réponse à leur question, elles ont la possibilité d'envoyer une demande par voie électronique.

166 565
appels
(+22% par rapport à 2015)

21 718
courriers

80 215
appels pour la permanence téléphonique
(+5,7% par rapport à 2015)

12 231
requêtes reçues par voie électronique

INFOSPLUS

Le service Besoin d'aide ? en 2016

462 Questions/Réponses diffusées

191 860 consultations des Questions/Réponses

Les **10** Questions/Réponses les plus consultées :

- Interrogation du casier judiciaire par les notaires : quelles formalités à la CNIL ?
- Opt-in, opt-out, ça veut dire quoi ?
- TAJ (Traitement d'antécédents judiciaires - anciens STIC et JUDEX) : puis-je faire supprimer mon inscription ?
- Comment faire une déclaration à la CNIL ?
- «Article 31» : comment savoir si mon employeur a fait des déclarations à la CNIL ?
- Peut-on me demander mes relevés de compte pour une demande de crédit ?
- FICOBA (Fichier national des comptes bancaires et assimilés) : les héritiers peuvent-ils identifier les comptes bancaires d'un parent décédé ?
- FICOBA (Fichier national des comptes bancaires et assimilés) : qui peut le consulter ?
- La CNIL, c'est quoi ?
- Faut-il déclarer un site web à la CNIL ?

LES ACTIONS DE FORMATION AUPRÈS DU MONDE ENSEIGNANT, UN AXE PRIORITAIRE POUR 2016

Avec l'entrée du numérique à l'école, les enseignants développent des pratiques pédagogiques en s'appuyant sur une grande variété d'outils numériques. Or, ces nouveaux usages peuvent soulever des difficultés en matière de protection des données personnelles et de la vie privée, tant pour eux-mêmes que pour leurs élèves. En 2016, la CNIL et le ministère de l'éducation nationale ont signé une convention de partenariat afin de sensibiliser les élèves et les enseignants aux enjeux éthiques soulevés par le numérique et à promouvoir un usage responsable et citoyen du numérique.

Former les personnels de l'éducation nationale, en présentiel et en ligne

Un plan d'action de formation des personnels éducatifs et des cadres a été décliné tout au long de l'année 2016. La CNIL est intervenue en avril auprès des publics de l'École supérieure de l'Éducation nationale, de l'Enseignement Supérieur et de la Recherche (ESEN), dans le cadre d'un séminaire de deux jours consacré à la thématique « Éduquer aux usages responsables des réseaux sociaux ». Ce temps d'échange a permis de préciser les besoins des enseignants et de faire remonter à la CNIL des cas pratiques. Les équipes de la CNIL se sont déplacées dans les académies, pour sensibiliser des publics éducatifs variés – enseignants du premier et du second degré, chefs d'établissements, inspecteurs de l'éducation nationale, représentants de brigades de prévention de la délinquance juvénile, conseillers pédagogiques – aux enjeux liés à l'utilisation du numérique à l'école, notamment concernant les données personnelles des mineurs. Enfin, la CNIL a apporté sa contribution à des parcours M@gistère, dispositifs de formation continue en ligne destinés aux enseignants. Des contenus et des ressources pédagogiques ont ainsi été proposés pour enrichir le parcours M@gistère sur la maîtrise de l'identité numérique. En outre, il a été convenu de créer un nouveau parcours, plus juridique, à l'attention des cadres de l'éducation nationale et des chefs d'établissement, qui sera opérationnel en septembre 2017.

Cette formation, jugée prioritaire par la Direction du Numérique pour l'Éducation, a pour objectif de préciser le cadre juridique dans lequel doivent s'inscrire les pratiques numériques des enseignants et les responsabilités de chaque acteur éducatif en la matière.

Former les formateurs

La CNIL a poursuivi ses actions de formation des formateurs afin de démultiplier les messages d'éducation citoyenne au numérique, en direction de différents publics relais : Jeunes Ambassadeurs des Droits de l'Enfant (JADE), Jeunes Ambassadeurs du Numérique pour l'Utilité Sociale (JANUS), community managers des clubs de football, réseau des régulateurs africains.

Le site du collectif EDUCNUM en forte croissance

En 2016, le collectif a accueilli de nouveaux membres : la Fondation MAIF, l'association Open Law, le Groupe MGEN. Le site www.educnum.fr a élargi sa part d'audience auprès des enseignants et personnels éducatifs. Le nombre de visiteurs a ainsi doublé entre 2015 et 2016, passant de 30 000 à 60 000. Les actus et contenus pédagogiques (fiches, études, guides pratiques) mis en ligne à un rythme hebdomadaire ont permis d'alimenter régulièrement le site en contenus nouveaux et attractifs.

Les Trophées EDUCNUM, saison 3

La CNIL et le Collectif ont lancé, en novembre 2016, la 3ème édition des Trophées EDUCNUM. Les étudiants de 18 à 25 ans ont été invités à proposer des projets pédagogiques visant à sensibiliser les collégiens (10-14 ans) aux bons usages du web. Le concours a bénéficié une nouvelle fois du soutien des ministères de l'Éducation nationale et de la Jeunesse et Sports. France Télévisions et France TV éducation ont relayé la communication sur le concours, via leurs sites et leurs réseaux sociaux. La CNIL a organisé des ateliers dans des écoles et des universités, à Paris et en région, pour faire la promotion du concours et accompagner les étudiants dans la construction de leurs projets. Les lauréats de 2015 ont pu bénéficier de conseils pour développer leur projet : accompagnement du Grand Prix du jury « Data game » - un jeu de société pour les 6-10 ans - par les éditions Play Bac ; test de l'atelier proposé par le Prix coup de cœur « T KI TOI ? » dans un collège et à la Gaité lyrique.

De plus, la CNIL et le ministère de l'Éducation nationale ont décidé de lancer la 2ème édition du concours national sur les usages responsables d'Internet, en l'élargissant au second degré. Le Groupe MGEN s'est joint à cette initiative.

« Le numérique offre aujourd'hui la possibilité aux jeunes, et notamment aux jeunes femmes, d'innover, d'entreprendre, de prendre des risques. Enseigner aux plus petits les bonnes pratiques pour pouvoir utiliser le numérique en toute confiance et dans le respect de sa vie privée et de celle des autres est un vrai challenge. »

Roxanne VARZA, marraine des Trophées EDUCNUM et Directrice de la Halle Freyssinet

PROTÉGER
les citoyens

Cette année encore, la CNIL a été saisie d'un nombre de plaintes très élevé, et ce, malgré le renforcement de la réponse de premier niveau assurée par le service des relations avec les publics qui permet de mieux qualifier les plaintes pour lesquelles la CNIL est compétente et de préparer leur instruction. Le service de plainte en ligne, disponible sur le site de la CNIL, est utilisé dans 74 % des cas. Ce nombre de plaintes traduit la sensibilisation croissante des personnes aux problématiques Informatique et Libertés et leur souci grandissant de maîtriser les usages qui sont faits de leurs données.

Albane et Chloé
Juristes au service des plaintes, pôle internet/ commerce/télécoms

Nos missions consistent à conseiller les personnes sur leurs droits Informatique et Libertés et à intervenir auprès des responsables de traitement lorsqu'elles rencontrent des difficultés pour exercer leurs droits (droit d'opposition, d'accès, de rectification et de suppression)). Lorsque les personnes nous signalent le non-respect d'une autre disposition de la loi (sécurité, pertinence des données collectées etc.), nous intervenons également auprès du responsable de traitement. L'instruction se traduit généralement par des échanges écrits avec l'organisme mis en cause. Selon la nature des manquements, et la coopération de l'organisme, nous pouvons ensuite proposer le dossier au service des contrôles ou au service des sanctions. Nous travaillons donc régulièrement en collaboration avec ces services.

Au-delà de l'instruction individuelle des dossiers, le travail effectué nous permet de contribuer à la doctrine de la CNIL, qui peut être précisée à la suite de plaintes. Nous coopérons également avec nos homologues et partenaires, au niveau français (Défenseur Des Droits, DGCCRF, Signal Spam) ou européen (autorités de protection des données des autres Etats membres).

Enfin, nous participons aux actions de communication, pour sensibiliser aussi bien les particuliers que les professionnels à la loi. Notre expérience nous permet de conseiller aux personnes d'adopter de bons réflexes quand elles diffusent leurs données en ligne : vérifier si les coordonnées du responsable du site sont indiquées et s'il est possible de le contacter pour demander la suppression des contenus, vérifier le paramétrage de diffusion des informations (public ou privé), se demander s'il est nécessaire de communiquer son identité, utiliser différentes adresses mails selon les finalités etc. Si nous avons un conseil à faire passer, c'est de bien réfléchir avant de publier des photos ou opinions, de paramétrer ses comptes pour ne partager que les données nécessaires et d'en sécuriser l'accès avec des mots de passe complexes et tenus secret.

Nous constatons tous les jours à quel point il est difficile de supprimer les informations une fois en ligne.

ENCORE UN NOMBRE ÉLEVÉ DE PLAINTES EN 2016 AVEC 7 703 PLAINTES REÇUES

Cette année, les plaintes concernent principalement les secteurs internet/téléphonie et commerce qui représentent à eux deux 66% des plaintes reçues.

- **33 % des plaintes concernent la diffusion de données personnelles sur internet** (site, réseau social, blog, forum etc.). La suppression des données, une fois qu'elles sont diffusées sur internet, s'avère souvent difficile. Les obstacles rencontrés par les personnes sont variés : absence de réponse de l'organisme ou personne ayant diffusé l'information, absence de procédure en ligne, refus de l'organisme de donner suite sans motiver sa décision, nombreuses reprises d'une information erronnée, etc. Dans ce contexte, les personnes exercent tout particulièrement leur droit au déréférencement, afin de réduire la visibilité de certains résultats associés à leur nom par des moteurs de recherche. En 2016, la CNIL a ainsi reçu plus de 400 demandes de déréférencement, soit plus de 1000 demandes depuis mai 2014. Il s'agit de personnes qui contestent le refus opposé par un moteur de recherche de déréférencer un contenu web associé à leurs nom et prénom dans les résultats de recherche. En effet, pour obtenir ce « droit à l'oubli », l'internaute doit d'abord s'adresser au moteur de recherche, généralement via un formulaire en ligne. Ce n'est qu'en cas de refus que la CNIL peut intervenir. Les personnes demandent principalement la suppression de liens URL diffusés sur des blogs/forums et pages web perso, et, dans une moindre mesure, sur les sites de presse, annuaires et réseaux sociaux.

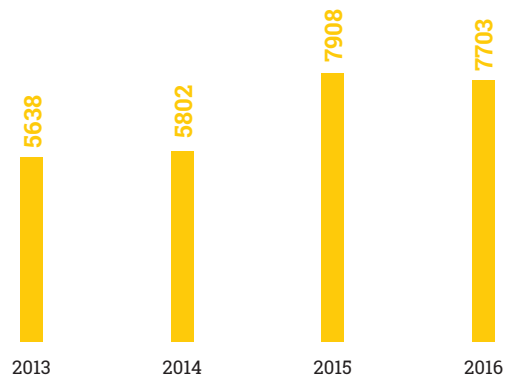
- **33 % des plaintes concernent le secteur commerce/marketing**, notamment sur la prospection commerciale par courriel, téléphone ou voie postale. Au-delà d'actions dans le cadre de l'instruction des plaintes, la CNIL est amenée à diffuser des conseils aux personnes pour leur permettre de se prémunir de démarchages non sollicités. Il est notamment recommandé de créer des adresses électroniques dédiées aux achats en ligne, aux réseaux sociaux, aux jeux et aux relations amicales, etc.

- **14 % des plaintes concernent les ressources humaines.** Le principal sujet de plainte dans le domaine du travail est la vidéosurveillance. Chaque système vidéo doit être mis en œuvre de manière proportionnée à son objectif (nombre de caméras, emplacement, orientation etc.) et respecter la vie privée des personnes filmées (pas de surveillance constante, notamment par l'intermédiaire d'un smartphone). Concrètement, sauf exception (par exemple une centrale nucléaire), un dispositif vidéo ne doit pas filmer de manière constante les employés, filmer les zones de pause, de repas, les vestiaires, les toilettes, le local syndical etc. La CNIL est également saisie de plaintes concernant le refus de la part d'employeurs de communiquer leur dossier professionnel à des salariés en faisant la demande. Elle intervient alors pour permettre aux personnes d'exercer effectivement ce droit, chaque salarié disposant d'un droit d'accès à son dossier professionnel.

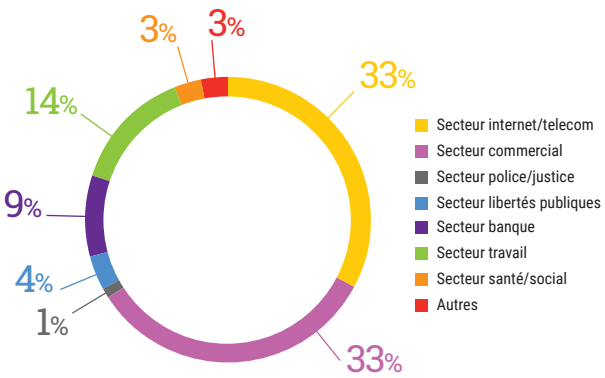
- **9 % des plaintes concernent la banque et le crédit.** Le principal motif de saisine de la CNIL reste l'absence de levée de l'inscription au fichier des incidents de crédit et de paiement (FICP) ou au fichier central des chèques et cartes après régularisation (FCC), qui peut avoir des conséquences particulièrement dommageables pour les personnes maintenues à tort dans le fichier.

- **3 % des plaintes concernent le secteur santé et social.** La majorité des plaintes est liée aux difficultés invoquées par les personnes pour accéder à leur dossier personnel (dossier médical, dossier CAF, Pôle emploi etc.). La CNIL a également reçu plusieurs plaintes relatives à la création de dossiers pharmaceutiques sans le consentement des personnes concernées.

Évolution du nombre de plaintes depuis 2013



Répartition des plaintes par secteur d'activité



Histoires vécues...

FUITE DE DONNÉES EN LIGNE

M. et M^me^ DUMONT ont pour projet de créer une chambre d'hôte à la campagne. Pour cela, ils contractent un prêt immobilier et donnent de nombreuses informations personnelles à leur assurance. Pour promouvoir la future « chambre d'hôte » sur les réseaux sociaux, Madame décide d'indexer la future demeure sur internet sur la base de son nom de famille. Elle découvre, en tapant ses nom et prénom sur les moteurs de recherche, que des données personnelles relatives à sa demande de prêt ainsi que celles de son mari apparaissent dans la liste des résultats.
M^me^ DUMONT réalise alors que n'importe qui peut savoir où elle vit, quelle est sa date de naissance, quel est le nombre et les montants de ses prêts immobiliers, mais aussi son poids, sa taille et des informations d'ordre médical données pour l'assurance du prêt ! Catastrophé, le couple saisit la CNIL.

La CNIL déclenche un contrôle dans les locaux de la société et constate que la diffusion des données sur internet résulte d'une fuite de données liée à une erreur de paramétrage d'un serveur et que tous les clients de la société sont potentiellement concernés par cette diffusion massive d'informations sensibles. Dans le cadre de ce contrôle, la CNIL rappelle à la société ses obligations en matière de sécurité et de confidentialité des données. Compte tenu de la gravité des faits constatés, la CNIL demande immédiatement à la société de rectifier ce paramétrage et une procédure de sanction est initiée. La formation restreinte de la CNIL constatant plusieurs insuffisances, décide d'adresser un avertissement à l'encontre de la société.

Parallèlement, la CNIL conseille aux plaignants d'effectuer une demande de déréférencement auprès des moteurs de recherche.

Les données du couple DUMONT et des autres plaignants ne sont rapidement plus en ligne.

DÉRÉFÉRENCEMENT D'INFORMATIONS DIFFUSÉES SUR UN BLOG

À la suite du refus adressé par le moteur de recherche à sa demande, Julien se tourne vers la CNIL pour obtenir le déréférencement d'articles, publiés sur un blog, relatant les actions d'un comité de soutien qui s'était créé en réaction à son licenciement.

Le moteur de recherche avait initialement refusé d'accéder à sa demande, considérant que les informations étaient relatives à la vie professionnelle de Julien et qu'elles présentaient un intérêt pour le public.

La CNIL a une analyse différente. En raison de l'ancienneté des articles, datant de sept ans, l'information n'est plus d'actualité. De plus, le blog n'étant plus administré depuis plusieurs années, il est impossible pour Julien d'exercer ses droits auprès du responsable du blog pour obtenir la suppression des contenus. La CNIL décide donc d'appuyer sa demande et, après un second examen, le moteur de recherche accepte d'y donner une suite favorable.

SUBVENTION DES ASSOCIATIONS ET NOMS DES ADHÉRENTS

Plusieurs associations ont saisi la CNIL de plaintes relatives à des demandes de communication par les mairies de la liste nominative de leurs adhérents pour bénéficier de subventions. La CNIL est intervenue auprès des mairies concernées afin de leur rappeler que de telles demandes ont été reconnues contraires au principe de la liberté d'association par le Conseil d'État en 1997 et ne constituent pas des données pertinentes au sens de la loi Informatique et Libertés. Les mairies ont renoncé à demander les noms des adhérents et limitent leur collecte au nombre d'adhérents, ce qui est une information suffisante pour les demandes de subvention.

INSTALLATION D'UN LOGICIEL ESPION POUR CONTRÔLER LE TRAVAIL D'UN SALARIÉ

Manon se rend compte qu'un logiciel de contrôle à distance est installé sur son ordinateur professionnel. Tous les jours, son chef contrôle et modifie son travail par ce biais. Il peut, à loisir, consulter son dossier personnel, ses courriers et toutes ses saisies.

Elle écrit à la CNIL pour faire cesser ce contrôle permanent et qu'elle estime intrusif.

La CNIL adresse alors un courrier à son employeur afin de lui rappeler que l'installation d'un logiciel de contrôle à distance n'est pas en soi illégale, mais qu'en revanche son utilisation doit respecter les règles Informatique et Libertés. Le recours à un dispositif de contrôle de l'activité doit ainsi d'être proportionné au regard de l'objectif poursuivi, ce qui n'est pas le cas d'un système qui permet de contrôler tout ce que fait un salarié en permanence.

A l'issue des échanges avec la société, l'employeur a décidé de mettre en place d'autres méthodes de contrôle de l'activité de Manon.

CONSERVATION DES DONNÉES BANCAIRES SUR UN SITE DE VENTE EN LIGNE

Après avoir acheté un livre sur un site internet, Emilie a la mauvaise surprise, lors d'un achat ultérieur, de constater que ses données bancaires sont pré-remplies sur le formulaire de commande. Or, quand elle avait acheté son livre, Emilie n'avait pas coché la case autorisant la conservation de ses coordonnées bancaires. Emilie saisit la CNIL, qui décide de contrôler le site concerné. Cette pratique étant confirmée, une mise en demeure est adoptée. Cette mise en demeure est clôturée à la suite de la mise en conformité de la société concernée.

ACCÈS À SON DOSSIER PROFESSIONNEL

Olivia adresse un courrier à son employeur pour solliciter la communication du décompte de ses heures de travail. Sa demande étant restée sans réponse, elle saisit la CNIL d'une plainte.

La CNIL intervient alors pour rappeler à son employeur ses obligations en matière de droit d'accès.

A la suite de cette intervention, la société a communiqué à Olivia le décompte de ses heures de travail.

ACTES ADMINISTRATIFS : ATTENTION AUX SITES NON OFFICIELS

La CNIL a constaté depuis plusieurs années l'émergence de sites web spécialisés dans l'intermédiation payante de services administratifs gratuits (demande d'actes d'état civil, de carte grise ou de relevé de points de permis de conduire etc.). Indexées contre rémunération dans les premiers résultats des moteurs de recherche, les annonces vantant les mérites de ces sites, dont l'activité n'est pas illégale, sont une source de confusion pour l'administré qui se méprend souvent sur leur caractère officiel.

En 2016, la CNIL a de nouveau été saisie de cette pratique. Plusieurs administrés d'une commune d'Ile-de-France sont passés par ces sites web et ont été débités de la somme forfaitaire prévue mais n'ont jamais reçu les actes demandés.

Pour rappel, toute personne peut gratuitement effectuer une demande d'acte d'état civil :
www.service-public.fr,
rubrique « Service en ligne » ou directement sur le site web officiel de la commune de naissance.

CE QUI CHANGE AVEC LE RÈGLEMENT ET LA LOI RÉPUBLIQUE NUMÉRIQUE

Le règlement comporte plusieurs avancées pour la protection des droits des personnes. La logique qui sous-tend ce texte est celle du renforcement de la maîtrise par l'individu du devenir de ses données. Cela se traduit par l'apparition de nouveaux droits, tels que le droit à la portabilité des données, le droit à la limitation du traitement ou le droit à réparation d'un dommage matériel ou moral. La notion de consentement est précisée et l'impératif de transparence affirmé.Les obligations en matière d'information sont également renforcées, notamment en cas de faille de sécurité.

Parallèlement, des dispositions spécifiques sont introduites pour le traitement des données des enfants, avec un droit d'opposition renforcé.

Ces changements seront applicables en mai 2018. Mais la loi pour une République numérique a d'ores et déjà introduit de nouvelles dispositions en reconnaissant aux personnes un droit de décider et de contrôler les usages qui sont faits de leurs données (droit à « l'autodétermination informationnelle »), la possibilité d'organiser le sort de celles-ci après leur mort ou d'exercer leurs droits par voie électronique. Un droit à l'oubli pour les mineurs est également consacré et les modalités d'information renforcées.

LE DROIT D'ACCÈS INDIRECT : UNE ANNÉE DE RELATIVE STABILISATION

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) peuvent en effectuer la demande par écrit auprès de la CNIL.

4 381 personnes se sont adressées à la CNIL en 2016 pour exercer leur droit d'accès indirect, ce qui marque, après 5 années consécutives de forte progression, une relative stabilisation des demandes en ce domaine.

La baisse globale des demandes (5 890 demandes en 2015) est liée à la mise en place, au 1er janvier 2016, du droit d'accès direct au fichier FICOBA pour les héritiers et notaires dans le cadre des successions (article L151 B du livre des procédures fiscales). Toutes les demandes de cette nature reçues par la CNIL après cette date ont été transférées pour traitement à l'administration fiscale en application des dispositions de l'article L 114-2 du code des relations des usagers avec l'administration, soit plus de 1 000 dossiers.

La CNIL demeure compétente, au titre du droit d'accès indirect, uniquement pour les demandes de particuliers qui souhaitent obtenir la communication des données relatives à leurs propres comptes bancaires enregistrées dans ce fichier. Ces demandes sont notamment formulées pour rechercher l'établissement détenteur d'un livret A, s'assurer de l'absence d'ouverture frauduleuse de comptes après la perte ou le vol de pièces d'identité ou obtenir un état des comptes détenus dans le cadre d'une procédure de divorce.

4 381

demandes

8 101

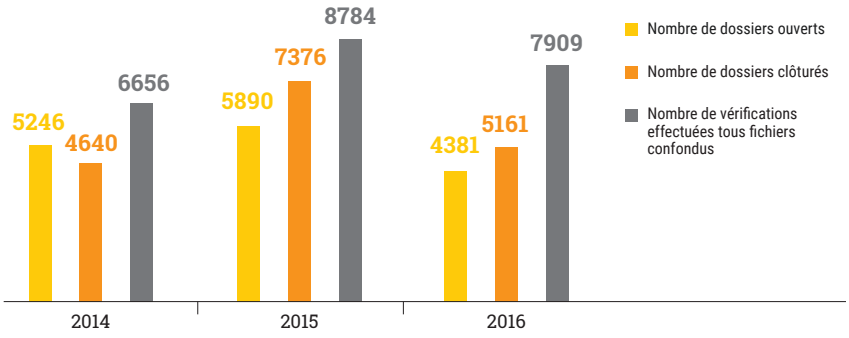
vérifications à mener

INFOSPLUS

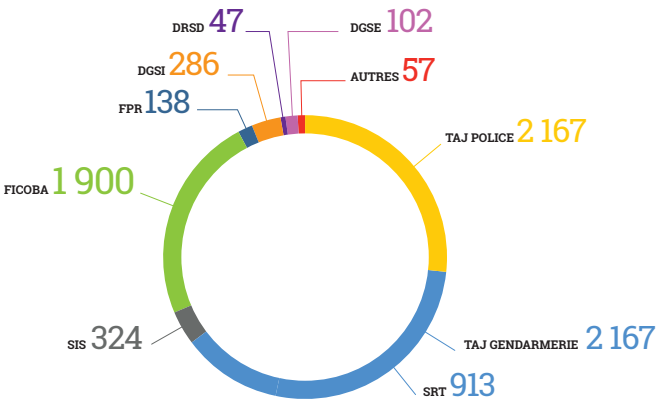
Le droit d'accès indirect comment ça marche ?

A réception de la demande accompagnée d'une copie d'un titre d'identité, un membre 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.

Évolution des demandes de droit d'accès indirect 2014/2016



Demandes de droit d'accès indirect 2016 : répartition par fichier des vérifications à effectuer



FICOBA : Fichier des Comptes Bancaires et Assimilés

TAJ police : Traitement d'Antécédents Judiciaires (procédure police)

TAJ gendarmerie : Traitement d'Antécédents Judiciaires (procédure gendarmerie)

SRT : services de renseignement territorial

SIS : Système d'Information Schengen

FPR : Fichier des Personnes Recherchées

DGSI: Direction Générale de la Sécurité Intérieure

DGSE: Direction Générale de la Sécurité Extérieure

DRSD : Direction du Renseignement et de la Sécurité de la Défense

Autres : Fichier des Courses et Jeux (FICOJ), Fichier des Interdits de Stades (FNIS), fichier relatif à la gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS), Europol…

Une progression des demandes d'accès au fichier TAJ

L'activité du service du droit d'accès indirect demeure néanmoins soutenue car le nombre de demandes relatives au Traitement d'Antécédents Judiciaires (TAJ), qui impliquent des vérifications importantes, en lien avec les services gestionnaires de fichier et les procureurs de la République territorialement compétents, a parallèlement progressé (+ 34%).

Cette évolution est notamment liée au contexte de l'état d'urgence et à la réception, au cours de l'année 2016, de plus de 400 demandes de ressortissants français souhaitant travailler sur le territoire suisse dans le domaine de la sécurité. En effet, les autorités de cet État ont imposé à ces personnes l'exercice de leur droit d'accès indirect auprès de la CNIL pour obtenir les données issues du fichier TAJ dans le cadre de leur enquête préalable de moralité.

Cette situation a été régularisée à la fin de l'année 2016 par une modification de l'article R. 40-29 du code de procédure pénale, pris après avis de la CNIL, qui permet désormais aux services de police français de procéder, sous certaines conditions, à des échanges d'informations sur les données de ce fichier avec leurs homologues étrangers dans le cadre d'enquêtes administratives. Cette procédure évite aux personnes de devoir exercer leur droit d'accès indirect, puisque les données sont directement échangées entre les autorités compétentes.
Afin de répondre à l'ensemble des attentes de la personne concernée, chaque demande reçue implique généralement qu'il soit procédé à des vérifications dans plusieurs traitements. Les 4 381 demandes reçues au cours de l'année 2016 représentent ainsi un total de 8 101 vérifications à mener. Concernant le fichier TAJ, une demande adressée à la CNIL implique une double vérification auprès des services de police et de gendarmerie.

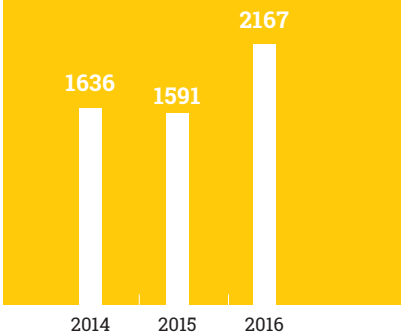
Au cours de l'année 2016, 7 909 vérifications ont été effectuées dont 54% ont porté sur le Traitement d'Antécédents Judiciaires (TAJ).

L'ensemble des vérifications menées en 2016 pour les procédures établies par la police nationale s'est traduit par :

- la suppression de 15% des enregistrements examinés,
- la mise à jour par mention des suites judiciaires favorables intervenues dans 21% des cas, ce qui a eu pour effet de rendre les personnes « inconnues » de ce fichier dans le cadre d'une consultation administrative (enquêtes pour l'obtention d'un agrément ou d'une habilitation pour l'exercice d'un emploi par exemple).

L'effet des mises à jour s'avère toujours plus important pour les personnes enregistrées dans le fichier par la gendarmerie nationale (39 %) car les affaires associées sont, à titre général, moins nombreuses et l'obtention d'une réponse de la part des procureurs de la République concernés est le plus souvent facilitée.

Demandes relatives au Traitement d'Antécédents Judiciaires (2014-2016)



2 167

demandes d'accès au TAJ

34%

de plus par rapport à 2015

7 909

vérifications ont été effectuées en 2016

54%

ont porté sur le TAJ

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	2307	1973
Nombre de personnes inconnues	614	1397
Nombre de personnes enregistrées uniquement en tant que victimes	348	188
Nombre de fiches de personnes « mises en cause » vérifiées	1345	388
- dont pourcentage de fiches supprimées	15%	16%
- dont pourcentage de fiches mises à jour par mention de la décision judiciaire favorable intervenue (acquittement, relaxe, non-lieu, classement sans suite) rendant la personne inconnue du fichier sous le profil de consultation administrative (enquêtes administratives)	21,5%	39%
- dont pourcentage de fiches rectifiées ayant eu pour effet de réduire le délai global de conservation de l'enregistrement	0,5%	0,5%
- dont pourcentage 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 procureurs de la République sur les suites judiciaires intervenues)	63%	44,5%

À RETENIR

De nouvelles conditions d'effacement du fichier TAJ

Afin de répondre à la condamnation de la France par la Cour européenne des droits de l'homme le 18 septembre 2014 (arrêt Brunet contre France), l'article 230-8 du code de procédure pénale qui fixe les conditions d'effacement de ce fichier a été modifié par la loi n° 2016-731 du 3 juin 2016.

Les procureurs de la République ou le magistrat référent en charge de ce fichier ont désormais la faculté de prescrire l'effacement d'infractions ayant bénéficié d'une décision de classement sans suite quel qu'en soit le motif (rappel à la loi, dédommagement de la victime). Leur décision concernant l'effacement ou le maintien des faits se fonde sur des motifs liés à la finalité de ce fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé.

Alors qu'elles étaient jusqu'à présent uniquement contestables devant le juge administratif, ces décisions doivent désormais faire l'objet d'un recours devant le président de la chambre de l'instruction du tribunal de grande instance (TGI) concerné ou, s'agissant de celles rendues par le magistrat référent, devant le président de la chambre de l'instruction de la Cour d'Appel de Paris. Un décret en Conseil d'État, qui sera soumis à l'avis de la CNIL, doit préciser les modalités de ces recours en termes de recevabilité et de délais.

Les effets de cette modification législative sont d'ores et déjà perceptibles dans le cadre des vérifications menées au titre du droit d'accès indirect : 7 personnes ont ainsi bénéficié au cours du second semestre 2016 d'un effacement de ce fichier, sur décision du procureur de la République, pour des faits ayant bénéficié de classement sans suite dont le motif n'ouvrait pas précédemment une telle possibilité.

FOCUS

Le contentieux du droit d'accès indirect relevant de la nouvelle formation spécialisée du Conseil d'État, chargée de procéder au contrôle de la régularité de l'inscription dans les fichiers intéressant la sûreté de l'État.

Une formation spécialisée a été instituée au sein du Conseil d'État par la loi n°2015-912 du 24 juillet 2015 relative au renseignement. Cette formation est compétente pour connaître du contentieux relatif à la mise en œuvre des techniques de renseignement, et de celui portant sur l'exercice du droit d'accès indirect à certains fichiers intéressant la sûreté de l'État dont la liste est définie par décret.

Elle peut être saisie par les personnes qui contestent la décision de refus de communication des données figurant dans ces fichiers, telle que révélée par la lettre de la présidente de la CNIL, adressée au terme des vérifications menées par un magistrat en charge du droit d'accès indirect.

Champ de compétence de la formation spécialisée (article R.841-2 du code la sécurité intérieure)

9 fichiers relèvent actuellement de la compétence de cette formation, à savoir :

- le fichier de la Direction Générale de la Sécurité Intérieure (DGSI)
- le fichier de la Direction Générale de la Sécurité Extérieure (DGSE)
- le fichier SIREX de la Direction du Renseignement et de la Sécurité de la Défense (DRSD)
- le fichier de la Direction du Renseignement Militaire (DRM)
- le fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)
- le fichier des personnes recherchées, uniquement pour les données intéressant la sûreté de l'État
- le Système d'Information Schengen (SIS) pour les données mentionnées au 2° de l'article R.231-7 du code de la sécurité intérieure
- le fichier du service à compétence nationale TRACFIN pour les données intéressant la sûreté de l'État
- le fichier BCR-DNRED de la Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)

Les requêtes portant sur la partie des fichiers non concernée par ces dispositions ou sur tout autre fichier relevant du droit d'accès indirect demeurent de la compétence du Tribunal Administratif de Paris en premier ressort.

Rôle et portée des décisions (article L.773-8 du code de justice administrative)

La formation spécialisée a accès, sans restriction et en dehors du contradictoire, à l'ensemble des données figurant dans le fichier, objets du litige.

L'accès à ces données lui permet de vérifier si la personne fait ou non l'objet d'un enregistrement et, si elle y figure, si les données la concernant sont pertinentes au regard de la finalité du fichier, adéquates et proportionnées.

- En l'absence de toute irrégularité, la formation spécialisée rejette la requête sans pouvoir apporter de plus amples précisions à la personne, y compris si elle s'avère inconnue du fichier ;
- En cas de constat d'une irrégularité, elle en informe la personne sans faire état d'aucun élément protégé par le secret de la défense nationale afin de lui permettre d'engager, si elle le souhaite, une action en responsabilité. Elle peut également ordonner que les données soient, selon les cas, rectifiées, mises à jour ou supprimées par le responsable du traitement.

La formation spécialisée est, sur le plan légal, uniquement chargée de procéder au contrôle de la régularité de l'inscription des données. Il ne lui revient pas d'apprécier le bien-fondé du refus de communication du responsable du traitement ni d'enjoindre ce dernier à communiquer tout ou partie des données à la personne concernée.

Au cours de l'année 2016, la CNIL a produit des observations dans le cadre de 102 requêtes affectées à cette formation spécialisée dont certaines renvoyées, par ordonnance, par le Tribunal Administratif de Paris initialement saisi. La formation spécialisée s'est réunie à deux reprises au second semestre 2016 et a d'ores et déjà pris 29 décisions (rejet des requêtes en l'absence d'irrégularité). Elle s'est également prononcée sur une question prioritaire de constitutionnalité.

Histoires vécues...

MONSIEUR K, 53 ANS, a appris qu'il faisait l'objet d'une inscription dans le fichier TAJ pour des faits dont il n'était nullement l'auteur mais pour lesquels il avait déposé plainte au nom de la société en sa qualité de gérant. Les vérifications de la CNIL ont conduit à la suppression de cette infraction (« escroquerie, faux documents concernant la circulation de véhicules, recel, contrefaçon, fraudes industrielles ou commerciales, abus de confiance ») qui lui avait été imputée à tort.

MONSIEUR F, 39 ANS, a souhaité engager une procédure de droit d'accès indirect au fichier TAJ après avoir reçu, dans le cadre de l'instruction de sa demande de renouvellement de sa carte professionnelle d'agent de sécurité privée, une lettre du CNAPS (Conseil National des Activités Privées de sécurité) faisant état d'une infraction datant de plusieurs années. En l'occurrence, Monsieur F faisait l'objet d'une inscription pour « délit de fuite » dont il n'était pas l'auteur puisque, non seulement à l'heure des faits il était sur son lieu de travail, mais surtout parce que cette affaire était imputable à la personne à laquelle il avait vendu son véhicule quelques semaines auparavant. Le procureur de la République ayant classé l'affaire pour « absence d'infraction », l'inscription a été effacée.

MONSIEUR C, 27 ANS, n'a pu obtenir le renouvellement de son contrat par son employeur en raison de l'enquête administrative menée, qui a révélé son inscription dans le fichier TAJ en tant qu'auteur d'une infraction. Au terme des vérifications de la CNIL, l'infraction de « menaces de mort faites sous condition », à laquelle s'appliquait un délai de conservation de 20 ans, a été requalifiée en « injures non publiques » et a été immédiatement supprimée car il s'agit d'une contravention de 4ème classe qui n'a pas vocation à faire l'objet d'une inscription dans ce fichier.

MONSIEUR H, 25 ANS a engagé une procédure de droit d'accès indirect auprès de la CNIL qui a révélé son inscription dans le fichier TAJ pour une affaire de « vol », requalifiée par le procureur de la République en « vol en réunion » auquel s'applique un délai de conservation de 40 ans. L'intéressé, accompagné d'un ami, avait pris possession d'une bicyclette en mauvais état déposée aux encombrants sur la voie publique dans le but d'en assurer la réparation. Les démarches de la CNIL ont permis, avec l'accord du procureur de la République, d'assurer la suppression de ces faits pour lesquels l'intéressé avait bénéficié d'un classement sans suite pour infraction insuffisamment caractérisée.

MONSIEUR S, 47 ANS, exerçait les fonctions d'agent de sécurité privée depuis de nombreuses années mais, à l'occasion du renouvellement de sa carte professionnelle, le CNAPS lui a opposé un refus au motif de son enregistrement dans le fichier TAJ en qualité de mis en cause pour une affaire de « vol avec arme » qui s'était déroulée dans le supermarché dans lequel il exerçait ses fonctions. Il avait effectivement été entendu dans le cadre de l'enquête judiciaire en raison de suspicion de complicité avec les auteurs de ce braquage. Au terme des vérifications menées par la CNIL, cette infraction a été supprimée, en accord avec le procureur de la République, car il avait bénéficié d'une décision judiciaire favorable (décision de classement sans suite pour infraction insuffisamment caractérisée).

MONSIEUR T, 34 ANS, admis sur liste complémentaire dans le cadre d'un concours organisé pour l'entrée dans une administration régalienne a appris que tous les lauréats étaient soumis à une enquête de moralité s'appuyant notamment sur la consultation du fichier TAJ. Au terme des vérifications sollicitées auprès de la CNIL, l'enregistrement dont il faisait l'objet pour « vol simple, falsification de chèques ou usage de chèques contrefaits » a été supprimé, en accord avec le procureur de la République, car il avait bénéficié d'une décision de classement sans suite pour infraction insuffisamment caractérisée.

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 pour les organismes publics et privés. En 2016, le nombre de décisions prises par la CNIL a été particulièrement important et notamment les avis, dont certains ont dû faire l'objet d'une instruction en urgence.

Céline
Juriste au service des affaires régaliennes et des collectivités territoriales

Le service des affaires régaliennes et des collectivités territoriales est composé de 8 personnes, organisé autour de trois grands « pôles », « police, justice, renseignement », « éducation nationale » et « finances publiques, collectivités territoriales, données publiques ». Les sujets sont donc particulièrement nombreux et riches. L'activité principale du service est d'instruire les dossiers de formalités préalables, c'est-à-dire les demandes d'autorisation et les demandes d'avis formulées par les responsables de traitements, en vue de leur examen par la Commission.

Aussi, nos interlocuteurs privilégiés sont les organismes publics, principalement les ministères (justice, intérieur, économie et finances, éducation nationale, etc.) et les collectivités territoriales. Nous répondons aussi aux demandes de conseil afin d'expliquer le droit applicable ou la position de la CNIL. Nous pouvons participer à des contrôles sur place et nous avons régulièrement des interventions à l'extérieur.

En charge des dossiers « police/justice/renseignement » avec l'une de mes collègues, notre activité principale consiste à préparer, sous l'autorité et en étroite collaboration avec les Commissaires de la CNIL, les projets de délibération examinés lors de séances plénières. La rédaction de ces avis intervient après des échanges poussés avec les ministères, par écrit ou à l'occasion de réunions.

Nous traitons environ 40 dossiers « police/justice/renseignement » par an, dont beaucoup sont en prise directe avec l'actualité et peuvent être particulièrement sensibles ; dans tous les cas, la CNIL doit trouver un équilibre entre des intérêts qui peuvent paraître contradictoires (vie privée, protection des données, protection de l'ordre et de la sécurité publics, etc. Enfin, comme cela a été le cas cette année, il n'est pas rare que l'on soit saisi en urgence ce qui impose d'être particulièrement réactif et organisé.

Cette réactivité, ce rapport avec l'actualité et les grands enjeux auxquels doivent faire face l'administration, rendent nos activités passionnantes, mais aussi très exigeantes.

FOCUS

Une nouvelle méthodologie de référence pour les recherches dans le domaine de la santé

Après concertation avec les principaux acteurs de la recherche en matière de santé, la CNIL a adopté, le 21 juillet 2016, une nouvelle méthodologie de référence (MR) relative aux traitements de données à caractère personnel mis en œuvre dans le cadre de recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès ou écrit de la personne concernée, la MR-003.

Cette nouvelle norme, source de simplification administrative permet un de gain de temps dans la mise en œuvre de nombreuses recherches.

Le même jour a été publiée une nouvelle version de la MR-001 dont l'évolution était rendue nécessaire par les dernières évolutions législatives et réglementaires touchant la recherche clinique.

Les travaux de simplification en matière de recherche dans le domaine de la santé se poursuivront en 2017, afin de faciliter les démarches et de favoriser la mise en œuvre des projets dans des délais garantissant la compétitivité de la France dans ce secteur.

En 2016, plus de 900 dossiers de recherche ont fait l'objet d'un engagement de conformité.

LA SIMPLIFICATION DES FORMALITÉS ADMINISTRATIVES : DES ALLÈGEMENTS QUI PORTENT LEURS FRUITS

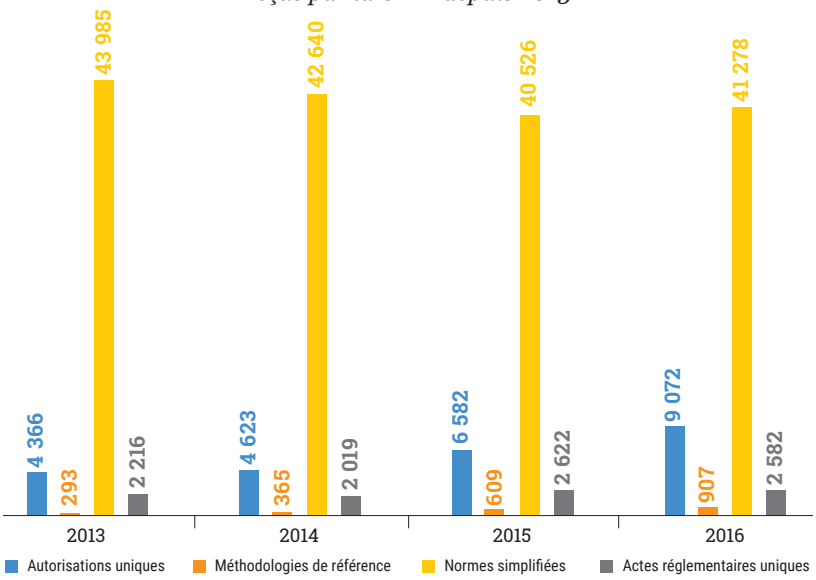
La CNIL est engagée depuis plusieurs années dans un processus de simplification administrative auprès des organismes publics et privés. Elle peut adopter des dispenses de déclaration, des normes simplifiées pour les traitements soumis à régime déclaratif, des autorisations uniques pour les traitements soumis à régime d'autorisation et des méthodologies de référence pour les recherches les plus courantes en matière de santé.

Pour les traitements du secteur public, la Commission rend des avis sur des projets d'actes réglementaires uniques dont la création reste à l'initiative des administrations concernées. Cependant, elle conseille et accompagne ces dernières afin d'alléger les formalités à accomplir (par exemple pour l'Éducation nationale ou pour les collectivités territoriales qui mettent en œuvre de nombreux traitements similaires).

Les normes de simplification adoptées par la CNIL permettent d'alléger considérablement les formalités des entreprises et des administrations, tout en homogénéisant les pratiques et en promouvant les plus vertueuses. En effet, les organismes n'ont qu'à faire un engagement de conformité à la norme concernée préalablement à la mise en œuvre de leur traitement. Cet engagement peut être accompli en ligne sur le site de la CNIL en quelques minutes.

En 2016, les effets de la simplification des formalités ont été particulièrement sensibles, notamment dans le champ des autorisations avec plus de 9 000 engagements de conformité reçus. Élaborés après concertation avec les acteurs d'un secteur, ces cadres demandent un investissement ponctuel important, mais se traduisent par la simplification de dizaines de milliers de démarches (plus de 54 000 dossiers pour 2016).

Nombre d'engagements de conformité à une norme de simplification reçus par la CNIL depuis 2013



LES AVIS ET AUTORISATIONS DE LA CNIL

Au titre de ses missions de contrôle a priori des fichiers et de conseil, la CNIL est notamment chargée d'autoriser les traitements de données les plus sensibles et de rendre des avis sur les projets de textes en séance plénière. En outre, en 2016, la Commission a été amenée à rendre 145 avis dont certains en urgence dans des délais très contraints.

Certaines autorisations ne sont cependant pas examinées en séance plénière et font l'objet d'une délégation de la plénière au Président et au Vice-président délégué. Toutefois, la Commission reste compétente pour examiner, à la demande du Président, celles des demandes d'autorisation qui présenteraient des difficultés ou une complexité particulières.

L'avis de la CNIL sur la vidéosurveillance dans les cellules de détention

La CNIL a rendu le 19 mai 2016 un avis sur un arrêté encadrant la mise en œuvre par l'administration pénitentiaire d'une vidéosurveillance permanente de certains détenus dont l'évasion ou le suicide pourrait avoir un impact important sur « l'ordre public ou l'opinion publique ». Il s'agit en effet de s'assurer qu'elles n'attentent pas à leur vie et ne tentent pas de s'évader, garantissant ainsi qu'elles répondent de leurs actes devant la justice.

La Commission a rappelé dans son avis que ce type de dispositif intrusif devait reposer sur une base légale suffisante, que les détenus concernés devaient être strictement définis et que ces dispositifs ne pouvaient être mis en œuvre qu'à titre exceptionnel.

Une mesure exceptionnelle qui doit faire l'objet de garanties fortes

Si la légitimité des objectifs poursuivis par ces dispositifs n'est pas contestée, l'utilisation de caméras vidéo filmant en permanence certains détenus soulève de forts enjeux, tant en matière de respect des libertés individuelles que du cadre juridique dans lequel ils doivent s'inscrire.

La Commission a tout d'abord rappelé que ces dispositifs, particulièrement intrusifs, devaient reposer, conformément à la Convention européenne des droits de l'homme et des libertés fondamentales, sur une base légale suffisante et assurant un équilibre entre l'ingérence dans la sphère privée du détenu et les troubles à l'ordre public qui résulteraient de son suicide ou de son évasion.

À cet égard, la Commission relève que l'arrêté publié prévoit plusieurs garanties procédurales permettant un encadrement plus précis de la mise en œuvre de ce dispositif (mention exprès du caractère exceptionnel de la mesure ; information de la personne détenue ; possibilité de faire valoir ses observations dans le cadre d'une procédure contradictoire et d'être assisté d'un avocat ; procédure spécifique en cas d'urgence ; avis écrit du médecin à tout moment, ce à quoi le ministère s'était engagé dans le cadre de l'instruction du dossier).

En outre, la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste est venue encadrer ces dispositifs et leur donner une base législative. La Commission a donc été suivie dans ses recommandations.

Un champ d'application à limiter

La CNIL a estimé que le champ des personnes concernées devait être strictement défini. À la suite des échanges avec la CNIL, le ministère de la Justice a limité expressément le périmètre aux personnes placées en détention provisoire et faisant l'objet d'un mandat de dépôt criminel. Comme la CNIL

CE QUI VA CHANGER AVEC LE RÈGLEMENT

Afin d'assurer une protection optimale et continue des données personnelles qu'ils traitent, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et être en mesure de démontrer cette conformité à tout moment (*accountability*).

La conséquence de cette responsabilisation des acteurs est la suppression de la plupart des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

La CNIL sera également amenée à rendre des avis comme elle le fait actuellement. En effet, le règlement prévoit que chaque autorité de contrôle dispose du pouvoir d'émettre, de sa propre initiative ou sur demande, des avis à l'attention du parlement national, du gouvernement, ou d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel.

De même, la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales prévoit également une obligation de consultation des autorités de contrôle sur les traitements relevant de son champ d'application.

l'avait demandé, l'arrêté publié a été modifié afin de préciser que seules les personnes faisant l'objet d'une mesure d'isolement pourraient être concernées par ces mesures de surveillance, sur décision du seul Garde des Sceaux. Enfin, l'arrêté prévoit désormais explicitement que ces dispositifs ne peuvent être mis en œuvre qu'à titre exceptionnel.

Si ces restrictions constituent une garantie importante, la CNIL a cependant rappelé au ministère de la Justice qu'il convenait de définir précisément les motifs qui pourraient fonder la décision du ministre de placer la cellule de ces personnes sous surveillance vidéo.

Une diminution significative des durées de conservation

Le projet d'arrêté initialement transmis prévoyait différentes durées de conservation des images : un délai de conservation d'un mois puis, à l'expiration de ce délai, une durée supplémentaire de six mois en base d'archive intermédiaire.

Si la durée maximale d'un mois ne posait pas de difficulté particulière au regard des durées traditionnellement appliquées aux dispositifs vidéo destinés à assurer la sécurité des biens et des personnes, la CNIL a estimé que les finalités poursuivies par les traitements ne justifiaient pas de conserver les données pendant six mois supplémentaires.

Le ministère a dès lors supprimé cette conservation d'une durée supplémentaire de six mois et la loi du 21 juillet 2016 retient également cette durée d'un mois.

Des précisions quant aux garanties entourant la mise en œuvre des dispositifs vidéo

L'instruction du dossier a été l'occasion de s'assurer que ces dispositifs ne permettraient pas la détection d'événements ou de mouvements anormaux, l'extraction de photographies ou encore l'enregistrement du son.

La CNIL a par ailleurs souhaité que des précautions soient prises quant au périmètre effectivement filmé, dans la mesure où les lieux d'intimité n'étaient pas exclus du champ de la caméra installée dans la cellule de détention. Le ministère s'est ainsi engagé à ce qu'un panneau d'occultation, placé devant les sanitaires, garantisse l'intimité corporelle de la personne prévenue. Par ailleurs, les caméras sont visibles et non dissimulées.

Les évolutions apportées au projet d'arrêté et l'adoption de la loi du 21 juillet 2016 témoignent d'une prise en compte des observations formulées par la Commission et de la mise en œuvre de garanties importantes. La Commission se montrera néanmoins attentive aux conditions effectives de mise en œuvre de ces traitements et fera, le cas échéant, usage de ses pouvoirs de contrôle.

3 078

décisions

DONT

1 976

autorisations de transfert de données hors UE

697

autorisations de recherche médicale ou évaluation des pratiques de soins

405

délibérations dont 145 avis sur des projets de texte et dont 190 autorisations (et 9 refus)

Les textes d'application de la loi de modernisation de notre système de santé du 26 janvier 2016, dite « LMSS »

Dans les mois qui ont suivi la promulgation de la loi, la CNIL a été saisie de 15 demandes d'avis sur des textes d'application.

Tout d'abord, la LMSS a redéfini les règles qui président au partage et à l'échange entre professionnels d'informations relatives aux patients. Désormais, le principe est celui d'une circulation de l'information au sein de « l'équipe de soins » sauf opposition de la part du patient. Les professionnels des champs social et médico-social, dans la limite de leurs missions et dans le seul intérêt du patient, peuvent aussi recevoir ces informations. Le principe du consentement exprès du patient a toutefois été maintenu dans le cas où l'information est amenée à être partagée en dehors d'une équipe de soins.

Ensuite, la LMSS a modifié le régime d'autorisation des recherches en santé en fusionnant les chapitres IX et X de la loi Informatique et Libertés. Le décret n° 2016-1872 du 26 décembre 2016, modifiant le décret d'application de la loi Informatique et Libertés, est venu préciser les contours de la nouvelle procédure et notamment les modalités d'information des personnes concernées ainsi que les rôles de deux nouveaux organismes : le comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, et l'Institut national des données de santé.

Dans une logique d'ouverture des accès aux données utiles pour les recherches d'intérêt public, la LMSS a également créé le Système national des données de santé (SNDS) dont les conditions d'accès ont été définies par le décret n° 2016-1871 du 26 décembre 2016. À cette occasion, la Commission a appelé l'attention du ministère de la santé sur l'importance des modalités d'exercice des droits des personnes et les mesures de sécurité à prévoir pour garantir la confidentialité des données.

Par ailleurs, la Commission a été amenée à se prononcer sur deux décrets encadrant les conditions de relance du dossier médical partagé ou « DMP »

(décrets n° 2016-914 du 4 juillet 2016 et n° 2016-1545 du 16 novembre 2016). L'objectif poursuivi par les pouvoirs publics est celui d'une large diffusion du DMP par des mesures techniques et organisationnelles facilitant son ouverture. La Commission a insisté sur la nécessité de mieux intégrer les usages possibles par le patient et le respect de ses droits.

Enfin, la Commission a aussi été saisie pour avis sur l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel qui remplace la procédure d'agrément des hébergeurs par une procédure de certification et crée une distinction entre les prestations d'hébergement des données de santé et d'archivage électronique des données de santé.

DERNIÈRE MINUTE

Le 19 janvier 2017, la Commission a rendu un avis sur le projet de décret en Conseil d'État qui précise les modalités d'utilisation du numéro de sécurité sociale (NIR) comme identifiant de santé, notamment les mesures destinées à empêcher son emploi à des fins autres que sanitaires et médico-sociales.

Le rappel des règles applicables à la communication politique

En novembre 2016, à la veille des différentes échéances électorales, la CNIL et le CSA ont publié un guide pratique élaboré conjointement, afin de rappeler les règles applicables à la communication politique. La CNIL a également précisé à quelles conditions les candidats et partis peuvent utiliser des données issues des réseaux sociaux.

Les opinions politiques, des données sensibles

La loi Informatique et Libertés définit les données personnelles relatives aux opinions politiques comme des données « sensibles ». À ce titre, leur enregistrement ou leur collecte doivent donc faire l'objet de précautions renforcées notamment en ce qui concerne l'information ou le consentement des personnes, la possibilité de s'opposer au traitement de leurs données mais aussi les mesures de sécurité. Les différentes campagnes électorales ont permis à la CNIL de constater que les citoyens ou électeurs étaient particulièrement soucieux de l'utilisation qui pouvait être faite de leurs données à des fins politiques.

L'accompagnement des professionnels

Dans la perspective des prochaines échéances électorales et des primaires lancées par les différentes tendances politiques, la CNIL a rappelé aux partis et candidats les recommandations relatives à la communication politique qu'elle avait publiées en 2012 et de nouveau reprises à l'occasion des élections départementales et régionales de 2014. De nombreuses fiches pratiques sont disponibles pour les candidats et partis sur le site de la CNIL, dans une page dédiée à la communication politique.

Le guide CSA/CNIL

Dans une démarche d'inter régulation, la CNIL et le CSA ont mis à disposition un outil unique et pédagogique qui contribue à l'accompagnement de la communication politique à l'ère numérique et à la construction collective d'un cadre de confiance.

L'objectif est de rappeler les principes élémentaires des lois relatives à la liberté de communication, applicable aux médias audiovisuels, et à la protection des données personnelles, pour les fichiers mis en œuvre par les candidats ou partis politiques. Le guide commun traite donc dans un même support des questions de pluralisme dans les médias audiovisuels et des règles Informatique et Libertés.

Les élections primaires de 2016/2017

Les élections primaires ont récemment fait leur apparition dans la vie politique française. Si ces consultations ont toutes pour but de désigner le candidat du parti en vue d'une élection à venir, elles ne concernent pas nécessairement le même corps électoral et peuvent ne pas faire appel aux mêmes modes de scrutin (vote papier ou électronique).

L'organisation, par un ou plusieurs partis politiques, d'une consultation ouverte à l'ensemble des électeurs (dite « primaire ouverte ») suscite des questions particulières en termes de protection des données. La CNIL s'est ainsi rapprochée des partis qui ont organisé des primaires afin de leur rappeler les règles à respecter, également disponibles sur son site. Elle a vérifié la destruction des fichiers mis en œuvre à cette fin, comme elle l'avait fait à l'occasion des primaires organisées par le PS en 2012.

L'utilisation des données issues des réseaux sociaux

En prévision des élections à venir, la CNIL a conduit, de mars à juin 2016, des auditions des principaux prestataires de logiciels de stratégie électorale auxquels les candidats et partis français ont recours de façon croissante.

Ces logiciels poursuivent en général deux objectifs :

- améliorer la communication politique en affinant les profils des contacts ou prospects par la collecte et le traitement de données plus nombreuses et plus précises et l'enrichissement de base de données ;
- passer d'une prospection ciblée en ligne à une prospection ciblée en face-à-face.

Dans les deux cas, les données disponibles sur les profils publics des réseaux sociaux peuvent être utilisées par ces prestataires.

La CNIL a donc souhaité approfondir l'analyse de ces nouveaux outils au regard de la loi Informatique et Libertés et préciser les conditions dans lesquelles ces données issues des réseaux sociaux peuvent être utilisées.

Le « *crawling* » des réseaux sociaux par les logiciels, aux fins de collecte et de traitement de données disponibles publiquement, n'est pas légal en l'absence d'information des personnes.

INFOSPLUS

Les missions de l'observatoire des élections

L'observatoire des élections est une structure de veille des pratiques de communication politique, de dialogue avec les partis et d'information régulière des électeurs.

Placé sous l'autorité d'un membre de la CNIL, l'observatoire des élections se compose d'une équipe pluridisciplinaire d'une dizaine d'agents.

L'Observatoire des élections a pour mission :

- d'informer les électeurs de leurs droits Informatique et Libertés ;
- de réagir rapidement aux pratiques qui pourraient révéler une méconnaissance de la loi Informatique et Libertés et, le cas échéant, de mener des contrôles ;
- d'accompagner les partis et les candidats dans la mise en place de leurs opérations de communication politique, en leur fournissant des outils et conseils pratiques pour se conformer à la loi Informatique et Libertés ;
- de proposer des pistes d'amélioration aux pouvoirs publics s'agissant du cadre juridique existant en matière de protection des données personnelles traitées à des fins de communication politique.

Pour remplir ces différentes missions, la CNIL met à la disposition des partis, candidats et électeurs différents outils juridiques et pratiques leur permettant de s'informer sur le cadre Informatique et Libertés applicables aux opérations de communication politique.

LES RELATIONS AVEC LE PARLEMENT

Au cours de l'année 2016, la CNIL a participé à une trentaine d'auditions parlementaires organisées par les commissions permanentes et organes de contrôle du Parlement.

S'agissant des projets de loi (PJL), l'examen du PJL pour une République numérique a permis à la CNIL, à la suite de l'avis rendu le 19 novembre 2015, d'être auditionnée par les rapporteurs des deux assemblées. La Commission a également été consultée par le Sénat sur le volet logement du PJL relatif à l'égalité et à la citoyenneté.

Les questions juridiques et techniques liées à l'application de la loi Informatique et Libertés qui surgissent de plus en plus fréquemment lors de l'examen de propositions de loi (PPL). Les auditions menées dans ce cadre d'examen ont concerné en 2016 des secteurs aussi divers que la sécurité (PPL renforçant le dialogue avec les supporters et la lutte contre le hooliganisme), le domaine social (PPL visant à améliorer l'accès au droit et à lutter contre la fraude sociale, PPL relative à l'exercice par la Croix-Rouge française de sa mission statutaire de rétablissement des liens familiaux), les élections (PPL ordinaire et organique rénovant les modalités d'inscription sur les listes électorales), la vidéo surveillance (PPL relative au respect de l'animal en abattoir). La CNIL a également répondu aux sollicitations des rapporteurs, dans les deux chambres, lors de l'examen des PPL ordinaire et organique portant statut général des autorités administratives indépendantes.

Après la publication du décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (fichier TES), la Commission des Lois du Sénat a souhaité auditionner la CNIL, lui donnant ainsi l'occasion de rappeler les notions essentielles pour bien comprendre le dispositif et le débat qui l'entoure et de présenter la teneur de l'avis rendu en formation plénière le 29 septembre 2016.

En-dehors de ces auditions techniques, la CNIL se félicite d'avoir pu, à la suite de l'envoi de son rapport annuel 2015 aux parlementaires, présenter ses activités et sujets d'actualité directement devant les députés et sénateurs, lors d'auditions organisées au dernier trimestre de l'année 2016 par les commissions permanentes concernées.

Dans le cadre des missions de réflexion, de prospective et de contrôle du Parlement, la CNIL a également participé aux travaux de plusieurs missions d'information et commissions d'enquêtes, telles que la mission d'information du Sénat sur l'organisation, la place et le financement de l'Islam en France et de ses lieux de culte ou encore la mission d'information sur l'offre automobile française de l'Assemblée nationale.

La CNIL est enfin régulièrement sollicitée par l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) et a ainsi été entendue au cours de l'année 2016 par ses membres sur le droit des objets connectés et le *Big data* dans l'agriculture.

ACCOMPAGNER
la conformité

La CNIL a fortement développé, ces dernières années, l'accompagnement de la mise en conformité des acteurs publics et privés qui traitent des données personnelles. Dans un univers numérique marqué par l'évolution permanente des technologies et des usages, les organismes qui traitent des données doivent assurer une protection optimale à chaque instant, et doivent pouvoir garantir cette protection aux personnes concernées. Il s'agit désormais d'un enjeu majeur de compétitivité : assurer une protection optimale des données dans l'univers numérique, c'est créer le cadre de confiance nécessaire au développement de l'activité et disposer d'un atout concurrentiel. La CNIL a donc développé son action d'accompagnement autour de trois axes : le déploiement des CIL, futurs délégués à la protection des données ; des outils visant à décliner les obligations applicables pour différents secteurs de l'économie (les « packs de conformité ») ; des outils de valorisation et de diffusion des bonnes pratiques (labels, BCR). La CNIL met ainsi à disposition des entreprises et administrations une gamme d'outils unique pour se préparer au règlement européen.

Ingrid
Juriste au service des CIL

Le service des CIL (SCIL) est composé de 7 personnes dont 6 juristes. Le rôle de notre service consiste à accompagner et à conseiller les Correspondants Informatique et Libertés (CIL) que ce soit en amont de leur désignation ou pendant l'exercice de leur mission. Notre activité est donc principalement tournée vers le conseil de ces professionnels. Nous conseillons ainsi les CIL et les futurs délégués à la protection des données principalement par écrit (adresse électronique dédiée) ainsi que par téléphone. Les sujets abordés sont très riches et vont de l'organisation de la conformité dans leur organisme à l'accompagnement pour la mise en place de projets innovants. Nous contribuons également aux travaux du G29 sur les lignes directrices relatives au délégué à la protection des données.

Il y a aussi une forte dimension pédagogique dans notre activité. En effet, chaque année nous sensibilisons plusieurs centaines de CIL à l'occasion de ces ateliers qui sont destinés à présenter soit le cadre général de la protection des données soit des thématiques plus ciblées. C'est un exercice passionnant qui implique de connaître aussi le terrain et de savoir répondre aux questions des CIL qui ont tous des profils différents.

Je considère que la curiosité intellectuelle et la communication sont des facettes importantes de mon activité car d'une part, nous sommes l'une des interfaces de la CNIL avec les professionnels et d'autre part nous échangeons au quotidien avec nos collègues des autres services.

« Désigner un CIL permet d'organiser sans attendre la conformité aux nouvelles règles de la protection des données personnelles. »

DU CIL AU FUTUR DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Alors que la désignation d'un(e) Correspondant(e) Informatique et Libertés (CIL) est actuellement optionnelle, ce sont 17 725 entreprises privées, collectivités territoriales ou associations qui se sont emparées de la fonction de CIL depuis sa création en 2005.

Le règlement général relatif à la protection des données (RGPD), qui s'appliquera en mai 2018, consacre cette bonne pratique de pilotage des opérations de conformité, en plaçant le futur « délégué à la protection des données » au cœur des nouvelles obligations des professionnels. Bientôt obligatoire pour certains organismes, le délégué bénéficie d'un renforcement de ses missions et moyens pour lui permettre d'agir de façon concrète et efficace.

Avec le règlement, le délégué à la protection des données sera principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

En tant que pilote de la conformité, le délégué à la protection des données s'assurera de la bonne tenue de la documentation relative aux traitements de données personnelles. À cet effet, le futur délégué devra être associé d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données, et détenir les ressources nécessaires à l'exécution de ses missions (notamment pour accéder aux données et aux traitements) ainsi qu'au maintien de ses connaissances.

C'est dans cette perspective qu'en 2016, la CNIL a renforcé l'information des professionnels concernant ce changement d'échelle, en enrichissant son site internet et les outils d'accompagnement dédiés aux CIL, tout en contribuant au niveau européen à l'élaboration de lignes directrices relatives au délégué.

« La mise en place de la fonction de délégué nécessite d'être anticipée et organisée dès aujourd'hui, afin d'être prêt en mai 2018. »

Élaboration de lignes directrices sur le « Délégué à la protection des données »

Dès février 2016, le G29 a identifié dans son plan d'actions annuel le besoin d'aider les professionnels (responsables de traitements et sous-traitants notamment) à mettre en œuvre le règlement de façon pragmatique. Pour ce faire, il a été décidé d'élaborer des lignes directrices relatives aux délégués à la protection des données.

Parallèlement, la CNIL a lancé une consultation en ligne en juin 2016 afin de recueillir auprès des professionnels les questions concrètes, les difficultés d'interprétation et des exemples de bonnes pratiques suscités par la mise en œuvre du règlement. Les nombreuses contributions reçues ont permis de répondre de manière pragmatique aux questions que se posaient les professionnels. La méthode de la consultation préalable aux travaux sur les lignes directrices a d'ailleurs été généralisée.

Publiées le 16 décembre 2016, les lignes directrices clarifient et détaillent les critères posés par le règlement sur le délégué à la protection des données, notamment en ce qui concerne :

- les notions d'autorité ou d'organisme public, d'activités de base, de grande échelle et de suivi régulier et systématique ;
- le rôle du délégué en matière de contrôle, d'analyse d'impact et de tenue du registre des activités de traitement ;
- la publication des coordonnées du délégué ;
- l'expertise et les compétences du délégué ;
- l'externalisation de la fonction ;
- la notion de conflit d'intérêts.

Se préparer : se former, recenser les actions et prioriser

La CNIL, qui a toujours manifesté son soutien aux CIL, a décidé de les accompagner plus spécifiquement en leur proposant des outils dédiés, eu égard à l'évolution de leur fonction. Elle a ainsi crée une nouvelle rubrique « Devenir délégué à la protection des données » sur son site internet, qui contient toutes les fiches pratiques et réponses aux questions fréquentes, permettant une juste compréhension du sujet et une bonne préparation de l'organisme à ses futures obligations.

En outre, deux outils sont mis à disposition pour aider les CIL à piloter leur activité et prioriser les actions à mener :

- Le référentiel du label « Gouvernance Informatique et Libertés » ;
- Le guide pratique de la prise de fonction.

En parallèle, les ateliers CIL se sont enrichis des nouvelles dispositions du règlement, des lignes directrices ainsi que des nouvelles dispositions issues de la Loi pour une République numérique. Forts de leur succès, les ateliers ont été suivis par plus de 1 200 personnes cette année et devraient être proposés pour certains d'entre eux, dans un format permettant un accès à distance à un plus grand nombre.

Plus largement, l'action de la CNIL à destination des CIL a été saluée par un taux de satisfaction de 94 %[1]. C'est pour cette raison que la CNIL poursuivra ses actions de préparation des CIL au règlement en travaillant notamment à l'évolution de leur extranet et aux modalités de désignation d'un délégué. Elle s'attachera enfin à sensibiliser les professionnels (responsables de traitement et sous-traitants) au règlement via des actions de communications à destination des réseaux organisés par secteur d'activités.

À RETENIR

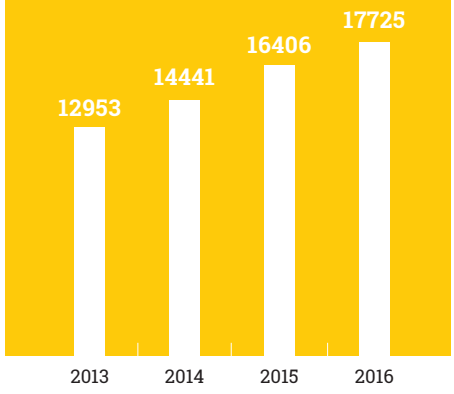
Les lignes directrices rappellent que le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement.

4 729
CIL ont été désignés dans 17725 organismes

1 230
personnes accueillies lors des 33 ateliers CIL

1 997
demandes de conseil traitées pour les CIL

Nombre d'organismes ayant désigné un CIL entre 2013 et 2016



1 Enquête téléphonique menée par IFOP du 28/11 au 2/12/2016 auprès de 1301 CIL ayant contacté la CNIL en 2016

LES PACKS DE CONFORMITÉ

Il s'agit d'un outil ancré dans la réalité des métiers et qui préfigure la conformité à l'heure du règlement.

Depuis 2014, la CNIL a lancé un nouvel outil : les « packs de conformité ». Ces packs, élaborés en concertation étroite avec les acteurs d'un secteur, permettent de promouvoir auprès de ceux-ci des bonnes pratiques, de décliner les obligations légales de manière opérationnelle et de simplifier les formalités administratives. Il s'agit d'un outil ancré dans la réalité des métiers et qui préfigure la conformité à l'heure du règlement, alliant responsabilisation et protection des données dès la conception et par défaut.

LES 6 PACKS DE CONFORMITÉ

Compteurs communicants : finalisé
Assurance : finalisé
Social : partiellement
Banque : partiellement
Véhicule connecté : en cours
***Open data* :** en cours

Les packs dans l'action sociale et médico-sociale

Après concertation avec un échantillon d'acteurs représentatifs du secteur, la CNIL a adopté trois autorisations uniques pour simplifier les formalités des organismes, œuvrant dans le champ de l'action sociale et médico-sociale.

Les trois autorisations uniques adoptées par la CNIL le 14 avril 2016 forment la première brique du pack de conformité « social ». Ces outils de simplification constituent un cadre de référence pour les acteurs de la sphère sociale et médico-sociale. Ils leur permettent de créer des traitements de données offrant suffisamment d'informations pour opérer un suivi personnalisé et efficace des personnes accompagnées, sans porter atteinte au respect de leur vie privée.

Les organismes, services et établissements peuvent procéder en ligne sur le site de la CNIL à un engagement de conformité à une ou plusieurs autorisations uniques correspondant au(x) traitement(s) dont ils ont besoin dans le cadre de leur activité.

Ces autorisations n'ont pas pour objet de permettre aux organismes de collecter, de manière systématique, l'ensemble des données qu'elles mentionnent : chaque organisme ne doit traiter que celles des données qui sont nécessaires à la finalité du traitement mis en place. Autrement dit, ce n'est pas parce qu'une autorisation unique prévoit la possibilité de collecter un type de donnée qu'il faut le faire systématiquement pour toutes les personnes concernées.

Sont également prévus de nouveaux outils de simplification, tels un guide sous forme de fiches pratiques pour expliquer de façon pédagogique les règles relatives à la protection des données personnelles et répondre à des questions concrètes des acteurs du secteur social et médico-social exprimées lors de la concertation.

À SUIVRE

Plus de 3 000 engagements de conformité aux 3 autorisations uniques déjà adoptées ont été réalisés. Le travail de simplification des formalités se poursuivra en 2017 avec l'adoption d'une norme simplifiée relative aux traitements mis en œuvre pour la gestion des services d'aide à domicile (soutien scolaire, aide-ménagère, etc.) et une autorisation unique relative aux traitements mis en œuvre pour la gestion des signalements de maltraitance des personnes vulnérables.

La poursuite des travaux du pack de conformité banque

Le second cycle de discussions, après l'adoption en 2015 d'une **première autorisation unique consacrée à la gestion des comptes bancaires et coffres forts inactifs** (autorisation unique n°45) a porté sur les projets de deux autorisations portant respectivement sur la **lutte contre la fraude externe et la lutte contre la fraude interne.**

Ces projets ont un large champ d'application puisqu'ils couvrent la lutte contre la fraude dans le cadre des activités relatives aux contrats portant sur les services et produits bancaires, financiers, de paiement et de monnaie électronique tels que définis aux livres II et III du code monétaire et financier (comptes, prêts et crédits, autres contrats et services bancaires et financiers) ainsi que les activités non bancaires et les produits et services dits « connexes », « annexes » ou encore associés délivrés par les organismes bancaires et financiers relevant du code monétaire et financier (exemples : opération de change, tenue de coffre-fort, etc.).

Pour cette raison, les deux autorisations se veulent plus précises sur la typologie des fraudes, l'échange d'informations intra-groupe, la mutualisation des données et la distinction entre les

problématiques propres à la fraude externe et interne.

Plusieurs points ont justifié un examen approfondi, notamment sur la définition de la fraude, le périmètre organique des autorisations uniques, le partage des données, etc.

Ces deux projets d'autorisation s'inscrivent dans le droit fil de l'autorisation accordée au secteur de l'assurance dans la mesure où ces deux secteurs sont étroitement liés et soumis au même régulateur sectoriel : l'autorité de contrôle prudentiel et de résolution, « ACPR ».

Il existe toutefois des différences inhérentes au secteur bancaire : tel est le cas pour les durées de conservation des alertes avant qualification (6 mois pour les assureurs) et 12 mois pour le secteur bancaire, ce délai étant justifié par les typologies de fraudes dont sont victimes les établissements du secteur bancaire.

Les travaux du 6ème pack de conformité « véhicule connecté »

La CNIL, soucieuse de favoriser les écosystèmes d'innovation et d'assurer la protection des données personnelles des usagers de l'automobile a lancé en mars 2016 ce pack en concertation avec les acteurs de la filière automobile, les entreprises innovantes du secteur des assurances et des télécoms, et les autorités publiques, afin de proposer des lignes directrices pour une utilisation responsable des données dans les prochaines générations de voitures.

L'enjeu est d'intégrer la dimension « protection des données personnelles » dès la phase de conception des produits et d'assurer la transparence et le contrôle par les personnes de leurs données.

Une telle démarche conditionne la confiance des utilisateurs, donc le développement pérenne de ces technologies. Elle permet en outre aux acteurs concernés d'être en conformité avec le règlement applicable le 25 mai 2018. Elle est enfin la traduction d'une régulation innovante, à la fois adaptative et concertée.

INFOSPLUS

La méthode de travail consiste à utiliser la même grille d'analyse que celle retenue pour le pack de conformité « compteurs communicants » :

1 Scénario « IN => IN » : les données collectées dans le véhicule restent dans le véhicule sans transmission au fournisseur de services

Exemple : *une solution d'éco-conduite qui traite les données directement dans le véhicule aux fins d'afficher des conseils d'éco-conduite en temps réel sur l'ordinateur de bord*

2 Scénario « IN => OUT » : les données collectées dans le véhicule sont transmises à l'extérieur pour fournir un service à la personne concernée

Exemple : *contrat de « Pay as you drive » souscrit auprès d'une société d'assurance*

3 Scénario « IN => OUT => IN » : les données collectées dans le véhicule sont transmises à l'extérieur pour déclencher une action automatique dans le véhicule

Exemple : *« Infotrafic » dynamique avec calcul d'un nouvel itinéraire suite à un incident sur la route*

Les travaux devraient être achevés au printemps 2017. La CNIL souhaite en effet favoriser l'élaboration rapide d'une « boîte à outils » de la conformité, qui fera l'objet de révisions périodiques afin d'assurer son effectivité.

À RETENIR

Toutes les données qui peuvent être rattachées à une personne physique identifiée ou identifiable, notamment via le numéro de la plaque d'immatriculation ou le numéro de série du véhicule sont des données à caractère personnel protégées par la loi Informatique et Libertés et le règlement général sur la protection des données.

Par exemple, les données relatives aux trajets effectués, à l'état d'usage des pièces, aux dates des contrôles techniques, au nombre de kilomètres ou au style de conduite constituent bien des données personnelles lorsqu'elles sont susceptibles d'être rattachées à une personne physique.

Le pack vise à sensibiliser les acteurs économiques du secteur automobile sur les principes de transparence et de loyauté de la collecte, qui impliquent a minima une information des personnes concernées, voire le recueil de leur consentement. Toutefois, la CNIL est consciente qu'un opt-in impliquant des paramétrages à chaque démarrage risque de dégrader l'expérience de conduite. Aussi, les règles applicables aux traitements seront fixées au cas par cas, notamment en fonction du scénario retenu, de la nature des données collectées et des attentes légitimes des usagers.

Une approche de protection des données dès la conception (« *privacy by design* ») doit être privilégiée. Elle peut se traduire par la mise en place de tableaux de bord facilement paramétrables, de façon à garantir à l'utilisateur la maîtrise de ses données.

LES LABELS : UN OUTIL DE CONFORMITÉ PLÉBISCITÉ

Poursuite des délivrances et renouvellements de labels

Preuve du succès et de la reconnaissance des labels, la Commission a été saisie, en 2016, de 42 demandes de labellisation, dont 8 en matière de gouvernance Informatique et Libertés.

À la fois gage de sécurité tant sur le plan juridique qu'informatique et instrument de valorisation des démarches entreprises, le label CNIL « gouvernance » est la démonstration de l'engagement de l'organisme demandeur. Il a séduit les organismes tant privés que publics, soucieux de mettre en avant leurs modalités de gestion des données personnelles, particulièrement respectueuses de la vie privée et des données personnelles, et de se préparer à l'entrée en application du règlement européen, avec notamment son principe de responsabilité (*accountability*).

Par ailleurs, délivrés depuis juin 2012, les labels CNIL « Formation » et « Audit de traitements » ont vu arriver dès 2015 les premières demandes de renouvellement. Ces procédures de reconduction se sont poursuivies en 2016, avec 12 labels sur 13 renouvelés cette année.

Attribution du premier label « coffre-fort numérique »

Un coffre-fort numérique est un espace de stockage numérique sécurisé, dont l'accès est limité à son seul utilisateur et aux personnes physiques qu'il a spécialement habilitées à cet effet. Il peut permettre de stocker par exemple des factures, des photos, des documents administratifs personnels.

Le label coffre-fort numérique atteste d'un service de qualité, respectueux de l'intégrité, de la disponibilité et de la confidentialité des données qui y sont stockées par les particuliers ou les professionnels.

« Dans les appels d'offre que je suis chargé de préparer, je veille désormais à la présence du label délivré par la CNIL. »

- Les données sont chiffrées à toutes les étapes du processus (transfert vers et depuis un coffre d'une part, stockage d'autre part).
- Le dispositif de chiffrement, notamment la taille de la clé utilisée, doit répondre aux exigences de l'ANSSI (Agence nationale de sécurité des systèmes d'information).
- Les mécanismes d'authentification des utilisateurs et des tiers mandatés doivent garantir une authentification forte (mots de passe à usage unique, envoi de codes par SMS, etc.).

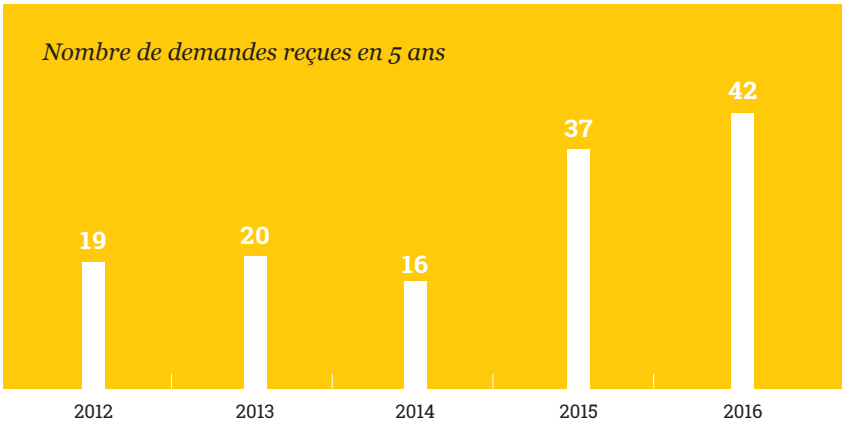
Ce premier label a été délivré le 21 juillet 2016 à une société, en sa double qualité d'opérateur et de fournisseur de service de coffre-fort numérique : en effet, cette société assure à la fois le fonctionnement opérationnel du système et sa vente directement auprès des utilisateurs, particuliers et professionnels.

« Depuis que j'ai le label formation octroyé par la CNIL, j'ai plus de clients qui ont sélectionné le cursus que je propose. »

4
référentiels

97
labels délivrés

136
demandes de labels reçues



100%
des labellisés arrivés à l'échéance des 3 ans ont renouvelé leur label

3,5
mois de délai moyen de délivrance

CE QUI VA CHANGER AVEC LE RÈGLEMENT

Le règlement encourage, en particulier au niveau européen, la mise en place de mécanismes de certification en matière de protection des données. La CNIL étudie la faisabilité des différentes pistes permettant de recourir à un (des) tiers certificateur(s), qui délivrerai(en)t les futures certifications : agrément par la CNIL elle-même d'organismes certificateurs qui certifieraient au niveau national voire européen, ou accréditation de tiers certificateurs par l'organisme national dédié (COFRAC) sur la base d'un référentiel d'accréditation défini en collaboration avec la CNIL, et en fonction du champ de la certification visée.

Outre une nouvelle procédure, il s'agit également pour la Commission de définir, avec ses homologues européens, le référentiel de certification. Là encore, plusieurs sujets sont à l'étude.

La CNIL est co-rapporteur des travaux menés au plan européen et selon le calendrier de travail élaboré par le G 29, des lignes directrices seront produites sur ces deux aspects courant 2017.

LES BCR

Simplification des transferts encadrés par des BCR

Les BCR sont des codes de conduite définissant la politique d'un groupe d'entreprises en matière de transferts de données personnelles effectués en dehors de l'Espace économique européen. Grâce à la mise en œuvre de mesures proactives – dites d'*accountability* (responsabilisation) – en sus des principes de la directive 95/46/CE, 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.).

Reconnaissant ainsi que la mise en oeuvre de BCR témoigne de l'engagement d'un groupe multinational à protéger les données personnelles lorsqu'elles sont transférées entre ses entités, la CNIL délivre depuis 2015 une autorisation unique par groupe ayant adopté des BCR.

Cela permet aux responsables de traitement soumis au respect des obligations de la loi Informatique et Libertés d'effectuer un engagement de conformité à l'autorisation unique BCR de son groupe (ou du groupe de son sous-traitant en présence de BCR « sous-traitant ») via le formulaire de déclaration simplifiée. Une fois cet engagement effectué, les responsables de traitement doivent tenir à la disposition des services de la CNIL une liste détaillée et à jour de chaque transfert. Ainsi, il n'est plus nécessaire de demander à la CNIL une autorisation par finalité de transfert.

En 2016, la CNIL a délivré

25 **autorisations uniques BCR contre 17 en 2015**

92 **groupes ont adopté des BCR**

29 **ont désigné la CNIL comme autorité chef de file**

CE QUI VA CHANGER AVEC LE RÈGLEMENT

Le Règlement consacre l'outil de conformité que sont les BCR initialement développées sous l'impulsion du G29 dans une optique de responsabilisation (*accountability*).

Outre les transferts fondés sur une décision d'adéquation, le règlement promeut une gamme d'outils pouvant être qualifiés de « garanties appropriées » : instruments juridiques contraignants entre autorités publiques, BCR, clauses contractuelles types de protection des données adoptées par la Commission ou par une autorité de contrôle, code de conduite, mécanisme de certification, clauses contractuelles ad hoc et enfin dispositions particulières insérées dans des arrangements administratifs entre autorités et organismes publics.

En fonction du mécanisme choisi le responsable de traitement peut être exonéré de toute demande d'autorisation pour ses transferts hors de l'UE.

Répartition par secteur d'activité des 92 groupes ayant officiellement adopté des BCR au 31 décembre 2016

BANQUE-ASSURANCE	
BCR « responsable de traitement »	ABN AMRO, AXA*, Citigroup, ING Bank, JP Morgan Chase & Co., Rabobank, Société Générale*,
BCR « responsable de traitement » et « sous-traitant »	Mastercard
INDUSTRIE	
BCR « responsable de traitement »	Aker Solutions, Airbus Group*, AkzoNobel, ArcelorMittal, BakerCorp, BMW, BP, Cargill, Continental, Corning*, D.E. Master Blenders 1753 (ex Sara Lee), DSM, Engie* (ex GDF SUEZ), Fluor, General Electric*, Johnson Controls, Michelin*, Osram, Safran*, Schlumberger, Schneider Electric*, Shell, Siemens, Total*, Maersk Group, Nutreco, Rockwool, Lego,
LUXE	
BCR « responsable de traitement »	Hermès*, LVMH*
NOUVELLES TECHNOLOGIES	
BCR « responsable de traitement »	Atmel, CA Plc, Flextronics, HP Enterprise*, HP Inc.*, Intel, Motorola Mobility, Motorola Solutions, NetApp, OVH*, Giese- cke & Devrient, IBM, Kværner ASA;
BCR « sous-traitant »	Salesforce*
BCR « responsable de traitement » et « sous-traitant »	Atos*, BMC Software*, Linkbynet*, Philips Electronics
SANTÉ	
BCR « responsable de traitement »	AstraZeneca, Bristol Myers Squibb*, Cardinal Health, CareFusion, GlaxoSmithKline, IMS Health, Novartis*, Novo Nordisk, Sanofi*, UCB, MSD, Amgen*
BCR « responsable de traitement » et « sous-traitant »	Align Technology
SERVICES	
BCR « responsable de traitement »	Accenture, Akastor, American Express, Ardian* (ex AXA Private Equity), CMA-CGM*, Deutsche Post DHL, Deutsche Telekom, eBay, EY (ex Ernst & Young), Hyatt, International SOS*, LeasePlan, Legrand*, Linklaters, Simon-Kucher & Partners, Spencer Stuart, Starwood Hotels and Resorts, Latham & Watkins, BT
BCR « responsable de traitement » et « sous-traitant »	First Data, Sopra HR Software* (ex HR Access), TMF Group, Capgemini*, BOX

** groupes ayant désigné la CNIL comme autorité chef de file*

PARTICIPER
à la régulation internationale

Outre la préparation du passage au règlement européen, qui a été au cœur de l'activité du G29, l'année 2016 a été fortement marquée par les travaux sur le nouvel accord *Privacy Shield* portant sur les transferts internationaux de données de l'Europe vers les États-Unis, qui s'est conclu fin juillet entre la Commission européenne et les autorités américaines. La CNIL, qui préside le G29 depuis 2014, a été particulièrement active, en étroite collaboration avec ses homologues européens.

Ismini
Juriste au service des affaires européennes et internationales

De manière générale, le service des affaires européennes et internationales conseille, développe, communique, promeut les positions de la CNIL sur les sujets présentant une dimension européenne et internationale.

Depuis 2014, Isabelle Falque-Pierrotin assure la Présidence du G29 (ensemble des «CNIL» européennes). De ce fait, le service coordonne l'activité du G29. Concrètement, cela comprend l'organisation des séances plénières réunissant les 29 membres du G29 tous les deux mois à Bruxelles, le suivi des 9 sous-groupes de travail, la participation à la définition de la feuille de route stratégique et la représentation extérieure du G29. Le service est aussi amené à travailler sur le fond des dossiers. Ainsi, le service est actuellement très impliqué sur l'élaboration de tous les outils permettant la mise en œuvre effective à l'échelle européenne du Règlement européen et du Privacy Shield. Pour ma part, je travaille en ce moment sur la mise à jour des référentiels transferts de données à la lumière du Règlement. Je m'occupe aussi de la préparation des communiqués de presse du G29. Je participe également à l'organisation du fablab, une journée de co-construction avec les représentants européens des fédérations et de la société civile à Bruxelles sur des sujets clés du Règlement Européen.

L'ADOPTION DU BOUCLIER VIE PRIVÉE « EU-US PRIVACY SHIELD »

« Le juge européen n'a pas uniquement rendu une décision sur les transferts entre l'Union et les États-Unis, c'est en réalité un nouveau standard mondial qui est en train de se dessiner. »

« Le G29 a exprimé avec force sa position sur la surveillance de masse et indiscriminée la considérant comme incompatible avec nos principes européens. »

Le G29 a fourni un travail considérable en 2016 afin de tirer toutes les conséquences de l'arrêt C-362/14 du 6 octobre 2015 de la Cour de Justice de l'Union Européenne (« arrêt Schrems ») et ainsi participer à la définition d'une solution pour les transferts de données personnelles vers les États Unis et au-delà.

À cet effet, le G29 a publié en février un document majeur identifiant les garanties européennes essentielles à respecter en matière de surveillance (« European Essential Garantees ») sur le territoire européen et sur tout autre territoire hors Union européenne suite à un transfert de données personnelles protégées par le droit de l'Union.

Il a mené cette évaluation à la lumière des textes et de la jurisprudence européens sur la surveillance et le respect des droits fondamentaux. **Ainsi, se dégagent quatre garanties essentielles à respecter :**

1. Les traitements doivent reposer sur des règles claires, précises et compréhensibles ;
2. La proportionnalité au regard de la finalité poursuivie doit être démontrée ;
3. Un mécanisme de contrôle indépendant doit exister ;
4. Une possibilité de recours effectif doit être offerte aux citoyens.

Le G29 s'est ensuite attelé à évaluer le projet de décision d'adéquation du 29 février 2016 sur le bouclier vie privée de la Commission Européenne avec ses annexes, à la lumière de ces 4 garanties essentielles.

Dans son avis du 13 avril, il a exprimé un grand nombre de préoccupations, dont certaines ont été prises en compte dans la décision finale adoptée par la Commission européenne le 12 juillet 2016.

Le 26 juillet 2016, le G29 s'est prononcé sur le texte définitif de la Commission soulevant un certain nombre de réserves concernant à la fois le volet commercial et l'accès par les autorités publiques et de renseignement américaines aux données transférées de l'Union européenne.

En ce qui concerne le volet commercial, le G29 a regretté le manque de règles spécifiques pour les décisions automatisées et l'absence d'un droit d'opposition. La manière dont les principes du Bouclier Vie Privée vont être appliqués aux sous-traitants aurait mérité également d'être davantage explicitée.

En ce qui concerne l'accès par les autorités publiques et de renseignement aux données transférées aux États-Unis dans le cadre du Bouclier Vie Privée, le G29 aurait souhaité des garanties plus strictes concernant l'indépendance du médiateur (Ombudsperson) et les pouvoirs qui lui sont accordés. Le G29 a noté l'engagement du Bureau du directeur des services de renseignement américains (Office of the Director of National Intelligence – ODNI) à ne pas effectuer de collecte massive et indiscriminée de données personnelles. Néanmoins, les autorités européennes ont regretté le manque de garanties concrètes permettant d'éviter que de telles pratiques aient lieu.

Depuis 1er août 2016, le Bouclier Vie Privée est entré en vigueur. Il est désormais possible de s'y référer pour transférer des données personnelles vers les États Unis, à condition que les entreprises destinataires des données se soient préalablement inscrites sur le registre tenu par l'administration américaine. Au-delà de cette obligation formelle, les entreprises américaines devront respecter les obligations et les garanties de fond prévues par le Bouclier Vie Privée.

Le G29 travaille actuellement à la mise en place concrète du Bouclier Vie Privée, notamment en préparant la première revue conjointe annuelle, laquelle sera un évènement important organisé par la Commission européenne. À cette occasion, les autorités de protection des données seront particulièrement vigilantes sur la prise en compte de leurs préoccupations. Cette revue sera donc un moment clé permettant d'évaluer la robustesse et l'effectivité des garanties prévues par le Bouclier Vie Privée.

Dans le cadre de la mise en place du Bouclier Vie privée, les autorités du G29 ont :

- adopté des supports d'information spécifiques à destination des individus et des entreprises. Ces outils peuvent être utilisés par chaque autorité nationale de protection des données personnelles pour sa propre démarche d'information ;
- auditionné une délégation américaine composée de représentants du ministère du commerce des États-Unis et de la FTC (Commission Fédérale du Commerce), des services de renseignement ainsi que du médiateur (*ombudsperson*) ;
- confirmé que le G29 serait l'organe européen de centralisation des plaintes (*EU centralized body*) compétent pour communiquer les plaintes à l'ombusdperson ;

DERNIÈRE MINUTE

Lors de la plénière des 7 et 8 février 2017, le G29 a adopté :

- des règles de procédures pour la composition et le fonctionnement de l'organe européen de centralisation des plaintes (*EU centralized body*) et du panel informel des autorités de protection des données en charge des plaintes commerciales (*EU informal panel of DPAs*) ;
- des formulaires de plaintes de nature commerciales et pour celles adressées à l'ombudsperson.

« Cette première revue sera l'occasion d'évaluer concrètement la robustesse et l'effectivité des garanties prévues par l'accord. »

De l'invalidation Safe Harbor à l'adoption du Privacy shield : dates clés

6 octobre 2015 — **Invalidation du *Safe Harbor***

31 janvier 2016 — **Date butoir fixée par le G29 pour la négociation d'un nouvel accord**

29 février 2016 — **Publication du projet de décision d'adéquation *Privacy Shield* par la Commission Européenne**

13 avril 2016 — **Publication de l'avis du G29 sur la décision d'adéquation de la Commission**

Publication du document « *European Essential Guarantees* » par le G29

12 juillet 2016 — **Adoption de la décision d'adéquation *Privacy Shield* par la Commission Européenne**

LA COOPÉRATION INTERNATIONALE

« Il s'agit ainsi de former de vrais citoyens numériques, responsables de leurs données et respectueux de celles des autres. »

Adoption du premier référentiel international de formation des élèves a la protection des données personnelles

Avec l'adoption d'un premier référentiel international lors de la 38ème Conférence mondiale des autorités de protection des données, les CNIL du monde entier ont rappelé que l'éducation des jeunes à la protection des données personnelles est un enjeu majeur.
Ce socle commun de compétences constitue un outil de formation pratique pour promouvoir l'éducation à la protection des données dans les programmes scolaires. Il développe en neuf domaines structurants, les composantes clé de la protection des données dont la connaissance et la compréhension sont considérées comme prioritaires.

Les objectifs de formation à atteindre sont clairs :

1 Acquérir une connaissance et une compréhension critiques des droits et des responsabilités dans notre univers numérique,

2 Développer une démarche réflexive sur les usages qui sont faits des données personnelles,

3 Appréhender les risques et maîtriser les pratiques permettant de se mouvoir dans l'environnement numérique avec confiance, lucidité et dans le respect des droits de chacun.

La CNIL qui est à l'origine de cette initiative s'est appuyée sur l'expertise des autorités de protection des données membres du groupe de travail international en Éducation au numérique, et de spécialistes de l'éducation. Il s'agit d'une première étape qui devra s'accompagner de la diffusion auprès des enseignants de ressources pédagogiques adaptées à la compétence abordée ainsi qu'à la tranche d'âge concernée. Pour réussir dans cette démarche, un travail en commun doit être mené, dans chaque pays, entre les autorités de protection des données, les autorités scolaires et les personnels enseignants. C'est la raison pour laquelle, la Présidente de la CNIL a saisi de cette question la ministre de l'éducation nationale afin d'obtenir son soutien.

POUR EN SAVOIR PLUS > www.cnil.fr/referentiel-formation
www.cnil.fr/resolution-education

La francophonie et l'AFAPDP

En 2016, 59 des 84 États et Gouvernements membres de la Francophonie disposent d'une loi et 51 d'entre eux d'une autorité de protection des données personnelles. L'AFAPDP s'est quant à elle enrichie de deux nouveaux membres : l'Autorité de régulation des télécommunications/tic de Côte d'Ivoire (ARTCI), compétente en matière de protection des données personnelles depuis 2013 et l'Autorité de protection des données personnelles (APDP) du Mali, installée en 2015. Ces adhésions s'inscrivent dans la continuité d'une coopération mise en place depuis 2015 et ont été votés à l'occasion de la 9ème Assemblée générale de l'AFAPDP, qui s'est tenue à Ouagadougou en septembre 2016. Les membres ont également adopté à cette occasion une résolution appelant à « la reconnaissance d'un droit à l'effacement et au déréférencement de portée universelle ». Celle-ci vient s'ajouter aux 15 résolutions et déclarations adoptées depuis 2009.

L'association a également permis à plusieurs de ses membres de prendre part à la Conférence internationale des commissaires à la protection des données et contribué à la traduction vers le français des débats. Elle a également organisé un évènement ouvert intitulé « La protection des données personnelles : un atout pour la Francophonie », afin de promouvoir ses activités auprès des participants à cette conférence annuelle. Au-delà de l'animation du réseau, l'AFAPDP est membre observateur du Comité consultatif de la Convention 108, encourageant l'adhésion des pays tiers membres de l'OIF et elle prend part aux activités du groupe de travail international sur la protection des données et l'action humanitaire.

26 juillet 2016
Publication de l'avis du G29 sur la décision de la Commission Européenne

27 septembre 2016
Confirmation que le G29 sera l'organe européen de centralisation des plaintes (*EU centralized body*) compétent pour communiquer les plaintes à l'ombusdperson

12 décembre 2016
Adoption des supports d'information spécifiques à destination des individus et des entreprises et audition d'une délégation américaine composée de représentants du ministère du commerce des États-Unis et de la FTC (Commission Fédérale du Commerce), des services de renseignement ainsi que du médiateur (*ombudsperson*).

CONTRÔLER
et sanctionner

Le contrôle sur place, sur pièces, sur audition ou en ligne permet à la CNIL de vérifier la mise en œuvre concrète de la loi. Un programme des contrôles est élaboré en fonction des thèmes d'actualité, des grandes problématiques identifiées et des plaintes dont la CNIL est saisie.
À l'issue des contrôles, la Présidente de la CNIL peut décider des mises en demeure. La formation restreinte de la CNIL, composée de 5 membres et d'un Président distinct du Président de la CNIL, peut prononcer diverses sanctions dont des sanctions pécuniaires d'un montant maximal de 3 millions d'euros. Ces sanctions peuvent être rendues publiques.

Leslie
Juriste
et Julien
Auditeur des systèmes d'information au service des contrôles

Notre mission consiste à vérifier la conformité des traitements de données, sur place (entreprises, collectivités locales, administrations) ou à distance (contrôles en ligne de sites internet). Nous menons un travail d'enquête en interrogeant les organismes concernés et en investiguant sur les postes informatiques et les dossiers papier. Nous travaillons toujours en binôme composé d'un juriste et d'un informaticien car le métier de contrôleur nécessite une bonne synergie entre les compétences juridiques et les compétences techniques.

Nous recueillons les éléments de preuve au format papier ou numérique (extractions de base de données, captures d'écran), qui le cas échéant matérialisent des manquements en vue d'une demande de mise en conformité ou d'une procédure répressive.

Le juriste veille notamment à la présence de mentions d'information prévues par la loi et analyse les contrats. Quant à l'auditeur, il se charge des requêtes informatiques et de l'évaluation des mesures de sécurité (accès aux fichiers, etc.).
À l'issue du contrôle, il exploite les extractions et les éléments techniques recueillis.
Nous menons des contrôles principalement sur les traitements de données de ressources humaines, sociales ou de santé. En 2016, nous avons contrôlé une cinquantaine d'organismes tels que des établissements de l'enseignement supérieur, des structures d'aide à la personne ou encore des entités du réseau de l'assurance maladie. Les dispositifs de vidéosurveillance et les violations de données personnelles représentent aussi une part importante de nos contrôles.

Nous participons aussi aux sessions d'information à destination des Correspondants Informatique et Libertés (CIL) et aux missions de coopération avec d'autres autorités de protection (Sénégal).

CONTRÔLER

La CNIL a réalisé 430 contrôles en 2016, conformément à ce qui était annoncé aux termes de son programme annuel (entre 400 et 450).

A l'aune des modifications introduites par la loi pour une République numérique et par le règlement européen sur la protection des données, les missions effectuées traduisent d'ores et déjà la volonté de la Commission de s'orienter vers de nouvelles stratégies de contrôle, plus complexes, conjuguant l'ensemble des pouvoirs à sa disposition pour constater d'éventuels manquements.
La Commission a ainsi procédé à plus de 100 contrôles en ligne, dont un nombre important a porté sur des failles de sécurité. Cet instrument de contrôle qui permet de recueillir des pièces et informations à distance, en se comportant comme tout utilisateur d'un service en ligne, a plus généralement prouvé son efficacité en complément de vérifications sur place.

94 contrôles ont permis à la CNIL de s'assurer de la conformité de dispositifs de vidéoprotection et de vidéosurveillance, qu'il s'agisse de vérifications diligentées à la suite de plaintes ou encore à l'initiative de la CNIL. Ces contrôles ont conduit à la mise en conformité, lorsque cela s'avérait nécessaire, des organismes concernés, par un rappel du régime juridique applicable, qui ressort tant du code de la sécurité intérieure que de la loi Informatique et Libertés, et des recommandations pratiques.

La Commission a par ailleurs effectué une trentaine de contrôles sur pièces et a effectué 5 auditions de contrôle dans ses locaux. Elle a également réalisé une dizaine d'audits à l'occasion du Sweep Day (action d'audit coordonnée au niveau européen).

En 2016, tout comme l'année précédente, 70 % des missions de contrôle réalisées ont concerné le secteur privé, 30 % le secteur public. S'agissant plus spécifiquement des contrôles en ligne, ce sont 90 % des vérifications qui ont été menées dans le secteur privé.

Bilans du programme annuel 2015

Ces bilans font suite aux premiers éléments présentés dans le rapport d'activité 2015.

Le paiement sans contact

La CNIL a adressé en 2015 des questionnaires de contrôle sur pièces à neuf banques françaises proposant des cartes de paiement sans contact. Les vérifications ont porté sur la nature des données accessibles par ce biais, les mesures de sécurité mises en œuvre, l'information du porteur de la carte et la désactivation de la fonction sans contact.

- Il a été constaté que les données lisibles sans contact à partir des cartes en circulation se limitent au numéro de la carte, à sa date d'expiration et aux données techniques nécessaires à son fonctionnement. Elles n'incluent pas l'historique des transactions. Outre le respect des mesures de sécurité définies par la norme ISO/IEC 14443, la plupart des banques mettent à disposition des clients en faisant la demande des étuis de protection. Enfin, sept des neuf banques contrôlées permettent de désactiver la fonction de paiement sans contact, et la CNIL s'est assurée que cette possibilité est portée à la connaissance de leurs clients. Les deux autres banques proposent de substituer à la carte de paiement sans contact une carte de paiement donnant accès aux mêmes services, sans surcoût.

430
CONTRÔLES

DONT

101
CONTRÔLES EN LIGNE

94
CONTRÔLES VIDÉO

INFOSPLUS

L'origine des contrôles

60%
sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;

20%
résultent du programme annuel décidé par les membres de la Commission ;

15%
s'inscrivent dans le cadre de l'instruction de plaintes ;

5%
sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction.

Les risques psychosociaux (RPS) en entreprise

Les enquêtes menées par les entreprises auprès de leurs salariés afin de mieux évaluer et lutter contre le stress au travail se sont multipliées ces dernières années et ont conduit nombre de salariés à saisir la CNIL de plaintes. Une série de contrôles a été menée en 2015, auprès d'organismes privés et publics, commanditaires ou prestataires d'enquêtes sur la prévention des risques psychosociaux.

- Ces contrôles révèlent, d'une manière générale, l'anonymisation des données des enquêtes dès la collecte des réponses apportées aux questionnaires, la mise en œuvre de procédés pour recueillir les données présentant des mesures de sécurité robustes et la suppression des données individuelles une fois l'enquête terminée.

Toutefois, il apparaît que les personnes interrogées ne sont pas suffisamment alertées sur le caractère facultatif des enquêtes, ni systématiquement destinataires de l'ensemble des informations prévues par la loi. Les enquêtes peuvent conduire à la collecte de données de santé en l'absence du consentement exprès des personnes. Enfin, nombre d'enquêtes ne donnent pas lieu aux formalités préalables adéquates auprès de la CNIL.

Le Système national des permis de conduire (SNPC)

Le Système national des permis de conduire (SNPC) contient des informations relatives aux titulaires de permis de conduire, aux personnes ayant fait une demande de permis ou ayant fait l'objet d'une décision d'annulation ou d'interdiction du permis, ainsi que des informations détaillées sur ces permis (catégorie, conditions restrictives, état de validité, déclaration de perte ou vol, décision de retrait, restrictions médicales, infractions au code de la route, suspension, annulation et interdiction de délivrance de permis, nombre de points, etc.).

Le SNPC a fait l'objet d'une série de contrôles sur place en 2015-2016, visant les acteurs institutionnels chargés d'en assurer le fonctionnement et de l'exploiter. Dans la continuité de ces investigations, le dispositif a fait l'objet de contrôles sur pièces portant plus particulièrement sur la gestion des cas d'homonymies, le retrait et la réattribution de points, et l'ensemble du parcours des données enregistrées dans le fichier, de la création du permis au décès du titulaire.

- La CNIL poursuit ainsi ses vérifications, axées sur le respect des exigences d'exactitude et de conservation limitée des données, et de l'effectivité des droits des personnes concernées.

Premiers éléments sur le programme annuel 2016

Ces premiers éléments portent sur les contrôles réalisés dans le cadre du programme annuel de 2016, actuellement en cours d'instruction et qui feront l'objet d'un bilan définitif dans le rapport d'activité 2017.

Le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM)

La CNIL a souhaité inscrire à son programme annuel de contrôles le dispositif « SNIIRAM » (Système national d'information inter-régimes de l'assurance maladie), qui constitue l'une des plus grandes bases de données de santé au monde. Créé en 1999 et mis en œuvre par la CNAMTS (Caisse nationale de l'assurance maladie des travailleurs salariés), le SNIIRAM contient en effet plusieurs dizaines de millions de données de santé issues des demandes de remboursements de frais de santé (feuilles de soins, factures de cliniques, etc.). Les données sont « pseudonymisées », de manière à empêcher l'identification des patients concernés.

Le SNIIRAM vise notamment à contribuer à une meilleure gestion des politiques de santé, en permettant à des autorités de santé publique de conduire des études portant, par exemple, sur le taux de couverture vaccinale des enfants ou encore de déceler des cas d'épidémies.

Des missions d'investigation ont ainsi été conduites auprès de la CNAMTS et de ses prestataires, ainsi que d'organismes utilisateurs des données du SNIIRAM.

- Il ressort des premiers éléments constatés que la gestion du système semble globalement satisfaisante au regard de la loi Informatique et Libertés. Toutefois, la CNIL poursuit son analyse sur la sécurité et la confidentialité des données, au regard de la sensibilité de ces dernières et du nombre de personnes concernées.

Le traitement API-PNR

Le système API-PNR (Advance Passenger Information - Passenger Name Record) est un fichier de contrôle des déplacements aériens, autorisé par la loi à titre expérimental en 2013 et mis en œuvre par les ministres de l'intérieur, de la défense, chargé des transports et chargé des douanes. Notamment destiné à contribuer à la lutte contre le terrorisme et le trafic de drogue, il enregistre les données de passagers transmises par les transporteurs aériens et concerne les vols à destination et en provenance de pays étrangers.
Les investigations prévues ont pour objet d'analyser le fonctionnement technique du dispositif et des raccordements aux systèmes d'information des entités prévues (autorités et transporteurs aériens notamment), de vérifier

le respect des finalités du traitement et de contrôler les modalités d'accès aux données.

Inscrit au programme annuel des contrôles par la CNIL en 2016, le système a fait l'objet de premières vérifications auprès des services ministériels concernés. Toutefois, compte tenu du report du déploiement définitif du dispositif, les contrôles menés actuellement par la CNIL portent sur l'expérimentation opérationnelle. Ils ont vocation à se poursuivre une fois le dispositif déployé, courant 2017.

Les courtiers en données (Data brokers)

La CNIL a inclus au programme annuel des contrôles de l'année 2016 les traitements mis en œuvre par les courtiers en données, communément appelés « *data brokers* ». En pleine expansion, l'activité de courtage de données fait intervenir un nombre croissant d'intermédiaires qui agrègent, enrichissent, transforment et commercialisent les données. Elle conduit à commercialiser des millions de données à caractère personnel et soulève des problématiques Informatique et Libertés majeures, nécessitant d'identifier précisément les obligations de chaque type d'acteur impliqué.

La CNIL a ainsi effectué 53 contrôles en 2016 auprès des différents types d'acteurs liés à l'activité de courtage de données.

Ces contrôles ont eu principalement pour objectif d'identifier les acteurs concernés et leur rôle dans le traitement de données collectées par certains et réutilisées par d'autres. En particulier, les vérifications ont porté sur le fondement légal des traitements, les conditions de collecte des données, leurs durées de conservation, l'information des personnes et la faculté pour elles d'exercer leurs droits, et sur les mesures de sécurité mises en œuvre. Au vu des constats effectués, la Commission adoptera les mesures qui s'imposent en 2017.

GROS PLAN

Failles de sécurité en ligne 24 h chrono à la CNIL

Il est 17h20, mercredi après-midi.

La CNIL reçoit un courriel signalant une faille de sécurité, qui rendrait librement accessibles sur internet les données personnelles de dizaines de milliers d'utilisateurs (nom, prénom, date de naissance, adresse, photographie, etc.). Les agents du service des contrôles vérifient immédiatement le signalement, évaluent la gravité des faits et envisagent la réalisation d'une mission de contrôle. Compte tenu des circonstances, une proposition de contrôle est transmise dans l'heure qui suit à la Présidente de la CNIL. Cette dernière décide alors de diligenter une mission de vérification en ligne.

Dès le lendemain matin, sur le fondement de la décision de la Présidente et de leur ordre de mission, deux auditeurs des systèmes d'information et un juriste procèdent aux constatations, depuis les locaux de la CNIL dédiés exclusivement aux contrôles en ligne. En parcourant le site concerné, ils décèlent rapidement la présence des données personnelles signalées, accessibles à tout internaute. Ils prennent alors copie d'un échantillon représentatif de données. Une fois le téléchargement terminé, les agents finalisent le procès-verbal, qui indique l'ensemble des vérifications effectuées.

Ils contactent alors par téléphone l'organisme éditeur du site contrôlé et demandent à être mis en relation avec son responsable des systèmes d'information. Ils font part à ce dernier des faits constatés et l'invitent à prendre toute mesure permettant de supprimer l'accès aux données par des personnes non autorisées.

Le responsable s'engage à mettre le site hors ligne, à identifier l'origine de la faille, à appliquer des mesures correctrices et à en rendre compte dès que possible. Vingt minutes plus tard, il confirme par courriel adressé à la CNIL la mise hors ligne du site, à titre préventif.

Il est 16h10, jeudi après-midi.

Et après ?

Le procès-verbal de contrôle en ligne est notifié à l'organisme considéré comme responsable des traitements. Le cas échéant, des vérifications complémentaires sont effectuées, par exemple pour apprécier les mesures de sécurité mises en œuvre avant et après la constatation de la faille. Ces vérifications s'effectuent généralement sur place. L'ensemble des pièces et informations recueillies font ensuite l'objet d'une instruction par les services de la CNIL. En présence de manquements à la loi Informatique et Libertés, notamment à l'obligation de sécurité et de confidentialité des données (art. 34), et sur proposition d'un rapporteur désigné par la Présidente de la CNIL, la formation restreinte de la Commission peut prononcer une sanction pécuniaire pouvant aller jusqu'à 3 millions d'euros ou un avertissement, au terme d'une procédure contradictoire. Ces sanctions peuvent être rendues publiques et s'accompagner de l'obligation d'informer individuellement chaque personne affectée par la faille de sécurité.

CE QUE CHANGE LE RÈGLEMENT
EN MATIÈRE DE CONTRÔLES DE NOTIFICATION DES VIOLATIONS DE DONNÉES

Le règlement européen sur la protection des données prévoit une obligation générale de notification des violations de données à la CNIL. Cette obligation, aujourd'hui limitée aux fournisseurs de services de communications électroniques, s'appliquera alors à tout responsable de traitement. Son non-respect sera passible d'une amende administrative pouvant s'élever à 10 M d'euros, ou 2% du chiffre d'affaires annuel mondial dans le cas d'une entreprise. Ces règles seront applicables à partir du 25 mai 2018.

Bilan des actions coordonnées au niveau européen et international

En 2016, la CNIL a une nouvelle fois contribué aux actions menées par les autorités européennes et internationales de protection des données. Elle s'est ainsi jointe au « Sweep Day » pour la quatrième année consécutive et a pris part aux travaux de mise en œuvre du règlement européen, s'agissant en particulier des procédures dites répressives (ou « d'enforcement »).

Sweep day, les objets connectés sont-ils transparents sur l'utilisation des données ?

Pour la quatrième année consécutive, la CNIL et 24 autres autorités de protection des données ont mené un audit sur plus de 300 objets connectés. Cette opération conjointe s'inscrit dans le cadre du GPEN (Global Privacy Enforcement Network - réseau mondial de coopération entre autorités de protection des données).

Lors de cette journée, la CNIL a examiné 12 objets connectés relevant des secteurs de la domotique (gestion du domicile), de la santé et du bien-être, en se plaçant du point de vue de l'utilisateur. Cette analyse a confirmé que l'utilisation d'objets connectés implique la collecte de nombreuses données personnelles, y compris les plus sensibles (habitudes de vie, état de santé des utilisateurs). Or, elle a également mis en évidence l'insuffisance des mesures de protection des données qui entourent ces objets et ce, dans les 3 secteurs concernés. L'information transmise à l'utilisateur sur les traitements de ses données s'avère notamment peu précise et est, dans la plupart des cas, commune à l'ensemble des services proposés par la société qui commercialise l'objet utilisé. L'utilisateur n'est par conséquent pas en mesure de prendre pleinement conscience de son exposition et des risques de ces objets sur sa vie privée.

Cet audit, au-delà de l'action de coopération entre autorités de protection des données, ouvre la voie à des vérifications plus approfondies, éventuellement dans le cadre de contrôles, des traitements de données liés aux objets connectés.

Sous-groupe « Enforcement » du G29

Lors de sa réunion plénière de décembre 2016, le Groupe de l'article 29 (G29) a donné mandat au sous-groupe « Enforcement » pour être un lieu d'échange entre autorités, s'agissant en particulier des stratégies répressives et des procédures transfrontalières.

Le sous-groupe a plus particulièrement pour mission de :

- coordonner les procédures répressives impliquant plusieurs autorités européennes,
- œuvrer à l'harmonisation des méthodes de travail entre autorités,
- éprouver les mécanismes de coopération prévus par le règlement,
- participer au développement de nouveaux outils.

La CNIL participe activement aux travaux du sous-groupe et intervient en particulier sur les procédures transfrontalières relevant de sa compétence. Elle contribue également à l'identification des évolutions rendues nécessaires par le règlement.

CE QUE CHANGE LE RÈGLEMENT
EN MATIÈRE DE CONTRÔLES

Le règlement européen sur la protection des données sera directement applicable dès le 25 mai 2018, pour tous les responsables de traitements et sous-traitants qui ont leur établissement principal sur le territoire de l'Union européenne. A défaut d'un tel établissement, il s'appliquera aux responsables de traitements dès lors que des résidents européens seront sensiblement impactés par les traitements mis en œuvre. Concrètement, les pouvoirs d'enquête de la CNIL sur le terrain sont maintenus. Elle pourra en effet toujours accéder aux locaux du responsable des traitements, ainsi qu'à toutes les données et à toutes les informations nécessaires à l'accomplissement de ses missions.

En présence de traitements de données transnationaux, des mécanismes de coopération entre autorités et d'application cohérente du règlement sont prévus. La CNIL pourra ainsi effectuer des enquêtes conjointes avec d'autres autorités de contrôle européennes et échanger avec elles des informations relatives aux organismes contrôlés. Elle pourra intervenir en tant qu'autorité chef de file ou se joindre à des procédures communes. Le cas échéant, les autorités pourront prendre des mesures répressives conjointes, dont des sanctions pouvant atteindre 20 millions d'euros.

82
MISES EN DEMEURE

DONT
4
PUBLIQUES

13
SANCTIONS

DONT
4
SANCTIONS PÉCUNIAIRES ET PUBLIQUES

9
AVERTISSEMENTS DONT 4 PUBLICS

SANCTIONNER

La Présidente de la CNIL a prononcé 82 mises en demeure dont 4 mises en demeure publiques.

Les responsables de traitement mis en demeure de se conformer à la loi Informatique et Libertés peuvent demander à la présidente de la CNIL un délai supplémentaire si la complexité du dossier l'exige. Le délai initial, qui ne peut excéder 3 mois, ne peut être renouvelé qu'une seule fois.

En 2016, le nombre de ces demandes a connu une nette augmentation. Les organismes mettent notamment en avant des difficultés techniques pour se mettre en conformité dans des délais contraints sur des sujets complexes (cookies, sécurité des données, archivage massif et purge des données, etc.).

La formation restreinte a prononcé 13 sanctions :

- 4 sanctions pécuniaires, toutes publiques
- 9 avertissements, dont 4 publics

Gossip, les potins anonymes : mise en demeure publique pour atteinte grave à la vie privée

La présidente de la CNIL a mis en demeure le 26 septembre 2016 la société WGM, éditrice de l'application mobile « Gossip, les potins anonymes ».

Tout en restant anonymes, les utilisateurs de l'application pouvaient mettre en ligne des contenus (rumeurs, photos, vidéos), appelés « gossip » concernant une personne faisant partie de leur répertoire téléphonique ou de leurs contacts Facebook. Tous les utilisateurs de l'application ayant cette même personne dans leur carnet de contacts ou leurs contacts Facebook étaient destinataires du « gossip ». La personne ciblée par le « gossip » n'était pas forcément utilisatrice de l'application et pouvait ignorer faire l'objet d'une rumeur.

La Présidente de la CNIL a relevé que l'application était utilisée afin de diffuser des commérages et des accusations notamment à l'encontre de mineurs, tels que « [prénom] a 10 ans mais a déjà le VIH » ou « [prénom et nom de famille] 14 ans alcoolique (...) », pouvant être indéfiniment propagés par l'ensemble des personnes ayant reçu le gossip. Ces ragots pouvaient ainsi porter de graves préjudices à la personne concernée et à son entourage.

Par conséquent, la Présidente de la CNIL a considéré que la société W.M.G avait méconnu **l'article 1er de la loi Informatique et Libertés qui dispose que l'informatique « ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».**

La Présidente de la CNIL a également considéré que le traitement de données ne reposait sur aucune base légale, en méconnaissance de l'article 7 de la loi. En particulier, la société ne recueillait pas le consentement de la personne ciblée par le gossip et ne poursuivait pas un intérêt légitime supérieur à ses intérêts ou droits et libertés fondamentaux.

Au regard de la gravité de ces manquements, du nombre d'utilisateurs de l'application (plusieurs centaines de milliers au jour du contrôle de la CNIL) et des risques pour les personnes concernées, notamment les mineurs, la Présidente de la CNIL a décidé de mettre publiquement en demeure la société WGM.

Enfin, compte tenu de la nature des manquements constatés, mais aussi des risques pour les personnes concernées, notamment les mineurs, la Présidente de la CNIL a transmis l'ensemble des constats opérés et la mise en demeure au Procureur de la République, sur le fondement de l'article 40 du code de procédure pénale, afin que celui-ci puisse, le cas échéant, procéder à des investigations complémentaires.

Dans le délai imparti par la mise en demeure, la société a fermé l'application qui n'est plus utilisable.

Les recours devant le Conseil d'État

La durée de publication d'une sanction de la CNIL doit être limitée

Dans une décision rendue le 28 septembre 2016, le Conseil d'État a partiellement annulé une délibération de la formation restreinte de la CNIL prononçant un avertissement public car aucune limite de temps n'avait été préalablement définie concernant la publication sur le site internet de la CNIL et sur le site Légifrance.

Tout en confirmant que l'avertissement et sa publicité étaient justifiés compte tenu de la gravité des manquements à la loi Informatique et Libertés, le Conseil d'État a indiqué que la sanction complémentaire de publication devait respecter le principe de proportionnalité. Ainsi, la légalité de cette sanction doit s'apprécier au regard du support de diffusion et de la durée pendant laquelle cette publication est accessible de façon libre et continue. Le Conseil d'État a considéré qu'en l'espèce, la sanction était excessive car aucune limite n'avait été fixée concernant la durée de publication de l'avertissement de manière non anonyme.

Chargée par le Conseil d'État de fixer cette durée de publication, la formation restreinte de la CNIL a décidé que, dans cette affaire, la sanction devait être publiée pendant deux ans en ligne avant que le nom des personnes morales soit anonymisé.

À RETENIR

À l'occasion de cette décision, le Conseil d'État a considéré que les autorités administratives disposant de pouvoirs de sanction ont pour obligation de limiter la durée de publication d'une telle décision afin de respecter le principe de proportionnalité.

CE QUE CHANGE LE RÈGLEMENT
EN MATIÈRE DE CONTRÔLES

Les autorités de protection pourront imposer des amendes administratives très conséquentes (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial d'une entreprise). Ces sanctions pécuniaires pourront être prises en complément ou à la place de nombreuses mesures correctrices (ordonner de communiquer à la personne concernée une violation de données, ordonner la rectification, l'effacement de données ou la limitation du traitement, retirer une certification, ordonner la suspension de flux de données vers un pays tiers, etc.)

Ces mesures et sanctions ne seront plus limitées au responsable de traitement mais pourront également être prises à l'égard d'un sous-traitant.

Dans l'hypothèse de traitements transfrontaliers, la CNIL travaillera en étroite coopération avec d'autres autorités de protection afin qu'une seule décision de sanction soit adoptée par l'autorité chef de file.

INFOSPLUS

Consolidation de la doctrine de la CNIL en matière de sécurité et de confidentialité

Les enjeux de sécurité informatique, et notamment de cybersécurité, occupent une place croissante dans la protection des données personnelles et, par suite, dans l'activité de la CNIL (cf. rapport annuel 2015). La formation restreinte de la CNIL a ainsi, dans plusieurs affaires, sanctionné des responsables de traitements pour des manquements à la sécurité et à la confidentialité des données personnelles, notamment dans le secteur de la vente en ligne.

Des enquêteurs de la CNIL ont par exemple constaté que des milliers de données de cartes bancaires étaient inscrites dans des zones de commentaires et accessibles à des prestataires d'une société. Dans une autre affaire, les contrôleurs ont librement accédé à des milliers de données contenues dans les répertoires du site web, dont des coordonnées et informations bancaires de clients.

La formation restreinte a considéré que le défaut de préjudice personnel ou d'accès frauduleux aux données est sans influence sur la caractérisation du manquement. En outre, le responsable de traitement ne peut s'exonérer de ses obligations si le manquement est le fait de son sous-traitant.

L'obligation d'assurer la sécurité et la confidentialité des données est encore renforcée par le règlement européen, qui sera applicable le 25 mai 2018 : outre que les organismes devront notifier à la CNIL les failles de sécurité dont ils pourraient faire l'objet, les manquements aux obligations de sécurité seront passibles de sanctions s'élevant à 10 millions d'euros ou 2% du chiffre d'affaires mondial.

DERNIÈRE MINUTE

Une définition stricte de la notion d'anonymisation des données

Dans une décision rendue le 8 février 2017, le Conseil d'État a rejeté une requête de la société JCDecaux France demandant à annuler un refus d'autorisation de la CNIL pour la mise en œuvre d'un traitement d'estimation de la fréquentation du quartier de La Défense. Le projet consistait en l'installation de boîtiers sur le mobilier publicitaire de la société afin de capter les adresses MAC des téléphones portables des personnes passant à proximité. Des panneaux devaient informer les personnes du déploiement de ce dispositif.

La CNIL a considéré que le procédé technique envisagé par la société pour assurer la confidentialité des données collectées (en l'espèce, par le troncage, le salage et le hachage de l'adresse MAC) ne pouvait être qualifié de processus d'anonymisation. Le Conseil d'État a confirmé la position de la CNIL, en relevant que le projet consistant à compter le nombre de personnes présentes à proximité du mobilier publicitaire, mais aussi à mesurer la répétition de leurs passages, était par nature incompatible avec une anonymisation des données. Enfin, le Conseil d'État a confirmé la position de la CNIL jugeant les moyens d'information des personnes insuffisants.

Le renvoi de plusieurs questions préjudicielles à la Cour de justice de l'Union européenne (CJUE) pour la mise en œuvre du droit au déréférencement

La CJUE, dans la célèbre décision Google Spain du 13 mai 2014, a consacré le droit au déréférencement, c'est-à-dire le droit pour toute personne de demander, sous certaines conditions, à l'exploitant d'un moteur de recherche de supprimer de sa liste de résultats certains liens la concernant. Si un refus est opposé, les personnes concernées peuvent saisir la CNIL qui doit alors examiner si les conditions permettant un déréférencement sont réunies.

En l'espèce, le Conseil d'État devait se prononcer sur quatre affaires pour lesquelles la Présidente de la CNIL avait confirmé le refus de la société Google Inc. de procéder au déréférencement et clôturé les plaintes dont elle était saisie. Les liens litigieux portaient sur des informations diverses telles que des articles de presse relatant la condamnation du plaignant pour agressions sexuelles sur mineurs ou encore un montage vidéo évoquant une relation entre l'une des requérantes et un personnage public. Pour statuer sur ces requêtes, le Conseil d'État a estimé, dans quatre décisions du 24 février 2017, que des précisions devaient être apportées par la CJUE sur les modalités de mise en œuvre du droit au déréférencement.
Plus précisément, par le biais de quatre questions préjudicielles, la juridiction a notamment demandé :

- si l'interdiction faite aux responsables de traitement de traiter des données sensibles (telles que les données relatives aux opinions politiques ou religieuses, à l'orientation sexuelle ainsi qu'aux condamnations pénales) était applicable aux moteurs de recherche.

- quelles sont les suites à donner aux demandes de déréférencement lorsque les informations concernées figurent dans des articles de presse, sont inexactes ou incomplètes ou encore lorsque leur publication est illicite.

LES LISTES DES ORGANISMES CONTRÔLÉS, DES MISES EN DEMEURE ET DES SANCTIONS SONT DISPONIBLES SUR LE SITE DE LA CNIL.

ANTICIPER
et innover

Dans le cadre de son activité d'innovation et de prospective, la CNIL met en place une veille pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée. Elle dispose d'un laboratoire lui permettant d'expérimenter des produits ou applications innovants. Elle contribue au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de *privacy by design*. Cette activité, développée depuis plusieurs années, lui permettra de répondre à la nouvelle mission de promotion des technologies de protection de la vie privée, notamment en matière de chiffrement, confiée par la loi pour une République numérique du 7 octobre 2016. Pour renforcer sa réflexion, elle a créé un comité de la prospective faisant appel à des experts extérieurs qui la conseille pour élaborer un programme annuel d'études et d'explorations.

Vincent
Technologiste au service de l'expertise technologique

Nous sommes 10 experts au sein du service (ingénieurs, chercheurs, consultants ou designers), chacun avec ses spécialités (cybersécurité, biométrie, objets connectés, Big data, cryptographie, anonymisation, santé, banque, gestion des risques, design, etc.).

Si la loi se veut agnostique des technologies, son application doit tenir compte de leurs évolutions et de leurs usages. Notre rôle est d'épauler les juristes sur les aspects techniques des dossiers dont la CNIL est saisie, d'anticiper les conséquences juridiques que peuvent avoir les choix technologiques, et de proposer des solutions techniques à des problèmes juridiques ; bref, être l'interface entre les juristes et la technique. Nous travaillons donc à la fois sur la doctrine, l'accompagnement à la conformité, et le contentieux. Ainsi, nous faisons des recommandations puis sommes confrontés à leurs résultats opérationnels.

Par ailleurs, nous collaborons beaucoup avec nos homologues, soit dans le cadre du G29, soit au travers de missions plus spécifiques. J'ai notamment pu passer 3 mois à la Federal Trade Commission (FTC) pour étudier les options de ciblage « Ethnic Affinity » de Facebook.

Nous avons enfin notre « Labo », où nous effectuons des expérimentations, pour identifier les usages émergents et nouvelles problématiques, vérifier la conformité d'équipements ou développer des preuves de concept, par exemple pour essayer de suivre les flux d'informations entre les différents acteurs de la publicité sur le web.

LINC : UN REGARD DIFFÉRENT

2016 aura été l'occasion pour la CNIL de structurer davantage ses activités d'innovation, de recherche et de prospective à travers la création de LINC, le « Laboratoire d'Innovation Numérique de la CNIL ».

Au-delà de son action de régulation, la CNIL catalyse des débats sur les enjeux associant éthique, libertés, données et usages du numérique. L'objectif de LINC est de proposer un regard différent aux citoyens, aux experts et aux professionnels, et d'animer une communauté de recherche et prospective sur la protection des données, en faisant connaître les travaux de chercheurs comme en diffusant les activités d'innovation de la CNIL.

« Explorer, échanger, expérimenter. »

LINC permet d'anticiper, informer et partager sur les tendances émergentes du numérique et leurs enjeux en matière de vie privée. C'est également une plateforme d'innovation, permettant aux équipes de la CNIL de conduire des projets d'expérimentation et de prototypage d'outils, de services ou de concepts autour des données.

Les activités de LINC se développent ainsi autour de 3 axes (explorer, échanger, expérimenter), qui trouvent leur expression dans 3 déclinaisons de LINC : un média en ligne linc.cnil.fr, un espace physique dans les nouveaux locaux de la CNIL et une refonte des activités du laboratoire.

Un nouveau média en ligne

La CNIL a lancé en avril 2016 le nouvel espace éditorial linc.cnil.fr où les équipes de la CNIL partagent leur veille, leurs réflexions, et documentent leurs explorations de sujets émergents.

LINC permet notamment de partager et diffuser plus largement les travaux de la CNIL en direction de l'ensemble des acteurs de l'innovation et de l'écosystème numérique (chercheurs, startups, labos, etc.).

En 2016, près de 70 articles ont été publiés sur des thèmes allant du véhicule connecté à la ville numérique, des drones à la robotique, en passant par l'intelligence artificielle ou les jeux vidéo.

Ces articles permettent également à la CNIL de dévoiler les coulisses de ses projets d'innovation, comme la réalisation d'une dataviz permettant d'explorer le règlement européen sur la protection des données, et de comprendre les liens et équilibres entre ces différents articles. Cette réalisation, inédite, a été mise à disposition sur le site internet de la CNIL, le code source étant diffusé en open source.

Un espace physique pour s'ouvrir et héberger des démonstrateurs

L'espace LINC, dans les nouveaux locaux de la CNIL, permet d'héberger et de diffuser des expérimentations qui ont vocation à rendre visible et mieux saisir le rôle des données dans les services numériques.

Ce lieu est aussi un point de contact et d'échange avec les écosystèmes d'innovation et du numérique, destiné à accueillir des intervenants externes porteurs de projets (entrepreneurs, chercheurs, auteurs, artistes) comme à organiser des événements de travail et de créativité.

Une plateforme de gestion de projets d'expérimentation et de recherche : le Labo

Depuis 2011, la CNIL développe, seule ou en partenariat, des projets de recherche et d'expérimentation dans le cadre de ses activités de laboratoire. C'est ainsi que CookieViz ou Mobilitics ont vu le jour.

Le labo de la CNIL est à la fois :

- une plateforme de tests et analyses au service de l'institution, qui permet d'obtenir une meilleure connaissance technique des écosystèmes que la CNIL régule ;
- une plateforme d'innovation pour porter et mener à bien des projets de « R&D ».

Il permet de tester des technologies en vue de sensibiliser les internautes et les responsables de traitements, et de mettre à leur disposition des outils (expérimentation, veille, analyse, prototypage, démonstrations, développement d'outils et services mis à disposition du public...).

Sur linc.cnil.fr, un espace « Expérimentations » réunit l'ensemble des ressources produites dans le cadre des projets Cookieviz et Mobilitics, dont le code source de Cookieviz, disponible sous licence libre GPLv3 sur le GitHub de linc (https://github.com/LINCnil).

PARTAGE !

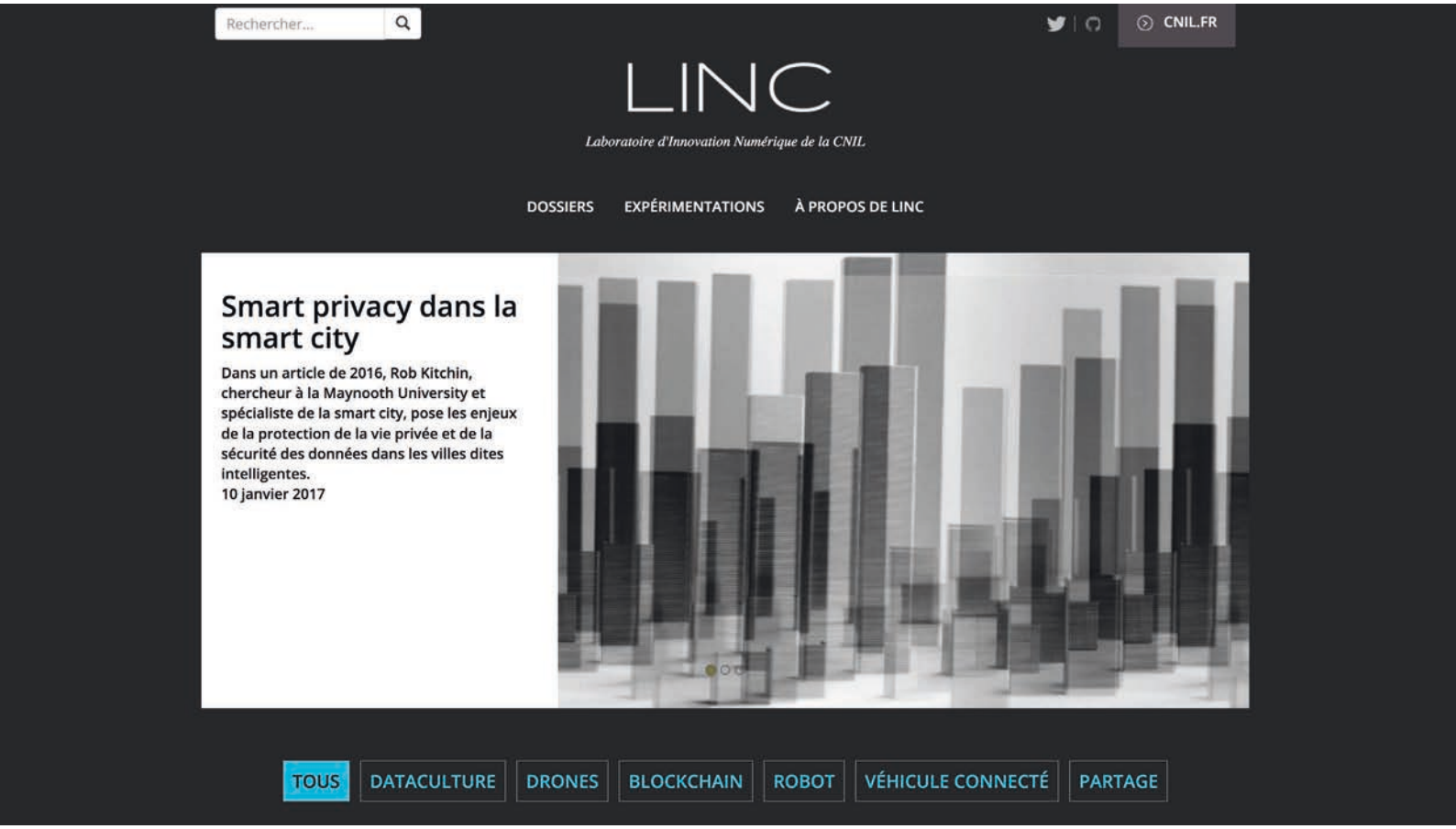
Motivations et contreparties au partage dans la société numérique

En 2015/2016, le Comité de la prospective, animé par LINC, a échangé sur la thématique du partage, ce qui a mené à la publication du quatrième cahier d'innovation et prospective de la CNIL.

Disponible en téléchargement sur le site de la CNIL, le cahier parcourt la notion de partage dans la société numérique, ses ressorts et les contreparties, les questions et débats portant sur le partage de la valeur et ses modèles économiques, les enjeux d'équilibre des pouvoirs entre plateformes et utilisateurs, ainsi que les leviers de régulation à envisager. Il propose notamment une taxonomie du partage, une cartographie de controverses et un scénario prospectif sur des usages possibles de la *blockchain*.

Le 29 juin 2016, le LINC organisait une rencontre autour des questions soulevées par le cahier. Près de cent personnes ont assisté à cette matinée, également riche en débats sur les réseaux sociaux.

Présidé par la Présidente de la CNIL, Isabelle Falque-Pierrotin, le comité de la prospective se compose de douze experts extérieurs : Laurent Alexandre, Pierre-Jean Benghozi, Stefana Broadbent, Dominique Cardon, Milad Doueihi, Claude Kirchner, Cécile Méadel, Tristan Nitot, Bruno Patino, Antoinette Rouvroy, Henri Verdier et Célia Zolynski, et de deux commissaires de la CNIL : Joëlle Farchy et Eric Pérès.



CRÉATION DU PRIX EUROPÉEN CNIL -INRIA

Le Prix CNIL-INRIA créé en janvier 2016 récompense un article scientifique dans le domaine des sciences du numérique traitant de l'amélioration de la protection des données personnelles ou de la vie privée. Le prix 2016 a été décerné à l'article: "ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data".

C'est à Bruxelles, lors de la 10ème édition de la Conférence internationale Computers Privacy and Data Protection (CPDP 2017), en présence d'Isabelle Falque-Pierrotin, Présidente de la CNIL et François Sillion, directeur général délégué à la science d'Inria, que les deux institutions ont remis le premier Prix CNIL-Inria- Protection des données, aux co-auteurs Michael Backes, Manuel Barbosa, Dario Fiore et Raphael M. Reischuk pour leur article ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data.

Il décrit des travaux de recherche qui permettent de vérifier les résultats d'un traitement informatique sur des données personnelles authentifiées par un tiers sans divulguer ces données. Pour cela, les auteurs proposent un nouveau système ADSNARK améliorant les schémas de « preuves sans divulgation de connaissances » (zero knowledge proofs), habituellement utilisés mais peu réalistes pour certains calculs.

Cet article a été initialement publié dans les actes de la conférence IEEE Security and Privacy 2015 de San Jose (Californie, Etats-Unis, 18 au 20 mai 2015). Le jury a souligné la grande qualité des résultats et a particulièrement apprécié le souci des auteurs de concilier solidité technique et facilité d'utilisation pratique. Les résultats obtenus répondent à un besoin croissant et peuvent permettre de mieux protéger la vie privée dans des domaines variés comme, par exemple, ceux de la santé ou des compteurs intelligents. On se félicite également du caractère européen du projet de recherche décrit dans l'article, qui a impliqué des chercheurs de quatre nationalités différentes. Les inscriptions pour la deuxième édition 2017 du Prix CNIL-INRIA sont ouvertes.

Les sujets de réflexion en 2017

Quelle place pour le citoyen dans la ville numérique ?

Ville numérique, connectée, intelligente, résiliente ou créative... quel que soit le terme, la donnée reste toujours au cœur des processus de la transformation urbaine. Mais la donnée ne rend pas la ville intelligente. Elle rend en revanche possible l'intelligibilité de la ville, par la visualisation et l'optimisation de services urbains comme les transports, l'énergie ou l'eau. Les mouvements et échanges physiques de la ville correspondent à autant de flux de données qu'il convient de maîtriser et de réguler, pour la protection des données personnelles et des libertés.

Depuis plus d'une décennie, les projets de villes dites intelligentes se sont étendus à travers le globe. Deux modèles et approches ont cohabité jusqu'à présent, la *smart city*, le plus souvent portée par de grands acteurs historiques de l'informatique, et la ville numérique des *« civic hackers »*[1], celle des petites entreprises et des citoyens qui construisent des services autour des données. Cet équilibre est aujourd'hui remis en cause par l'arrivée des « industriels de la donnée ».

Deux modèles : Smart city vs civic hackers

Le concept de *smart city* représente une vision centralisée, *top down* et bureaucratique de la gestion urbaine : chacun des aspects est mesurable et contrôlable. Le mode de fonctionnement s'organise autour d'un ou plusieurs opérateurs, clés de voûte de l'ensemble, et englobe des traitements de données liés à tous les secteurs des infrastructures publiques, des transports, de l'énergie, etc. L'individu, bien que destinataire final du service, ne prend pas une part active dans la dynamique de la ville, voire la subit. À Songdo (Corée), Masdar (Émirats Arabes Unis), ou Singapour, les capteurs disséminés dans la ville promettent de tout mesurer : la propreté des espaces publics, la densité de population en temps réel ou le mouvement de chaque véhicule sur le territoire.

Dans l'approche *bottom up*, des développeurs indépendants utilisent les données pour promouvoir de nouvelles pratiques urbaines, plus collaboratives. On peut citer l'application de géolocalisation *Foursquare*, la cartographie collaborative *Open Street Map* ou des initiatives de *crowdsourcing* comme *Fix My Street* au Royaume-Uni, dont les utilisateurs font remonter les « *bugs* » de la cité aux autorités par une appli-

1 Anthony Townsend, *Smart Cities - Big Data, Civic Hackers, and the Quest for a New Utopia*, éd. W. W. Norton & Company, octobre 2013

« Dans la ville toujours plus connectée, les citadins pourront-ils rester maîtres de leurs données ? »

cation géolocalisée sur smartphone. Les données agrégées produites dans le cadre de l'utilisation de ces services peuvent parfois être mises au service de la collectivité, à l'image de Strava, qui revend à Seattle des informations sur le trafic urbain à vélo.

En fait, ces deux modèles fonctionnent comme des idéaux types. On en retrouve des caractéristiques dans de nombreuses métropoles.

« Industriels de la donnée », de nouveaux acteurs, pour de nouveaux enjeux

De nouveaux entrants, qui ne sont ni plus ni moins que les plateformes mondialisées de l'internet, arrivent sur le marché de la gestion urbaine. C'est fort des données qu'elles ont elles-mêmes collectées, de leur capacité à opérer techniquement et d'une forme de légitimité liée à la convocation de la multitude[2] qu'ils entendent s'imposer aux villes. Parmi ces nouveaux acteurs, on retrouve notamment *SideWalkLabs* (Alphabet – Google), *Waze* (propriété d'Alphabet), et *Uber*. Chacun propose déjà aux collectivités des outils de visualisation des flux de trafic ou travaille à des véritables tableaux de bord urbains. En offrant des services clés en main, à l'apparente gratuité, et en important leurs modèles économiques dans l'espace urbain, ils parviennent à imposer des contrats dont ne ressortent pas toujours les principes protection de la vie privée et des libertés. Le rapport des collectivités à ces nouveaux entrants et les modalités de « vivre ensemble » qu'ils trouveront – depuis la DSP (délégation de service public) au simple partenariat - seront l'un des enjeux majeurs pour les années à venir, pour l'acteur public, mais également pour les citoyens.

À SUIVRE

Quelle égalité devant la smart city ?

La ville dite « intelligente » soulève de nombreux enjeux, sans qu'ils soient limités à la protection de la vie privée et des libertés. La CNIL traite déjà de nombreux dossiers autour des bâtiments intelligents, du mobilier urbain connecté, des compteurs communicants... mais au-delà, la smart city interroge sur le fondement même de la définition de la ville et de son rapport aux citoyens. Pensée pour les métropoles, elle implique de lourds investissements, difficilement accessibles aux petites collectivités, pour des niveaux de services toujours plus élevés pour ses habitants, posant ainsi la question de l'égalité devant le service public. La gestion des flux par le numérique sera-t-elle facteur d'émancipation et de rapprochement des périphéries, ou bien génératrice d'inégalités ? Dans cette ville toujours plus connectée, les citadins pourront-ils rester maitres de leurs données, pourra-t-on évoluer dans l'espace urbain sans avoir à les troquer ? Quels seront les modèles économiques de la ville ? Autant de questions que la CNIL explorera en 2017 dans la 5ème édition du cahier IP, sur le thème de la place du citoyen dans la ville connectée.

2 Nicolas Colin, Henri Verdier, *L'âge de la multitude : entreprendre et gouverner après la révolution numérique*, éd. Armand Colin, 2012

Éthique et numérique : les algorithmes en débat

et éthique numérique
les algorithmes en débat

DÉFINITION

Qu'est-ce qu'un algorithme ?

Un algorithme est la description d'une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée. Par exemple, une recette de cuisine est un algorithme permettant d'obtenir un plat à partir de ses ingrédients ! Dans le monde de plus en plus numérique dans lequel nous vivons, les algorithmes mathématiques permettent de combiner les informations les plus diverses pour produire une grande variété de résultats : simuler l'évolution de la propagation de la grippe en hiver, recommander des livres à des clients sur la base des choix déjà effectués par d'autres clients, comparer des images numériques de visages ou d'empreintes digitales, piloter de façon autonome des automobiles ou des sondes spatiales, etc.

Pour qu'un algorithme puisse être mis en œuvre par un ordinateur, il faut qu'il soit exprimé dans un langage informatique, sous la forme d'un logiciel (souvent aussi appelé « application »). Un logiciel combine en général de nombreux algorithmes : pour la saisie des données, le calcul du résultat, leur affichage, la communication avec d'autres logiciels, etc.

Certains algorithmes ont été conçus de sorte que leur comportement évolue dans le temps, en fonction des données qui leur ont été fournies. Ces algorithmes « auto-apprenants » relèvent du domaine de recherche des systèmes experts et de l'« intelligence artificielle ». Ils sont utilisés dans un nombre croissant de domaines, allant de la prédiction du trafic routier à l'analyse d'images médicales.

72 %* **des Français estiment que les algorithmes représentent un enjeu de société**

3 Étude réalisée par l'IFOP du 9 au 11 janvier 2017 auprès d'un échantillon de 1001 personnes, représentatif de la population française âgée de 18 ans et plus. Questionnaire auto-administré en ligne.

Les Français et les algorithmes : notoriété et perception

D'après un sondage mené par l'IFOP [3] pour la CNIL en janvier 2017, les algorithmes sont présents dans l'esprit des Français mais de façon assez confuse. Si 83 % des Français ont déjà entendu parler des algorithmes, ils sont plus de la moitié à ne pas savoir précisément de quoi il s'agit (52%). Leur présence est déjà jugée massive dans la vie de tous les jours par 80% des Français qui considèrent, à 65%, que cette dynamique va encore s'accentuer dans les années qui viennent.
Concernant l'opinion sur les algorithmes, une courte majorité (53%) estime qu'ils sont plutôt sources d'erreurs contre 47% qui pensent qu'ils sont fiables. Mais la confiance s'élève à mesure que le niveau de connaissance sur les algorithmes progresse. Un effort de pédagogie et de transparence peut donc contribuer à renforcer la confiance.

Sous un angle marketing, 57% des Français pensent que les algorithmes limitent l'étendue des choix proposés. Chez les plus jeunes, la tendance s'inverse, puisque 53% des moins de 35 et 56% des 18-24 ans mettent plutôt en avant le fait que les algorithmes proposent plus de choix.

Enfin, c'est sous l'angle de la perception citoyenne que l'opinion est la plus tranchée en fonction de l'âge. Si 2/3 des Français (64%) considèrent que les algorithmes représentent plutôt une menace en raison de l'accumulation de données personnelles sur les choix, les goûts et les comportements, les 18-24 ans inversent cette tendance nettement affirmée puisque 51% estiment

au contraire que les algorithmes représentent une opportunité.

Une nouvelle mission confiée à la CNIL

La loi pour une République numérique du 7 octobre 2016 a confié à la CNIL la mission de conduire une réflexion sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques. La CNIL a choisi d'y répondre rapidement en initiant un cycle de débats publics, ateliers ou rencontres.

Les algorithmes, un enjeu primordial

En 2017, cette réflexion portera sur les algorithmes à l'heure de l'intelligence artificielle. En effet, ceux-ci occupent dans nos vies une place importante, bien qu'invisible. Résultats de requêtes sur un moteur de recherche, ordres financiers passés par des robots sur les marchés, diagnostics médicaux automatiques, affectation des étudiants à l'Université : dans tous ces domaines, des algorithmes sont à l'œuvre. Ces derniers mois, le sujet des algorithmes s'est invité dans le débat public et a suscité une forte attention médiatique. Face à ces interrogations, des réactions diverses et souvent passionnées, entre enthousiasme, fascination, inquiétude et contestations se font jour. Les progrès récents de l'intelligence artificielle et du machine learning renforcent encore l'ampleur des défis posés. Faire des algorithmes l'objet d'un vaste débat public pour faire progresser la connaissance et la réflexion par la société civile s'impose donc comme une nécessité.

Un débat public décentralisé, initié par la CNIL

Le rôle de la CNIL consiste à initier un processus de discussion collectif que feront vivre tous ceux – institutions publiques, société civile, entreprises – qui souhaitent y prendre part en organisant des débats et manifestations multiformes. La CNIL assurera la coordination et la cohérence de ces diverses manifestations.

Une quinzaine d'organismes se sont déjà associés à cette initiative.

Le 23 janvier, la CNIL a lancé un cycle de débats publics sur ce thème en organisant un après-midi d'échanges autour de deux tables rondes.

La première, intitulée Des algorithmes et des hommes a réuni :

- **Paul Duan** (Bob emploi)
- **Roger-François Gauthier** (Professeur de politique éducative comparée, Paris V)
- **Jean-Philippe Desbiolles** (IBM France)
- **Rand Hindi** (Cnnum, Snips)
- **Antoine Garapon** (IHEJ)

La seconde table-ronde intitulée Loyauté, transparence, pluralité a réuni :

- **Dominique Cardon** (Sciences Po, Médialab)
- **Antoinette Rouvroy** (Université de Namur)
- **Bruno Patino** (Arte)

Une présentation de la plateforme Transalgo (Inria) était proposée par **Nozha Boujemaa**.

Les discussions ont permis d'identifier une série de questions éthiques générales soulevées par les algorithmes :

1. **Comment s'assurer que la prédiction et la recommandation fournies par les algorithmes soient une aide à la prise de décision et à l'autonomie ? Comment se prémunir d'une déresponsabilisation de l'homme et d'une perte d'autonomie ?**

2. **Faut-il fixer des limites à l'utilisation des algorithmes ?** Peut-on identifier des domaines, des cas où le recours à des algorithmes serait techniquement possible mais se heurterait à une impossibilité éthique ?

3. **Quelle éthique des données ?**

4. **Quelle elle est la réalité du risque souvent invoqué de l'« enfermement » algorithmique ?** Comment faire en sorte que les algorithmes favorisent la pluralité ?

5. **Quelles procédures imaginer pour éviter que l'utilisation des algorithmes n'ait pas pour effet l'imposition à tous de systèmes de valeurs particuliers (ceux des développeurs et d'intérêts privés déterminant les critères de fonctionnement des algorithmes ou encore ceux de l'entité qui a fourni les données traitées par l'algorithme)** ? Comment sont perçues des solutions telles que la loyauté, la transparence, l'explicabilité des algorithmes ?

6. **Comment éviter que la personnalisation accrue permise par les algorithmes n'ait des effets de fragmentation de l'espace public, de démutualisation, etc ?**

À SUIVRE

À l'automne 2017, la CNIL rendra publique la synthèse des échanges et des contributions. Il s'agira d'établir une cartographie de l'état du débat public et un panorama des défis et enjeux. Des pistes ou propositions pour accompagner le développement des algorithmes dans un cadre éthique pourraient faire par la suite l'objet d'arbitrages par les pouvoirs publics.

Lancement de la collection : « POINT CNIL »

Partant du constat que les questions de protection des données personnelles n'ont jamais été aussi omniprésentes dans notre société mais qu'elles restent trop souvent l'apanage d'un petit cercle d'experts, la CNIL a décidé de lancer une nouvelle collection d'ouvrages didactiques, de format poche et à prix modique, les « POINT CNIL ».

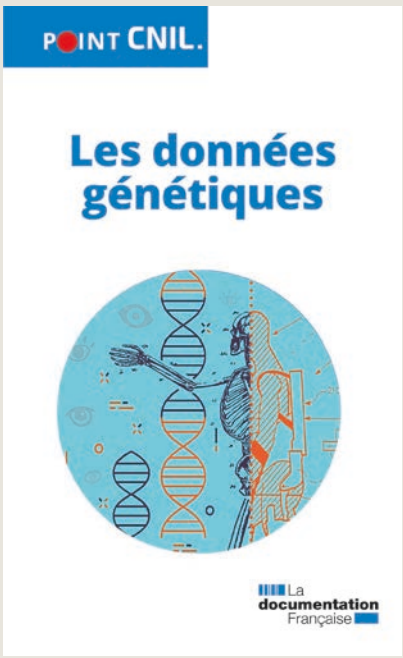
Cette collection, thématique, a vocation à s'adresser aussi bien au grand public curieux des sujets de société et désireux d'en savoir plus sur la protection des données personnelles dans tel ou tel domaine qu'aux étudiants, enseignants, éducateurs intéressés, dans le cadre de leurs cursus de formation, à développer leurs connaissances et à approfondir les questions Informatique et Libertés sur des sujets précis.

La collection POINT CNIL propose :

- Un état des lieux du thème abordé selon une approche qui se veut synthétique et pédagogique,
- Un exposé de la problématique,
- Un état des lieux de la doctrine avec une approche pluridisciplinaire, tenant compte éventuellement d'expériences étrangères,
- Une présentation des questions restées ouvertes,
- Une bibliographie

Il s'agit ainsi de rendre plus accessibles les avis et recommandations de la CNIL ayant un rapport avec la thématique proposée et, par voie de conséquence, d'intégrer les questions de protection des données personnelles partout où elles peuvent contribuer à susciter ou à alimenter le débat public.

Ces ouvrages, dont le rythme de publication devrait être annuel, sont édités par La Documentation Française.



Un premier numéro consacré aux données génétiques.

Les données génétiques ne sont pas des données personnelles comme les autres. Particulièrement intimes, de plus en plus signifiantes, potentiellement très discriminantes, ces données bénéficient, de ce fait, d'un statut très protecteur, récemment renforcé avec le règlement européen. Leur utilisation est aujourd'hui strictement encadrée par la loi et par la CNIL, qu'il s'agisse des banques de données génétiques créées à des fins de recherche médicale, de diagnostic et de thérapie ou, dans le domaine judiciaire, des traitements d'identification par empreintes génétiques. Mais avec l'essor de ce que l'on appelle le *Big data* génomics, l'usage des données génétiques tend à se banaliser, de nouveaux acteurs émergent et un véritable marché des données génétiques se développe, avec en germe, de nouveaux enjeux éthiques tant pour l'individu que pour la société dans son ensemble. Risques de manipulations génétiques, de nouvelles discriminations sociales sur fond de déterminisme génétique, croyance en une preuve biologique jugée parfaite, en une vérité génétique absolue, autant de questionnements que ce premier numéro a pour ambition de présenter et d'explorer sous le regard de la protection des données.

Ce premier numéro devrait être disponible en librairie à la fin du 1er semestre 2017.

Les Ressources

LES RESSOURCES HUMAINES

En 2016, la CNIL a dû faire face à l'augmentation soutenue de ses missions traditionnelles, et à l'accroissement de son périmètre d'intervention, notamment avec l'entrée en vigueur de la Loi pour une République numérique du 7 octobre 2016. Ce texte législatif conforte et élargit les compétences de la CNIL (pouvoir de sanction renforcé, affirmation de la mission de promotion de l'utilisation des technologies protectrices de la vie privée, certification de la conformité des processus d'anonymisation des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation, conduite d'une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques). Les premiers effets ont été immédiats, avec la hausse sensible entre octobre et décembre des saisines de la CNIL pour avis par le Gouvernement. Les autres missions vont se déployer en 2017.

Pour faire face à ses missions en 2016, la CNIL a bénéficié d'une allocation complémentaire de 6 emplois par le législateur, passant de 189 emplois en 2015 à **195 emplois en 2016**, soit une progression de 3,1%. Les nouveaux emplois ont permis de consolider les équipes dédiées aux activités « traditionnelles » de la CNIL (réponses aux demandes de conseil, instruction des demandes d'autorisation, , instructions de plaintes, contrôles, sanctions) afin d'améliorer constamment la qualité du service rendu aux usagers, mais aussi de renforcer les équipes en raison des dernières missions confiées par le législateur (contrôles en ligne).

La mise en œuvre du règlement européen sur la protection des données personnelles en mai 2018 implique une évolution majeure de l'institution, notamment pour accompagner les agents dans l'appropriation du nouveau cadre juridique applicable et l'évolution de leurs métiers. Un plan de formation renforcé a donc été mis en place.

L'année 2016 a également été marquée par le déménagement de la CNIL sur un nouveau site (Fontenoy-Ségur) et par son adhésion à des mutualisations de certaines fonctions supports qui s'est traduite par le transfert de 4 emplois à la Direction des services administratifs et financiers des services du Premier ministre.

DONNÉES SOCIALES

195 emplois fin 2016

41 ans Âge moyen

63% de femmes

37% d'hommes

53% des agents travaillant à la CNIL sont arrivés entre 2011 et 2016

75% des agents occupent un poste de catégorie A

38% des postes occupés par des juristes

22% des postes occupés par des assistants

12% des postes occupés par des des ingénieurs / auditeurs

LES RESSOURCES FINANCIÈRES

En 2016, le budget alloué à la CNIL s'élève à **16 964 049 €** en autorisations d'engagements et à 18 710 003 € en crédits de paiement, répartis comme suit : 13 842 41 € pour le budget de personnel (rémunérations, titre 2) et 3 121 208 € en autorisations d'engagements et 4 867 162 € en crédits de paiement pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6).

L'évolution des crédits alloués au budget du personnel s'explique par la création des 6 postes.

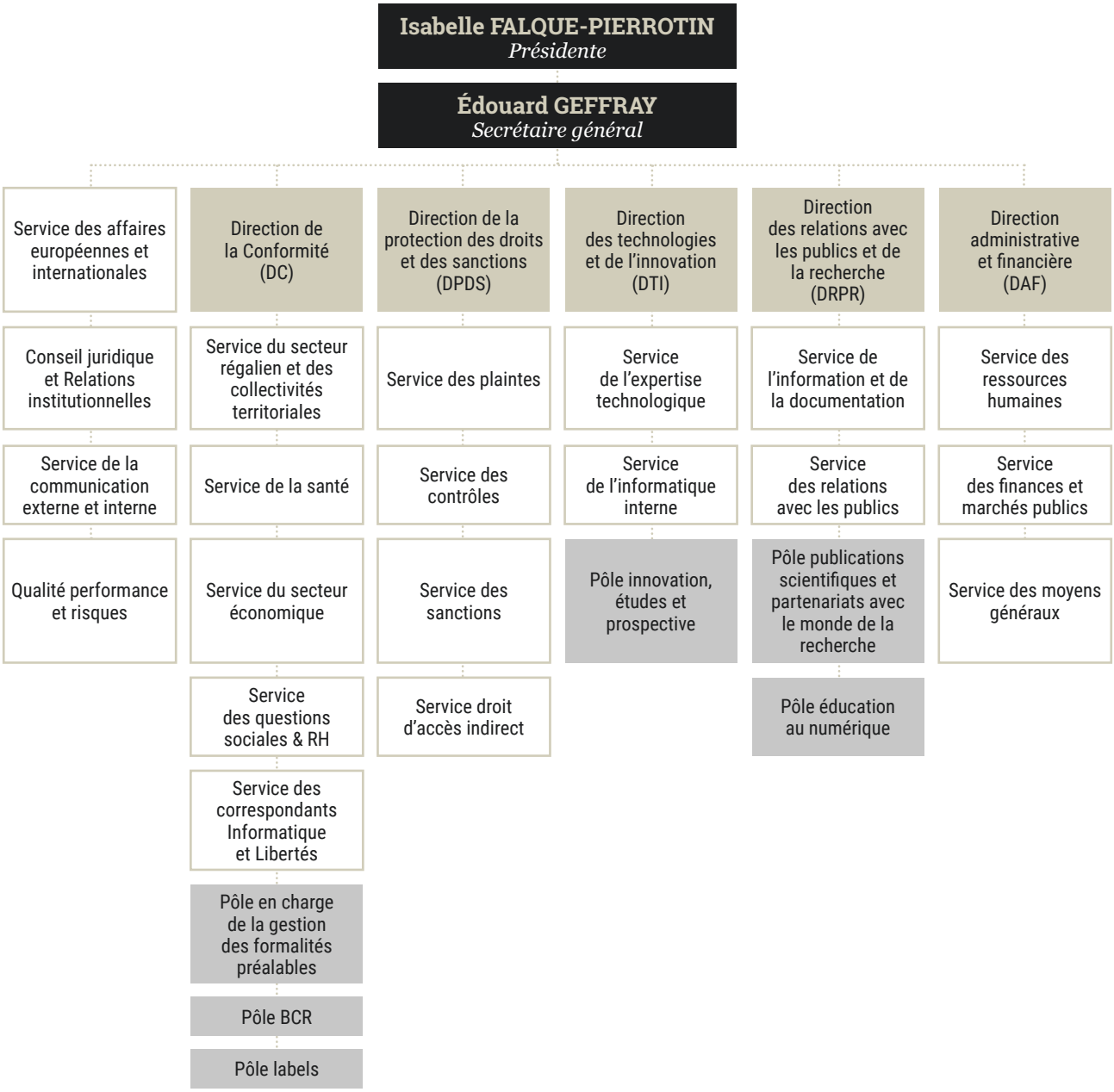
Le budget de fonctionnement diminue de 6.5% en raison de :

- une politique volontariste de réduction de ses dépenses par la CNIL : alors que les crédits ouverts en 2012 s'élevaient à 5,6 millions, ils ne sont plus que de 4,867 millions en 2016, alors que l'activité a considérablement augmenté sur cette même période ;
- l'effort budgétaire demandé aux institutions publiques, particulièrement contraignant en 2016 avec un gel en début d'exercice et un sur-gel des crédits en cours de gestion,
- la diminution des crédits liés à la finalisation de la refonte du Schéma Directeur des Systèmes d'Information (SDSI)
- la poursuite de la mutualisation d'achats en lien avec les services du Premier ministre et la direction des achats de l'État dans le but de dégager des économies,
- l'impact de la renégociation des baux de la CNIL, avec une économie de 730 000 € en 2016.

L'année 2016 a permis de finaliser le schéma directeur des systèmes d'information (SDSI) dans des conditions satisfaisantes et conformes au calendrier prévu, afin d'améliorer le service aux usagers (cf. Besoin d'aide ?) et la productivité de l'institution (plaintes en ligne) et d'internaliser des projets métiers, comme les outils de consultation pour le règlement européen.

CRÉDITS 2016	Autorisations d'engagement	Crédits de paiement
Budget LFI	**17 460 865**	**19 358 641**
Titre 2	13 912 403	13 912 403
Hors Titre 2	3 548 462	5 446 238
Budget disponible	**16 964 049**	**18 710 003**
Titre 2	13 842 841	13 842 841
Hors Titre 2	3 121 208	4 867 162
Budget Consommé	**15 649 997**	**17 188 894**
Titre 2	13 185 872	13 185 872
Hors Titre 2	2 464 125	4 003 022

Organigramme des Directions et Services



Commission Nationale de l'Informatique et des Libertés
3, Place de Fontenoy - TSA 80715 - 75 334 PARIS CEDEX 07 / www.cnil.fr / Tél. 01 53 73 22 22 / Fax 01 53 73 22 00

Conception & réalisation graphique : LINÉAL 03 20 41 40 76 / www.lineal.fr

Impression et diffusion : Direction de l'information légale et administrative
Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr

Crédit photo : CNIL, Fotolia, istockphoto

Diffusion
Direction de l'information légale et administrative

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

ISBN : 978-2-11-145387-6
DF : 5HC45680
Prix : 15 €

Commission nationale de l'informatique et des libertés
3, Place de Fontenoy
TSA 80715
75 334 PARIS CEDEX 07
Tél. 01 53 73 22 22
Fax 01 53 73 22 00

www.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles