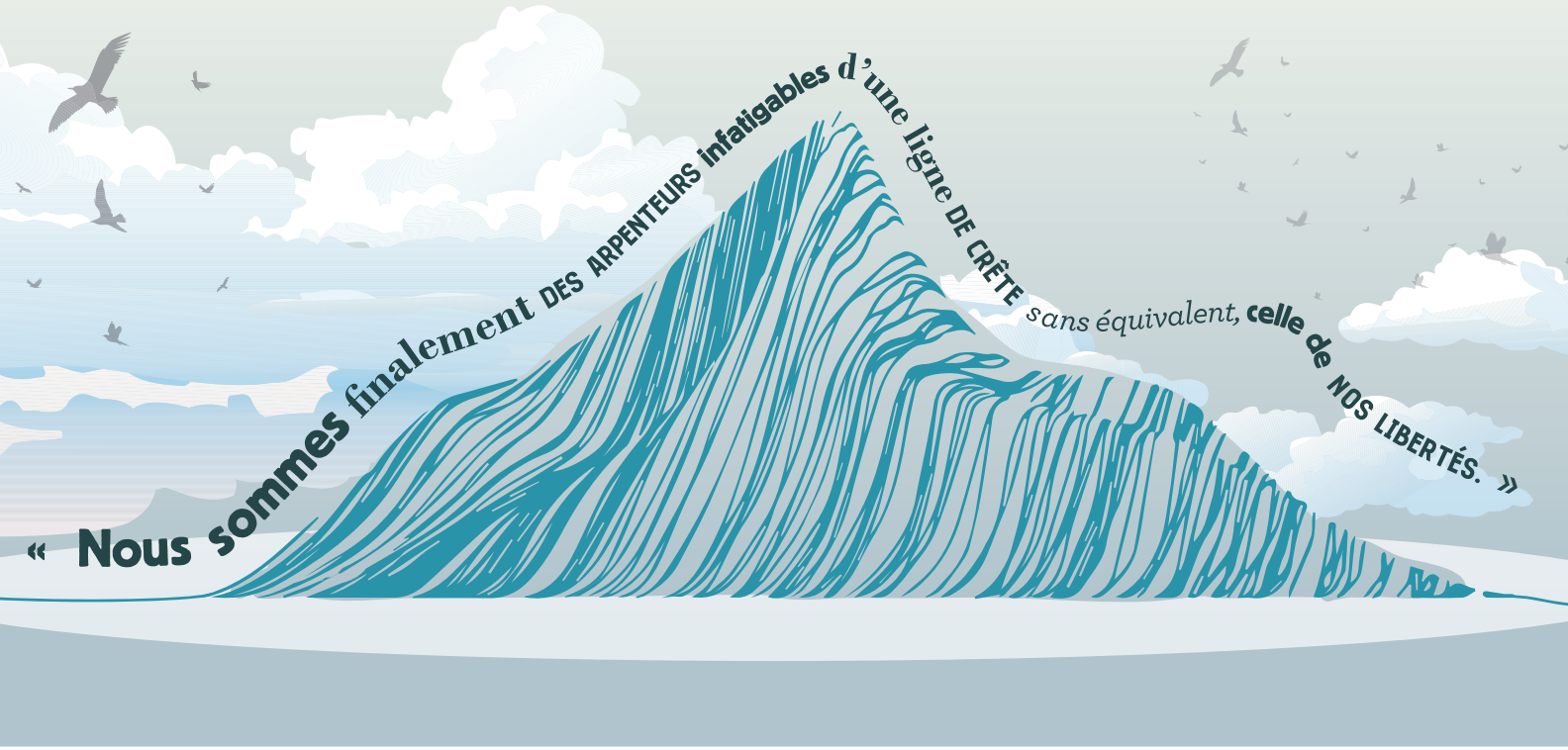
2017

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

LES CHIFFRES CLÉS 2017

CONSEILLER & RÉGLEMENTER

4 124 DÉCISIONS ET DÉLIBÉRATIONS DONT

2 964 AUTORISATIONS DE TRANSFERT DE DONNÉES HORS UE

810 AUTORISATIONS RECHERCHE MÉDICALE OU ÉVALUATION DES PRATIQUES DE SOINS

350 DÉLIBÉRATIONS DONT :

177 AVIS SUR DES PROJETS DE TEXTE

101 AUTORISATIONS

ACCOMPAGNER LA CONFORMITÉ

5 107 CIL SONT DÉSIGNÉS DANS :

18 802 ORGANISMES

98 DEMANDES DE LABELS REÇUES EN 2017

29 DEMANDES DE LABELS RGPD (labels Gouvernance ou Formation actualisés au regard du RGPD reçues)

117 DÉTENTEURS DE BCR DONT :

32 ONT DÉSIGNÉ LA CNIL COMME AUTORITÉ CHEF DE FILE

123 LABELS DÉLIVRÉS

PROTÉGER

8 360 PLAINTES

4 039 DEMANDES DE DROIT D'ACCÈS INDIRECT

(fichiers de police, de gendarmerie, de renseignement, etc.)

8 297 VÉRIFICATIONS EFFECTUÉES

+4,9 % PAR RAPPORT À 2016

INFORMER

155 000 APPELS

320 INTERVENTIONS LORS DE CONFÉRENCES, COLLOQUES, SALONS, ETC.

14 701 REQUÊTES SUR LA PLATEFORME « BESOIN D'AIDE »

+21%

93 500 FOLLOWERS SUR TWITTER

4,4 MILLIONS DE VISITES SUR CNIL.FR

+1,8 MILLION

CONTRÔLER & SANCTIONNER

341 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT :

47 CONCERNANT LA VIDÉOPROTECTION

79 MISES EN DEMEURE

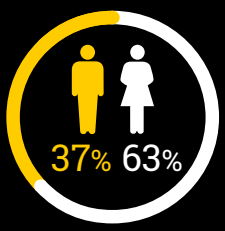
14 SANCTIONS DONT :

- **9** SANCTIONS FINANCIÈRES (6 PUBLIQUES)
- **5** AVERTISSEMENTS (2 PUBLICS)

RESSOURCES HUMAINES

BUDGET : **17 MILLIONS D'€**

198 emplois



40 ans
Âge moyen

36% DES POSTES OCCUPÉS PAR DES JURISTES

26% PAR DES ASSISTANTS

14% PAR DES INGÉNIEURS / AUDITEURS

76% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A

51% DES AGENTS TRAVAILLANT À LA CNIL SONT ARRIVÉS ENTRE 2012 ET 2017

8 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 2017

Janvier 2017

09/01
Caméras-piétons utilisées par les forces de l'ordre : l'avis de la CNIL

27/01
Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers

Avril

18/04
Création du système national des données de santé (SNDS) : quels usages avec quelles garanties ?

Juin

29/06
Windows 10 : clôture de la procédure de mise en demeure à l'encontre de Microsoft corporation

Février

17/02
Règlement européen : une nouvelle consultation sur le profilage, le consentement et la notification de violations

Mai

16/05
Facebook sanctionné pour de nombreux manquements à la loi Informatique et Libertés

Juillet

11/07
Observations de la CNIL sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme

20/07
Lancement de la vidéo du YouTuber Kevin Tran de sensibilisation aux usages responsables d'Internet et à la protection des données auprès des jeunes en partenariat avec MGEN

27/07
Hertz France : sanction pécuniaire pour violation de données personnelles

Septembre

13/09

Les données génétiques : premier titre de la nouvelle collection point CNIL

28/09

Admission post-bac (APB) : mise en demeure pour plusieurs manquements

Décembre

04/12

Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité

15/12

Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle

Novembre

22/11

RGPD : un logiciel pour réaliser son analyse d'impact sur la protection des données (PIA)

13/12

La CNIL publie son avis sur le projet de loi relatif à la protection des données personnelles

18/12

Transmission de données de Whatsapp à Facebook : mise en demeure publique pour absence de base légale

LES MEMBRES DE LA CNIL

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 a présidé le G29 (groupe des CNIL européennes) de février 2014 à février 2018.
Depuis septembre 2017, elle préside la conférence internationale des autorités de protection des données.

06

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)

02

Joëlle FARCHY

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

04

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.

05

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.

07

Loïc HERVE

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

08

Sylvie ROBERT

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

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.

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

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.

13

Marie-Hélène MITJAVILE

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

14

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.

15

Jean LESSI

Secrétaire général

16

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.

17

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.

18

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.

LES MEMBRES ÉLUS DE LA FORMATION RESTREINTE

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

COMMISSAIRE DU GOUVERNEMENT

- Nacima BELKACEM
- Adjoint, Michel TEIXEIRA

AVANT-PROPOS DE LA PRÉSIDENTE

Isabelle FALQUE-PIERROTIN
Présidente de la CNIL

© Frédérique Plas

2018 : UNE ANNÉE EXCEPTIONNELLE POUR LA PROTECTION DES DONNÉES EN FRANCE ET EN EUROPE

1978 – 2018 : LA CNIL, 40 ANS ET PLUS QUE JAMAIS DANS L'AIR DU TEMPS

2018 constitue une année exceptionnelle pour la CNIL et plus généralement pour la protection des données en France et en Europe. En janvier, la CNIL a fêté ses 40 ans, quelques mois seulement avant le vote de la nouvelle loi Informatique et Libertés et l'entrée en application du Règlement européen sur la protection des données en mai prochain. Je profite de cet anniversaire pour revenir brièvement sur cette histoire riche et singulière qui est celle de la CNIL.

Singulière parce que la CNIL est née d'un scandale, d'un trouble ressenti à l'humanité à travers le projet Safari, révélé par le Monde en 1974.
Riche parce qu'en quarante ans, au fil de ses évolutions successives, la CNIL est toujours là ; cette institution s'est imposée dans le paysage familier des Français. **Elle est devenue une « marque » reconnue en France et dans le monde.**

Les Français la connaissent bien et lui font confiance. Ils sont des dizaines de milliers à faire appel à elle chaque année. Elle a reçu plus de 8 000 plaintes en 2017 et 4 000 demandes de droit d'accès indirect.

Au plan international, c'est une référence écoutée. La CNIL a assuré la présidence du G29 pendant 4 ans jusqu' à février

2018, ce qui nous a offert un levier d'action exceptionnel pour construire l'Europe des données. La présidence de la conférence mondiale, effective depuis septembre 2017 et pour un an, constitue aussi un vecteur de diffusion de l'approche française de la protection des données et de notre vision de la régulation. Les autorités de protection des données francophones se sont fortement inspirées de la loi française et des modes d'intervention de la CNIL. L'Association francophone de protection des données qui réunit 19 de ces autorités et que la CNIL accompagne étroitement vient de fêter ses 10 ans.

La réussite de cette marque est d'abord due à la robustesse des principes inscrits dans la loi de 1978 à l'issue du travail magistral de la Commission Tricot. Dans les brouillards et les turbulences d'un univers numérique souvent difficile à déchiffrer, ces principes constituent une boussole pour garder le cap. Ces principes sont régulièrement questionnés dans leur pertinence aux évolutions. On s'interroge par exemple, aujourd'hui, avec le développement de l'intelligence artificielle en France pour savoir s'ils sont encore efficients. Je suis convaincue que oui, que leur simplicité et leur plasticité a permis à la CNIL de faire face à l'ensemble des évolutions qu'elle traversait, qu'ils constituent un soft power remarquable dans l'affrontement stratégique que nous vivons sur le numérique. Ceci se fait à partir d'un substrat intellectuel solide qui place la personne humaine au centre et que c'est cet ancrage qui caractérise l'ADN du numérique à la française.

L'autre caractéristique de la CNIL consiste à ne pas camper sur ces principes fondateurs mais, à partir de ceux-ci, de se réinventer en permanence depuis 40 ans. Comment pourrait-il en être autrement quand on parle de révolution numérique, de transformation digitale ? Les mots nous manquent pour décrire ce qui se passe. Une chose est sûre : la donnée personnelle est devenue un point nodal et un révélateur de nos sociétés, au cœur des pratiques d'exposition et de mise en scène de soi des individus, des nouveaux modèles économiques, des rapports de force géostratégiques, mais aussi des imaginaires et des utopies contemporaines.

Le troisième atout de la CNIL pour rester dans l'air du temps, c'est son collectif : agents, commissaires, tous aux parcours et origines si variés, tous fortement engagés, forment une famille bigarrée, tumultueuse par moments, mais cette diversité et ces tensions sont très utiles face aux sujets de société sur lesquels nous devons « capturer » le pacte social.

Compte tenu de ces 3 caractéristiques, d'abord protectrice des personnes face aux grands fichiers publics, la CNIL progressivement s'est faite aussi **régulatrice économique de la donnée.** Elle a fait pivoter son activité vers l'accompagnement et la mise en conformité des entreprises et des administrations. Elle a investi dans la corégulation car dans un univers complexe et évolutif comme le numérique, l'action publique doit se compléter et s'appuyer sur des outils plus souples, négociés avec les acteurs. En complément à la répression s'est alors développé le coaching numérique. Aujourd'hui, la CNIL est un régulateur complet capable de mobiliser tous les outils, du plus souple au plus contraignant.

Cette métamorphose permanente a permis à la CNIL de défendre les libertés et à promouvoir une informatique au service de chaque citoyen et de la dignité humaine. De ce fait, l'histoire de la CNIL est aussi celle de grandes évolutions et de grandes batailles, lumineuses ou douloureuses, qui ont jalonné depuis quarante ans notre histoire collective : combats et décisions sur le fichage des homosexuels, sur le programme GAMIN qui devait, au début des années 1980, automatiser la protection infantile, sur la protection du droit à l'oubli, sur le contrôle des fichiers de renseignement. **En fait, la CNIL est un entrepreneur permanent des libertés.**

N'ayons cependant pas d'illusions. La CNIL n'a pas toujours remporté ses combats. Certains ne sont pas terminés. Certaines de ses victoires seront remises en causes. Elle reste un contre-pouvoir. Un lanceur d'alerte aussi. À l'heure de la captation toujours accrue de la moindre parcelle de nos vies, à l'heure aussi d'une prise de conscience de la fragilité des systèmes d'information dont nous sommes de plus en plus dépendants, ce rôle est plus que jamais nécessaire.

« En fait, la CNIL est un entrepreneur permanent des libertés.»

« Le Règlement rééquilibre les règles du jeu. Il renforce l'individu. En un mot, il dessine un véritable modèle européen du numérique, facteur de confiance et potentiellement d'attractivité. »

ET MAINTENANT ? QUEL HORIZON POUR L'UNIVERS NUMÉRIQUE, QUEL AVENIR POUR NOS LIBERTÉS ?

Nous avons un devoir de lucidité. L'univers numérique s'est construit tout entier autour de la fluidité des usages. Des services associés intimement à nos vies quotidiennes ont favorisé une forme d'inconscience des enjeux. Nous avons, chacun individuellement, laissé une forme d'apathie nous gagner. Des forces considérables œuvrent dans le sens d'un abaissement des exigences collectives en matière de protection. Tout cela se développe sous les meilleurs prétextes. On nous explique que « tout ceci est pour le bien de l'humanité, de la démocratie, de la liberté individuelle ». La technologie se pare alors d'un habit de moine évangélisateur.

En Europe même, un discours d'abandon se fait entendre insidieusement. Il n'est pas rare d'entendre dénigrer notre modèle protecteur des libertés et des personnes. On vante l'exemple américain, qui serait plus efficient. On exalte les géants chinois du numérique. On agite l'illusion de la propriété des données comme un concept moderne permettant aux individus de gagner de l'argent et de rééquilibrer les rapports de force avec les grands acteurs de l'Internet, alors que cela ne ferait que creuser le déséquilibre et fragiliser le modèle européen nouvellement négocié qui promeut des outils novateurs comme le droit à la portabilité ou le recours collectif.

Ces discours témoignent surtout d'une incroyable volonté de ne pas voir. L'observation d'autres écosystèmes que le nôtre devrait pourtant finir de nous ouvrir les yeux sur le potentiel d'asservissement des individus que recèle le numérique.

Alors, il ne s'agit pas de condamner l'innovation ! La CNIL a de façon constante œuvré depuis plusieurs années à assouplir, simplifier, accompagner celle-ci. Il s'agit de dire que nous devons nous battre pour dessiner la société numérique non pas en singeant les autres mais sur notre terrain, celui d'une combinaison subtile des libertés et de l'innovation, de considérer qu'il s'agit là d'un savoir-faire européen spécifique qui nous est envié. Et que, par exemple, sur la question de l'intelligence artificielle où le contexte géostratégique nous ouvre des opportunités, ce modèle peut emporter l'adhésion. Le rapport présenté par la CNIL en décembre 2017 sur les enjeux éthiques de l'intelligence artificielle et des algorithmes pourra être aussi une pierre apportée à l'élaboration d'un standard européen ou mondial, puisque ce thème sera à l'agenda de la conférence mondiale des autorités de protection en octobre 2018 à Bruxelles.

La mise en œuvre du Règlement européen sera l'enjeu déterminant des prochaines années. Ce texte complexe suscite des inquiétudes compréhensibles. Mais l'essentiel est ailleurs. Le Règlement modernise notre cadre juridique tout en restant fidèle à nos principes. **Il rééquilibre les règles du jeu. Il renforce l'individu. En un mot, il dessine un véritable modèle européen du numérique, facteur de confiance et potentiellement d'attractivité.** Ce que nous serons capables de faire chez nous, en France et en Europe, sera scruté dans le monde entier. Rien n'est joué, tout va se jouer.

Il faut donc montrer que l'Europe va gagner ce pari et qu'elle est capable de faire vivre ce modèle européen.

Pour relever ce défi crucial, la CNIL va devoir, une nouvelle fois, se transformer, réinventer ses manières de faire, intégrer encore plus étroitement son action à celle de ses partenaires européens dans le cadre d'une coopération qui sera renforcée. Je suis confiante dans sa capacité à le faire et ce sera un nouvel épisode de son histoire si riche.

En somme, entre accompagnement et combats, la CNIL, aura trouvé au cours des quarante années passées le moyen de n'être jamais ni tout à fait la même, ni tout à fait une autre. Nous sommes finalement des arpenteurs infatigables d'une ligne de crête sans équivalent, celle de nos libertés.

MOT DU SECRÉTAIRE GÉNÉRAL

UNE ANNÉE DE PRÉPARATION ACTIVE DE LA TRANSITION, DOUBLÉE D'UNE TRÈS FORTE ATTENTE DES PROFESSIONNELS ET DES PARTICULIERS

Jean LESSI
Secrétaire général

L'année passée a été placée, dans la continuité de la précédente, sous le sceau de la préparation active de la transition entre deux cadres juridiques, celui issu de la loi du 6 février 1978 et de ses modifications ultérieures, et celui dessiné par le règlement général sur la protection des données qui entrera en application le 25 mai 2018. Il s'agit, on le sait, non pas d'un déplacement du curseur mais d'un changement majeur d'esprit et d'outils, dans le sens d'une plus grande responsabilisation sur le traitement des données, du développement d'une culture de l'auto-évaluation des risques et de la conformité continue, et d'une régulation à l'échelle européenne. En 2017, le collège et les services de la CNIL ont œuvré pour préparer au mieux cette transition majeure.

Le premier chantier a été la participation de la CNIL à la finalisation du nouveau cadre juridique. Associée en amont aux réflexions de la Chancellerie, la Commission a ainsi rendu le 30 novembre dernier son avis, dans des délais très courts, sur le projet de loi relatif à la protection des données, qui assure les « branchements » entre les procédures nationales devant la CNIL (en matière de conformité ou répressive) et les procédures européennes, adapte la loi de 1978 au nouveau cadre, exploite certaines des marges de manœuvre laissées aux États par le règlement et transpose la directive dite police-justice du 27 avril 2016. Ce projet de loi pose, comme il le devait, la « brique » nationale du nouvel édifice européen. Le texte devra toutefois être réécrit, à court terme, pour garantir à l'ensemble des acteurs la lisibilité et la sécurité juridique qu'appelle la complexité de la matière données personnelles. La CNIL a par ailleurs contribué activement, au niveau européen, à la préparation des lignes directrices du G29, qui garantissent une interprétation commune des grandes notions du RGPD, par exemple sur la portabilité ou l'autorité chef de file.

Enfin, la CNIL a travaillé, d'initiative, à l'explicitation des modalités de transition entre les deux cadres juridiques, sur lesquelles de nombreux acteurs s'interrogeaient, et en particulier sur la transition entre les outils de conformité forgés dans le cadre de la loi de 1978 (formalités préalables, labels) et les nouveaux outils consacrés par le RGPD (étude d'impact sur la vie privée, certification). Ce travail a donné lieu à des communications début 2018 à l'attention des professionnels concernés, dans une optique essentielle : donner la priorité à l'appropriation des nouveaux outils en capitalisant sur l'expérience acquise dans le maniement des anciens.

Le deuxième chantier principal de l'année 2017 a consisté à « donner de la chair » à ce nouveau cadre juridique, pour en favoriser l'appropriation concrète par tous. La CNIL est

« C'est en étant en mesure de s'adresser à des publics dont les besoins diffèrent qu'un service public comme la CNIL contribue à l'égalité de tous devant le RGPD. »

très attendue sur cette dimension pédagogique, comme en témoignent le nombre exceptionnellement élevé de visites sur le site internet (4,4 millions, en hausse de 40 % par rapport à 2016) ainsi que l'augmentation du nombre de demandes d'information adressées à la CNIL par voie de requête électronique (14 701 requêtes, en hausse de 21 % par rapport à 2016), la mise en place d'un nouveau serveur vocal interactif pour améliorer l'accueil et l'orientation des appels téléphoniques, ou encore l'activité soutenue de la communauté @cnil sur les réseaux sociaux. Cette tendance est cohérente avec l'attention croissante portée par les citoyens au respect de leurs droits (les plaintes ont franchi la barre des 8 000 en 2017, pour la première fois), et la prise de conscience montante par les professionnels non seulement de leurs obligations mais aussi des opportunités d'une bonne gestion des données personnelles de leurs publics qu'offre une démarche de conformité réussie.

La CNIL a ainsi développé de nouveaux outils pédagogiques et pratiques à l'attention des professionnels : mise en ligne d'une rubrique dédiée au règlement sur le site cnil.fr, ainsi que d'une page dédiée au délégué à la protection des données ; définition d'une méthode de préparation au RGPD en 6 étapes ; mise à disposition d'un modèle de registre au format prévu par le règlement ; mise en ligne d'un logiciel libre « PIA » pour accompagner les professionnels dans leurs analyses d'impact sur la protection des données ; élaboration d'un guide sur la sous-traitance ; enrichissement des foires aux questions (FAQ) disponibles, pour ne citer que quelques-unes des initiatives. Au-delà d'ailleurs du seul RGPD, la CNIL a poursuivi sa démarche consistant à mettre à disposition du public des conseils très pratiques, en se fondant sur les résultats des contrôles qu'elle conduit ou sur les préoccupations qui lui remontent par le biais des plaintes ou de demandes d'information, par exemple en fin d'année sur les jouets connectés.

La CNIL a par ailleurs cherché à adapter davantage ses contenus aux besoins spécifiques de certains publics, afin de diffuser plus largement et plus efficacement la culture de la protection des données : actions nombreuses d'éducation au numérique, vidéos en partenariat sur les réseaux sociaux, lancement des travaux d'un guide propre aux PME-TPE, réflexions sur l'approche du milieu des start-ups, etc. Ces outils seront complétés avant le 25 mai 2018 pour éclaircir des questions particulièrement fréquentes et fondamentales, avec notamment la mise à disposition de nouveaux modèles d'information ou de contenus actualisés sur les droits des personnes. C'est en étant en mesure de s'adresser par des canaux différents, avec des outils variés, à des publics dont les besoins diffèrent, qu'un service public comme la CNIL contribue à l'égalité de tous devant le RGPD.

Le troisième chantier a été la poursuite de la mise en ordre de marche de la CNIL, en interne, pour la mise en application de ce système inédit de gouvernance européenne à partir du 25 mai. Ce travail dans les coulisses, invisible pour le public, est la condition de réussite des deux précédents chantiers. La CNIL a poursuivi un effort soutenu de formation interne de ses agents, testé en situation les nouveaux outils de conformité (gestion des notifications de violation de données), engagé l'adaptation de ses systèmes d'information et participé à la mise en place du système d'information européen, ainsi que la rédaction des protocoles internes de traitement des dossiers transfrontaliers en coopération avec les autorités homologues des autres États membres.

Sur ces bases, le 25 mai ne sera pas, cela a déjà été dit, un couperet : ce sera le début d'un nouveau paradigme qui fera nécessairement l'objet d'un apprentissage collectif. La CNIL a indiqué quelle serait dans un premier temps sa politique de contrôle du respect des nouvelles obligations issues du RGPD, une politique pragmatique et axée prioritairement sur l'accompagnement. Plus généralement, l'appropriation de ces nouveautés, considérables, sera progressive, et il appartiendra à chacun, dans son rôle, de faire vivre ce nouveau cadre juridique. La CNIL, régulateur des données personnelles, poursuivra en 2018, dans chacun de ses métiers, son objectif d'élever le niveau de conformité, de protection des personnes et donc de confiance dans la société numérique.

« Le 25 mai ne sera pas un couperet mais le début d'un nouveau paradigme qui fera nécessairement l'objet d'un apprentissage collectif. »

Analyses

Lutte contre le terrorisme : extension du champ d'intervention des enquêtes administratives et allongement de la liste des traitements de données consultés

Dans le cadre des politiques de lutte contre le terrorisme, le Gouvernement a adopté plusieurs dispositifs élargissant de manière considérable le champ d'intervention des enquêtes administratives. Au-delà de l'augmentation substantielle du nombre de personnes concernées, les nouveaux dispositifs ont conduit à étendre la liste des traitements utilisés et à autoriser leur consultation automatique et simultanée. Cette multiplication des dispositifs de criblage de grande ampleur appelle une vigilance particulière et la définition de garanties fortes pour assurer le respect des droits des intéressés.

Depuis 2016, la CNIL s'est prononcée sur plusieurs nouveaux dispositifs d'enquêtes administratives. Ces nouveaux dispositifs visent à renforcer les contrôles opérés pour prévenir la réalisation d'attentats terroristes ou d'actes susceptibles de porter atteinte à la sûreté de l'État. Si le niveau de menace terroriste élevé justifie incontestablement d'adapter et de moderniser les outils de détection des risques, des garanties fortes doivent être prévues pour s'assurer que les enquêtes administratives, qui conduisent au traitement de données particulièrement sensibles sur un nombre de plus en plus important de personnes, ne portent pas d'atteintes excessives au droit au respect de la vie privée des intéressés.
À cette exigence générale, s'ajoute la nécessité de prévoir des mesures permettant d'éviter qu'une personne soit écartée de l'exercice d'un droit, de l'accès à certaines fonctions ou à certains lieux, sur le fondement de données insuffisamment vérifiées, incomplètes ou non mises à jour.

L'EXTENSION DU CHAMP D'INTERVENTION DES ENQUÊTES ADMINISTRATIVES

La réalisation d'enquêtes administratives visant à s'assurer que le comportement d'une personne n'est pas incompatible avec l'exercice de fonctions spécifiques, avec l'accès à des lieux sensibles ou avec la manipulation de produits particulièrement dangereux n'est pas nouvelle. Ces enquêtes aboutissent généralement à l'adoption d'un avis favorable ou défavorable à une décision de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation. Les dispositifs dont a été saisie la CNIL depuis l'année 2016 marquent toutefois une extension du champ d'intervervention des enquêtes administratives et présentent la particularité de permettre le renouvellement de ces enquêtes postérieurement à une décision autorisant l'exercice de mission, l'accès à des lieux ou l'utilisation de certains produits.

Des cas de recours enquêtes administratives préalables étendus

L'une des principales illustrations de l'extension du champ d'intervention des enquêtes administratives est l'adoption par le législateur d'un dispositif spécifique aux « grands événements »[1]. Ce dispositif impose aux organisateurs d'événements exposés à un risque exceptionnel de menace terroriste de demander l'avis de l'autorité administrative, qui doit être pris après enquête administrative, concernant l'accès de toute personne, à l'exception des spectateurs et des participants, à un établissement ou une installation accueillant ces grands événements. Le respect de cette procédure est requis pendant toute la durée de l'événement mais également pendant sa préparation. Comme l'a relevé la CNIL dans son avis n° 2017-047 du 9 mars 2017 relatif au projet d'acte réglementaire pris pour l'application du dispositif relatif aux grands événements, son champ d'application est particulièrement large puisque des événements peuvent être regardés comme exposés à un risque exceptionnel de menace terroriste en raison de leur ampleur, mais également en raison de leurs *« circonstances particulières »*. Dans le contexte actuel, compte tenu de l'importance de la menace terroriste, de très nombreux événements pourraient ainsi entrer dans cette catégorie. Il a d'ailleurs déjà été mis en œuvre à plusieurs reprises dans des contextes différents, notamment à l'occasion du sommet international sur le climat du 12 décembre 2017, du carnaval de Nice et de la Fête du citron à Menton.

Le dispositif relatif aux grands événements se distingue ainsi des procédures d'enquêtes administratives préalables plus anciennes concernant l'accès à des lieux dont la nature même justifie certaines précautions, comme des centrales nucléaires ou des zones militaires. En outre, des catégories de personnes très diverses peuvent être concernées par le dispositif, notamment les fournisseurs, les techniciens chargés de la mise en œuvre et de la logistique de l'événement, les personnels effectuant la maintenance ou l'entretien des établissements ou installations, les prestataires de services, les personnels exerçant une activité commerciale dans les établissements ou installations, les personnels chargés de la relation avec la presse et de la communication, les sponsors, les volontaires et bénévoles ou encore les journalistes accédant à des zones non accessibles au public. Le dispositif prévoit expressément, par ailleurs, que la qualité de résident dans la zone concernée ne fait pas obstacle à la mise en œuvre de la procédure[2].

« Dans le contexte actuel, compte tenu de l'importance de la menace terroriste, de très nombreux événements pourraient ainsi entrer dans cette catégorie. »

1 Sur ce dispositif, voir l'article L. 211-11-1 du code de la sécurité intérieure, issu de l'article 53 de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant les garanties de la procédure pénale, et les articles R. 211-32 à R. 211-34 du même code.

2 Voir l'article R. 211-33 du code de la sécurité intérieure.

L'extension du champ d'intervention des enquêtes administratives préalables peut également être illustrée par l'adoption d'un dispositif spécifique aux recrutements et affectations en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes ou d'une entreprise de transport de marchandises dangereuses[3]. Participe de la même extension, l'adoption d'un dispositif autorisant la réalisation d'enquêtes administratives visant les responsables de traitements de données à caractère personnel dont la finalité exige la collecte de données révélant la qualité de militaire et toute personne qui pourrait accéder aux données enregistrées dans ces traitements[4]. Cette tendance devrait se poursuivre en 2018, la CNIL ayant été saisie d'un projet de loi visant à autoriser la réalisation d'enquêtes administratives relatives aux demandeurs d'asile et aux personnes bénéficiant du statut de réfugié ou de la protection subsidiaire, afin de vérifier que la personne n'entre pas dans l'un des motifs d'exclusion de la protection ou de retrait tenant à l'existence de menaces graves pour l'ordre public.

D'un contrôle préalable à un contrôle potentiellement continu

Au-delà de l'augmentation exponentielle du nombre de personnes concernées par les enquêtes administratives, les nouveaux dispositifs adoptés depuis l'année 2016 présentent, pour plusieurs d'entre eux, la particularité d'autoriser le renouvellement des enquêtes administratives postérieurement à une décision autorisant l'exercice de fonctions, l'accès à des lieux ou l'utilisation de certains produits.

Cette possibilité a d'abord été prévue dans le cadre du nouveau dispositif, précédemment évoqué, relatif au transport public de personnes ou au transport de marchandises dangereuses, les enquêtes administratives pouvant être réalisées préalablement aux recrutements et affectations mais également si le comportement d'une personne occupant un emploi dans les secteurs concernés *« laisse apparaître des doutes sur la compatibilité avec l'exercice des missions pour lesquelles elle a été recrutée ou affectée »*[5].

> « Le dispositif d'enquêtes administratives préalables à des décisions administratives a été complété par des enquêtes postérieures à ces décisions. »

C'est ensuite le principal dispositif d'enquêtes administratives préalables à des décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation qui a été complété par le législateur, en 2017, pour autoriser la réalisation d'enquêtes administratives postérieurement aux décisions administratives en cause afin de s'assurer que le comportement des personnes concernées n'est pas devenu incompatible avec les missions, les accès à des lieux ou l'utilisation des produits autorisés[6]. Ce dispositif concerne un nombre particulièrement important et une grande diversité de décisions et de personnes. Sont ainsi concernés, par exemple, des personnes employées pour participer à une activité privée de surveillance et de gardiennage, les fonctionnaires et agents contractuels de la police nationale, les militaires, mais également les agents de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi) appelés à participer à la mise en œuvre des missions de la commission de protection des droits, les personnes autorisées à faire courir des lévriers, ou encore des arbitres et assesseurs de parties de pelote basque. La possibilité de procéder à de nouvelles enquêtes alors qu'une première décision administrative favorable a été prise traduit le souhait légitime de s'adapter à l'aggravation de la menace terroriste et au risque que le comportement et les intentions des personnes évoluent postérieurement à l'avis favorable dont elles ont pu faire l'objet. Cependant, la plus grande diversité des catégories de personnes susceptibles d'être concernées par les enquêtes et la possibilité de les renouveler appellent une rigueur encore plus grande dans la détermination des critères justifiant leur réalisation. Sur ce point, le dispositif spécifique à la sécurité des transports précise qu'une nouvelle enquête n'est réalisée que si le comportement de la personne laisse apparaître des doutes sur la compatibilité avec l'exercice des missions pour lesquelles elle a été recrutée ou affectée[7], alors qu'aucune précision n'encadre le renouvellement des enquêtes dans le cadre du dispositif général d'enquêtes administratives complété en 2017[8]. Cette imprécision résulte peut-être d'un choix du législateur d'autoriser le renouvellement des enquêtes même en l'absence de circonstances nouvelles, par exemple selon une fréquence prédéterminée. En toute hypothèse, la CNIL considère que la question des critères conduisant au renouvellement des enquêtes administratives doit faire l'objet de la plus grande attention de la part du Gouvernement, pour mieux prévenir le risque que la réalisation ou le renouvellement d'enquêtes administratives, qui engendre nécessairement une immixtion dans la vie privée des intéressés, ne découle en pratique de critères arbitraires ou discriminatoires.

3 Voir l'article L. 114-2 du code de la sécurité intérieure, créé par la loi du 22 mars 2016 relative à la prévention et à la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs, puis modifié par la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique

4 Ce dispositif a été justifié par les menaces terroristes particulières visant les militaires. Pour plus de précisions, voir les articles L. 4123-9-1 et R. 4123-45 à R. 4123-51 du code de la défense, ainsi que la délibération de la CNIL n° 2016-388 du 8 décembre 2016 portant avis sur un projet de décret portant application de l'article L. 4123-9-1 du code de la défense.

5 Article L. 114-2 du code de la sécurité intérieure.

6 Le dispositif évoqué est plus précisément fondé sur les dispositions de l'article L. 114-1 du code de la sécurité intérieure, modifié par la loi n° 2017-1510 loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

7 Article L. 114-2 du code de la sécurité intérieure.

8 L'article L. 114-1 du code de la sécurité intérieure précise uniquement qu' il peut être procédé à des enquêtes administratives *« en vue de s'assurer que le comportement des personnes physiques ou morales concernées n'est pas devenu incompatible avec les fonctions ou missions exercées, l'accès aux lieux ou l'utilisation des matériels ou produits au titre desquels les décisions administratives mentionnées au I ont été prises »*.

L'ADÉQUATION DE LA LISTE DES TRAITEMENTS CONSULTÉS

Outre l'extension du champ d'intervention des enquêtes administratives, les dispositifs adoptés au cours des dernières années conduisent à un allongement de la liste des traitements de données à caractère personnel susceptibles d'être consultés dans le cadre de ces enquêtes.

Les dispositifs législatifs précités, qu'il s'agisse du dispositif relatif aux grands événements, de celui spécifique à la sécurité des transports ou du dispositif plus général d'enquêtes administratives notamment liées à l'accès à certains emplois publics, prévoient ainsi que les enquêtes administratives peuvent donner lieu à la consultation de traitements automatisés relevant de l'article 26 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, étant précisé que cet article recouvre l'ensemble des traitements qui intéressent la sûreté de l'État, la défense ou la sécurité publique, ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. Sur cette base, des actes réglementaires ont défini des listes plus précises de traitements consultables[9], mais ces listes marquent une nette augmentation du nombre de fichiers utilisés dans le cadre d'enquêtes administratives et une diversification des catégories de traitements susceptibles d'être consultés, avec la possible utilisation de plusieurs traitements intéressant la sûreté de l'État.

Or, comme la CNIL l'a rappelé dans son avis n° 2017-152 du 18 mai 2017 relatif à un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé ACCRED (Automatisation de la consultation centralisée de renseignements et de données), seuls les traitements comportant des données pertinentes au regard de l'objet et des enjeux spécifiques de l'enquête administrative réalisée doivent être consultés. La définition d'une liste unique de traitements susceptibles d'être consultés est en particulier problématique dans le cadre du dispositif précédemment évoqué d'enquêtes liées à des décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, ces décisions administratives étant particulièrement nombreuses, très diverses et ne présentant pas toutes le même degré de sensibilité[10]. La Commission a dès lors pu souligner que la consultation des traitements FSPRT, GESTEREXT et CRISTINA, particulièrement sensibles et intéressant la sûreté de l'État, ne devaient pas être systématiquement consultés[11]. Ainsi, pour garantir la stricte proportionnalité du dispositif, la liste des traitements automatisés susceptibles d'être consultés doit être adaptée aux nécessités spécifiques de l'enquête administrative réalisée.

> « La CNIL a souligné que l'enregistrement des données relatives aux origines raciales ou ethniques n'était pas justifié pour le traitement ACCRED. »

Cette adaptation doit également conduire, le cas échéant, à n'autoriser la consultation que d'une partie des informations enregistrées dans un traitement. En effet, comme pour tout traitement de données à caractère personnel, seules les catégories de données adéquates, pertinentes et non excessives au regard des finalités poursuivies par les enquêtes administratives doivent pouvoir être collectées et conservées. Ainsi, la CNIL a relevé, s'agissant du fichier des personnes recherchées (FPR), qui est divisé en sous-fichiers regroupant les personnes inscrites en fonction du fondement juridique de la recherche et qui comporte des données à caractère personnel dont l'enregistrement résulte de motifs judiciaires et administratifs très divers, que la consultation effectuée devait être limitée, dans le cadre du dispositif relatif aux grands événements, aux sous-fichiers susceptibles de contenir des informations pertinentes au regard de l'objectif de prévention des atteintes à la sécurité des personnes, à la sécurité publique ou à la sureté de l'État[12]. La Commission a également souligné, concernant le traitement ACCRED que l'enregistrement de données relatives aux origines raciales ou ethniques n'était pas justifié, une telle catégorie de données ne pouvant pas être regardée comme pertinente pour l'appréciation de la dangerosité de comportements ou d'agissements de personnes. Cet avis a été suivi par le Gouvernement, qui a supprimé du projet de décret l'autorisation de la collecte de données relatives aux origines raciales ou ethniques.

9 Ainsi, par exemple, s'agissant des enquêtes administratives liées aux grands événements, l'article R. 211-32 du code de la sécurité intérieure, issu du décret n° 2017-1218 du 2 août 2017, qui définit une liste de 9 traitemens susceptibles d'être consultés.

10 Voir les articles R. 114-2 à R. 114-5 du code de la sécurité intérieure, qui fixent la liste des décisions pouvant donner lieu, en application de l'article L. 114-1 du code de la sécurité intérieure, à des enquêtes administratives .

11 Voir l'avis n° 2017-152 du 18 mai 2017 relatif à un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé ACCRED.

12 Délibération n° 2017-047 du 9 mars 2017 portant avis sur un projet de décret pris pour l'application de l'article L. 211-11-1 du code de la sécurité intérieure et relatif à l'accès aux établissements et installations accueillant des grands événements exposés, par leur ampleur ou leurs circonstances particulières, à un risque exceptionnel de menace terroriste.

LES GARANTIES DEVANT ENTOURER L'AUTOMATISATION DE LA CONSULTATION DES TRAITEMENTS

La très forte augmentation du volume d'enquêtes à prendre en charge et le renforcement des contrôles effectués à leur occasion ont conduit à confier la réalisation d'une grande partie des enquêtes administratives à deux nouveaux services à compétence nationale : le « Service national des enquêtes administratives de sécurité » (SNEAS), rattaché à la Direction générale de la police nationale[13], et le « Commandement spécialisé pour la sécurité nucléaire » (CoSSeN), rattaché à la Direction générale de la gendarmerie nationale[14]. En outre et dans une même démarche de rationalisation des enquêtes administratives, un nouvel outil a été créé pour permettre la consultation automatique et simultanée des traitements utilisés dans le cadre des enquêtes administratives prises en charge par ces deux nouveaux services à compétence nationale. Cet outil est le traitement de données à caractère personnel ACCRED précédemment évoqué, qui permet en outre de centraliser l'ensemble des informations collectées dans le cadre de l'enquête.

L'application ACCRED dispose en effet d'une interface offrant la possibilité d'intégrer une liste de personnes au sujet desquelles l'avis de l'autorité administrative est demandé. Cette application permettra, d'une part, de consulter simultanément et automatiquement de multiples traitements, notamment le FPR et le traitement des antécédents judiciaires (TAJ), et d'autre part, d'adresser automatiquement la liste des personnes faisant l'objet de la demande d'avis à la Direction générale de la sécurité intérieure (DGSI), qui met en œuvre le traitement CRISTINA, et à la direction mettant en œuvre le traitement GESTEREXT, afin qu'elles vérifient manuellement si les personnes figurent dans ces traitements. L'objet de ces consultations est alors de vérifier si les personnes au sujet desquelles l'enquête est réalisée sont inscrites dans les fichiers concernés. Les réponses à ces consultations, qui permettent de visualiser la mention « inconnu » ou « levée de doute » pour chaque fichier consulté de manière automatique et « sans observation » ou « levée de doute » pour les traitements CRISTINA et GESTEREXT, seront réceptionnées et automatiquement intégrées par le traitement ACCRED.

> « La CNIL a souligné qu'en cas de levée de doute résultant d'une consultation automatique, un complément d'information était nécessaire. »

L'automatisation des consultations et échanges d'informations réalisés dans le cadre d'enquêtes administratives présente indiscutablement des avantages et répond à la nécessité d'accélérer et de faciliter les enquêtes, compte tenu de l'extension de leur champ d'intervention. Elle soulève toutefois, dans un contexte de massification des enquêtes administratives, des risques importants au regard des droits des intéressés. En effet, la réception automatique d'un message indiquant « levée de doute » révèle uniquement qu'une personne est inscrite dans un traitement. Il est dès lors essentiel, lorsque des traitements sont consultés automatiquement avec un retour révélant uniquement l'inscription d'une personne, que les agents des services en charge de la réalisation des enquêtes disposent des moyens et de la marge d'appréciation nécessaires pour procéder à des vérifications complémentaires et analyser de manière globale la situation de l'intéressé.

La CNIL a ainsi souligné qu'en cas de levée de doute résultant d'une consultation automatique, un complément d'information était nécessaire et que ce complément ne devait pas se limiter à la consultation des informations enregistrées dans le traitement dans lequel l'intéressé est inscrit, l'avis rendu sur la compatibilité du comportement de l'agent avec l'accès à des missions, zones ou produits spécifiques ne devant pas découler de la seule inscription d'une personne dans un fichier. Une telle prudence de la Commission s'explique notamment par les risques liés à l'absence de mise à jour récente ou à l'absence de vérification des informations enregistrées dans cet unique traitement.

13 Service créé par le décret n° 2017-668 du 27 avril 2017.

14 Service créé par le décret n° 2017-588 du 20 avril 2017.

L'EXIGENCE DE FIABILISATION ET D'ACTUALISATION DES DONNÉES UTILISÉES

À titre général, la loi Informatique et Libertés impose aux responsables de traitements de ne traiter que des « données exactes, complètes et, si nécessaire, mises à jour » et d'adopter les mesures appropriées *« pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées »*[15]. Cette obligation revêt une importance particulière dans le cadre de dispositifs d'enquêtes administratives, l'utilisation de données inexactes ou non mises à jour pouvant notamment conduire à écarter de manière injustifiée une personne de l'accès à des emplois. L'absence d'actualisation des informations contenues dans le TAJ pourrait par exemple faire croire qu'une personne fait toujours l'objet d'une procédure judiciaire alors qu'elle a bénéficié, en réalité, d'une décision favorable.

S'ajoute à cette problématique générale, une problématique spécifique aux fichiers de police et de renseignements susceptibles d'être consultés dans le cadre des enquêtes administrative. La nature même de ces fichiers peut conduire à enregistrer des informations qui résultent de déclarations ou d'indices qui n'ont pas encore fait l'objet de toutes les vérifications nécessaires pour les fiabiliser. L'utilisation de ces données dans le cadre d'une enquête administrative aboutissant à un avis pouvant justifier un refus de recrutement, d'habilitation ou d'agrément milite donc également en faveur de l'adoption de garanties particulières.

Enfin, la durée de conservation relativement longue des données collectées dans le cadre des enquêtes administratives, qui est par exemple de 5 ans pour le traitement ACCRED, ne permet pas d'exclure que les données collectées à l'occasion d'une enquête administrative soient réutilisées pour des enquêtes ultérieures. Si la conservation des résultats d'enquêtes administratives en vue de la facilitation d'enquêtes administratives futures a été jugée envisageable par la Commission, il lui apparaît impératif qu'un nouvel avis ne puisse jamais être pris sur la base unique d'éléments collectés dans le cadre d'enquêtes administratives antérieures, alors même, une fois encore, que ces données pourraient ne plus être à jour. Sur ce point, le Gouvernement a indiqué que des éléments antérieurs ne constitueront jamais les informations uniques d'une enquête et que l'accès des agents aux résultats des enquêtes antérieures ne les dispensera d'aucune des consultations et vérifications à réaliser. S'il s'agit d'un engagement important, la Commission restera particulièrement vigilante sur l'effectivité des garanties prévues et l'évolution, encore en cours, des nouveaux dispositifs d'enquêtes administratives.

> « Si le niveau de menace terroriste élevé justifie incontestablement d'adapter et de moderniser les outils de détection des risques, des garanties fortes doivent être prévues. »

LES FICHIERS UTILISÉS :

Les fichiers susceptibles d'être consultés dans le cadre d'enquêtes administratives réalisées par des services relevant du ministère de l'intérieur sont principalement :

- le traitement d'antécédents judiciaires (TAJ), prévu aux articles L. 230-6 et R. 40-29 du code de procédure pénale ;
- le fichier des personnes recherchées (FPR), prévu par le décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées ;
- le traitement « enquêtes administratives liées à la sécurité publique » (EASP), prévu aux articles R. 236-1 et suivants du code de la sécurité intérieure ;
- le traitement « prévention des atteintes à la sécurité publique » (PASP), prévu aux articles R. 236-11 et suivants du code de la sécurité intérieure ;
- le traitement « Gestion de l'information et prévention des atteintes à la sécurité publique (GIPASP), prévu à l'article R. 236-21 et suivants du code de la sécurité intérieure ;
- le fichier des objets et véhicules signalés (FOVeS), dont la création, suite à son expérimentation, est prévue par un projet d'acte réglementaire examiné par la Commission ce même jour ;
- les fichiers FSPRT, CRISTINA et GESTEREXT, qui font l'objet d'une dispense de publication de l'acte réglementaire qui les autorise en application de l'article 26-III de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et au décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

15 Article 6-4° de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Numérisation de l'Éducation nationale :

la CNIL appelle à l'adoption d'un socle de principes généraux protecteurs des données personnelles, adaptés aux spécificités du secteur

Depuis plusieurs années, le secteur de l'Éducation nationale est marqué par une utilisation croissante du numérique à des fins administratives ou pédagogiques. Malgré les efforts du ministère de l'Éducation nationale pour développer différents cadres protecteurs des données personnelles des élèves et des enseignants, de nombreux établissements scolaires et écoles recourent à des ressources numériques ne respectant aucun de ces cadres. C'est pourquoi la CNIL s'implique largement dans cette transition numérique afin de rappeler les principes régissant la protection des données personnelles et les bonnes pratiques en la matière.

LA TRANSITION NUMÉRIQUE DU MINISTÈRE DE L'ÉDUCATION NATIONALE

Le secteur de l'Éducation est, depuis plusieurs années, marqué par une véritable transition numérique. La première mutation en résultant concerne le développement, par le ministère de l'Éducation nationale lui-même, d'applications numériques à destination des élèves, de leurs familles et des personnels. Ce mouvement n'échappe pas à la CNIL qui est notamment chargée de veiller à la conformité de ces traitements aux principes de la loi Informatique et Libertés.

Le livret scolaire unique (LSUN)

À titre d'illustration, l'année 2017 a été marquée par la création d'une application nationale de suivi de la scolarité, dans les écoles élémentaires et les établissements du second degré, dénommée **livret scolaire unique numérique (LSUN)**[16]. Le LSUN, qui concerne les élèves du CP à la troisième, contient le suivi des acquis des compétences ainsi que les appréciations des enseignants. Il est en outre assorti d'un service en ligne (téléservice) facultatif à l'attention des élèves et de leurs responsables légaux qui pourront ainsi accéder en ligne au livret scolaire.

L'examen du projet de texte créant le LSUN a permis à la CNIL de rappeler au ministère que l'information des personnes concernées par ce livret scolaire, prévue par la loi Informatique et Libertés, ne devait pas seulement être fournie aux utilisateurs du téléservice mais à tous les usagers concernés par le livret scolaire[17].

L'application Esculape pour la médecine scolaire

En 2017, le ministère a également mis en place l'application « Esculape », permettant aux médecins scolaires de dématérialiser les dossiers médicaux des élèves. Les dossiers médicaux des élèves étaient en effet largement gérés par les médecins scolaires sur support papier. L'utilisation du seul support papier ne répondant plus aux besoins de l'activité des médecins scolaires, le ministère a créé un nouvel outil dont les fonctionnalités doivent permettre l'amélioration de l'organisation du travail des médecins et le suivi des élèves, notamment en cas de changement de secteur d'intervention du médecin ou de changement d'établissement de l'élève.

Dans la mesure où « Esculape » est mis à disposition de près de 2 000 médecins scolaires, qu'il concerne un grand nombre de personnes, principalement mineures (élèves des premier et second degrés d'enseignement public et privé sous contrat), et qu'il contient des données de santé, données faisant l'objet d'une protection particulière, le ministère a associé la CNIL au déploiement de ce projet. Les échanges entre la CNIL et le ministère ont, par exemple, permis d'ajuster la durée de conservation des données et de mettre en place des mesures de sécurité adaptées aux risques.

Les services fournis par des tiers

En parallèle du développement de ces applications plutôt destinées à une gestion administrative, le ministère de l'Éducation nationale a également opéré sa transition numérique en ce qui concerne les services pédagogiques offerts aux élèves. Il s'est ainsi, depuis plusieurs années, engagé dans une **ouverture encadrée de l'utilisation de services fournis par des tiers** tels que les éditeurs scolaires ou les collectivités territoriales avec les espaces numériques de travail (ENT).

L'objectif est ainsi de permettre aux fournisseurs de ces services d'intégrer l'écosystème de l'Éducation nationale tout en respectant certains référentiels nationaux. Cette stratégie à plusieurs niveaux doit permettre d'éviter l'effet dissuasif de certains cadres jugés trop contraints.

Là encore la CNIL exerce pleinement son rôle de conseil et d'accompagnement. Elle a en effet eu l'occasion d'examiner certains de ces cadres développés par le ministère pour promouvoir des solutions numériques respectueuses de la protection des données personnelles.

> « Le secteur de l'Éducation nationale est marqué par la grande diversité des offres de services numériques qui bouleversent les pratiques traditionnelles. »

16 Arrêté du 24 octobre 2017 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Livret scolaire unique numérique » LSUN.

17 Délibération n° 2017-159 du 18 mai 2017.

La charte de confiance des services numériques

En 2017, le ministère de l'Éducation nationale a sollicité l'avis de la CNIL sur un projet de charte de confiance des services numériques pour l'Éducation. Cette charte devait rappeler les principales dispositions du code de l'Éducation, du code des marchés publics et de la loi Informatique et Libertés applicables à ces services. Elle devait aussi prévoir des stipulations allant au-delà de ces dispositions légales afin que les conditions d'utilisation des services numériques soient adaptées aux besoins du secteur de l'Éducation, notamment en termes de protection des données personnelles.

La CNIL a estimé intéressante l'initiative prise par le ministère d'inciter les fournisseurs de ces services à s'engager dans une offre de services numériques respectueux des droits des personnes. Elle a toutefois regretté l'absence de caractère contraignant de cet instrument. À ce jour, la charte de confiance en question n'a pas été adoptée.

Les espaces numériques de travail (ENT)

L'année 2017 a également été marquée par la refonte de l'encadrement des espaces numériques de travail (ENT). En effet, les pratiques ayant évolué depuis 2006, le cadre développé à ce moment-là par le ministère ne correspondait plus aux besoins des acteurs concernés.

Les ENT permettent à leurs utilisateurs, en renseignant une fois leurs « identifiants », d'accéder en ligne à de nombreux services ou ressources liés à la vie scolaire et à la pédagogie : cahier de texte, outils de vie scolaire (gestion des absences, des notes, etc.), service de paiement des frais d'inscription dans l'enseignement supérieur, services collaboratifs à usage des enseignants, mais également accès à des ressources pédagogiques telles que des banques de données, des ouvrages de référence, des dictionnaires et des manuels numériques. Ces dispositifs s'inscrivent dans un projet généralement développé au niveau académique et associant de nombreux acteurs tels que les collectivités territoriales. Afin d'assurer le déploiement des ENT dans un cadre de confiance devant notamment garantir la sécurité des données traitées, le ministère a imposé le respect d'un schéma directeur des espaces numériques de travail (SDET).

L'avis de la CNIL sur ce projet de refonte a permis que plusieurs précisions utiles soient mentionnées dans l'arrêté modifiant le cadre relatif aux ENT. Par exemple:

- l'identité du responsable de traitement dans les écoles (le DASEN) est désormais expressément mentionnée,
- il est prévu que le lieu de naissance de l'élève ne soit enregistré que dans l'hypothèse où celui-ci ne disposerait pas de numéro identifiant national élève (INE) ou que ce numéro serait en conflit avec un autre,
- est fixée une durée maximale de conservation des données dans l'enseignement supérieur à l'issue de laquelle, en l'absence de retour de l'intéressé, le compte ENT doit être supprimé.

« La CNIL appelle à l'adoption, par le ministère, d'un socle commun de principes généraux protecteurs des données personnelles, adaptés aux spécificités du secteur de l'Éducation nationale, à respecter quel que soit le mode d'accès aux ressources pédagogiques. »

Le gestionnaire d'accès aux ressources (GAR)

La CNIL a en outre été saisie du « gestionnaire d'accès aux ressources » dit GAR, développé par le ministère, afin de permettre l'accès, dans un cadre respectueux des règles de protection des données à caractère personnel, à des ressources pédagogiques numériques éditées par des fournisseurs privés. Ce dispositif, qui s'inscrit dans la logique du règlement européen sur la protection des données personnelles (RGPD), est assez novateur puisqu'il s'appuie sur :

- une équipe de personnels du ministère chargée en amont d'apprécier la proportionnalité des données personnelles sollicitées par un fournisseur de ressources au regard d'une ressource numérique précise,
- un portail internet à destination des fournisseurs de ressources,
- une seule et même interface de mise en relation permettant aux utilisateurs de disposer, de manière transparente, de nombreuses ressources,
- une solution technique qui agit comme un « filtre » pour ne transmettre, aux fournisseurs de ressources, que les données personnelles nécessaires,
- un contrat d'adhésion et des référentiels techniques et de sécurité imposant aux fournisseurs de ressources de respecter des principes ou obligations tels que, par exemple, la non réutilisation commerciale des données personnelles des élèves et des enseignants ou le fait pour le fournisseur de permettre la récupération aisée par les utilisateurs de leurs données.

Dans son avis sur le GAR, la CNIL a estimé qu'au-delà des garanties offertes par ce dispositif spécifique, **la situation générale de l'utilisation de services numériques dans l'Éducation nationale demeurait insatisfaisante du point de vue de la protection des données personnelles**. En effet, le caractère uniquement facultatif du recours au GAR permet que les usagers et personnels puissent accéder à des ressources et services numériques ne respectant ni le cadre de confiance imposé par le GAR, ni aucun autre cadre prévu par le ministère pour protéger les données à caractère personnel traitées dans le cadre du service public de l'Éducation, amoindrissant ainsi l'effet utile des différents cadres établis par le ministère.

LES ENJEUX SOULEVÉS PAR LA TRANSITION NUMÉRIQUE DU SECTEUR DE L'ÉDUCATION DU POINT DE VUE DE LA PROTECTION DES DONNÉES

Tout d'abord, le fait que les données scolaires concernent essentiellement des personnes mineures et qu'elles contiennent des appréciations, des évaluations sur la « valeur », les compétences, les « performances » et même le comportement des élèves leur confère un caractère hautement personnel qui requiert dès lors une approche adaptée. Le règlement européen sur la protection des données personnelles, qui renforce les droits des personnes et porte une attention particulière aux mineurs, devrait permettre d'affermir cette démarche.

En outre, le secteur de l'Éducation nationale est marqué par la grande diversité des offres de services numériques qui bouleversent les pratiques traditionnelles : déploiement d'équipements informatiques mobiles facilitant l'accès aux ressources en ligne, services de stockage dans le *cloud*, outils collaboratifs avancés, réseaux sociaux pédagogiques, applications pour faciliter la communication entre les enseignants et les familles.

Bon nombre de ces usages du numérique ne répondent à aucun des cadres proposés par le ministère mais séduisent néanmoins par leur efficacité, leur simplicité d'utilisation voire même parfois par leur gratuité. Sans remettre en cause l'utilité de ces services numériques, la CNIL relève que leur utilisation est susceptible de soulever des interrogations quant au respect des principes régissant la protection des données personnelles.

Cette situation a également suscité de la part d'associations de parents d'élèves comme de syndicats d'enseignants, plusieurs saisines auprès de la CNIL. Ces organisations s'inquiètent notamment des conditions dans lesquelles certains acteurs clés du numérique lorsqu'ils offrent leurs services auprès du monde éducatif sont susceptibles d'utiliser, pour leur propre compte, les données scolaires.

Le recours à des solutions numériques « grand public », dont les conditions générales d'utilisation (CGU) ne prennent pas en compte les spécificités d'une utilisation à des fins administratives ou pédagogiques, dans le cadre du service public de l'Éducation, est fréquent alors même que leurs CGU n'interdisent généralement pas la publicité, la réutilisation à des fins commerciales des données personnelles ou encore le profilage.

Même les solutions numériques dédiées au secteur de l'Éducation, avec des conditions d'utilisation spécifiques, ne sont pas toujours conçues selon le principe du *privacy by design* destiné à garantir que la protection de la vie privée est intégrée dès leur conception. Il est ainsi souvent difficile pour le responsable de traitement de savoir où exactement sont hébergées les données personnelles des élèves et des personnels dont il a la charge, de s'assurer que celles-ci ne sont pas conservées indéfiniment ou qu'elles font l'objet de mesure de sécurité satisfaisantes.

C'est pourquoi la CNIL estime qu'il est essentiel que le travail amorcé par le ministère pour encadrer de tels usages soit poursuivi et approfondi afin d'assurer d'une protection effective des données personnelles des élèves. Elle appelle ainsi à l'adoption, par le ministère, d'un socle commun de principes généraux protecteurs des données personnelles, adaptés aux spécificités du secteur de l'Éducation nationale, à respecter quel que soit le mode d'accès aux ressources pédagogiques.

Ces principes pourraient notamment inclure des exigences allant au-delà du simple rappel des obligations légales telles que notamment l'interdiction de réutiliser, à des fins commerciales, les données des élèves, l'hébergement des données personnelles au sein de l'Union européenne, ou encore le fait de permettre la récupération aisée des données personnelles des élèves et des personnels.

INFOSPLUS

Learning analytics ou analyse de l'apprentissage

- Il s'agit de l'analyse des traces numériques d'apprentissage afin de mieux comprendre et optimiser celui-ci.
- Ces analyses portent aussi bien sur les traces d'utilisation des services telles que le nombre de clics par lien dans un e-module donné, la fréquence et le temps d'utilisation d'un service que sur les performances des personnes concernées, les traces d'interactions, ou encore des données sociodémographiques telles que l'âge, le sexe, le niveau d'Éducation.
- L'analyse de ces données doit notamment permettre d'améliorer les formations, en personnalisant l'apprentissage.

Enfin, le secteur de l'Éducation nationale est également marqué par le fait que **le développement du numérique peut conduire à la constitution de gisements de données massifs et par là même à des possibilités infinies d'exploitation de celles-ci notamment à des fins de meilleure connaissance des élèves ou d'amélioration des pratiques pédagogiques.**

Il en va ainsi des *learning analytics* ou « analyses de l'apprentissage ». S'ils peuvent être légitimes dans leur principe, de tels usages requièrent une certaine prudence au regard des modèles prédictifs de comportements qu'ils peuvent être amenés à bâtir. Les *learning analytics* peuvent en effet être utilisés pour « prédire » des situations d'échecs, des abandons dans certaines formations en ligne, pour détecter des élèves à risque, pour les affecter dans une filière « adaptée à leur profil ». Or, comme l'a souligné la CNIL dans son rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, **les *learning analytics* ne sont pas sans soulever la question de l'enfermement algorithmique alors que de telles analyses des données d'apprentissage ne devraient pas avoir pour objet ni pour effet un déterminisme sur les parcours scolaires les élèves**.

Pour toutes ces raisons, la CNIL considère qu'il est indispensable de définir des règles claires pour de tels usages des données des élèves.
Ainsi, un travail doit être mené pour :

- **déterminer** les finalités pouvant légitimement être poursuivies au titre de ces analyses ;
- **délimiter** les conséquences que de telles analyses peuvent emporter sur les personnes concernées ;
- **définir** les mesures concrètes permettant de s'assurer du respect des deux points précédents ;
- **garantir** la nécessaire transparence sur une telle utilisation des données personnelles des élèves.

Compte tenu de ces différents enjeux, la protection des données personnelles des élèves demeure une priorité pour la CNIL et l'arrivée du règlement européen permettra de renforcer cette protection.

FOCUS

Mise en demeure d'APB (Admission post-bac)

Le rôle de la CNIL ne se limite pas à un contrôle a priori de la conformité du projet de traitement à la loi Informatique et Libertés. Elle veille aussi au respect a posteriori de ces principes destinés à protéger la vie privée des personnes.

En mars 2017, elle a ainsi contrôlé le traitement admission post-bac (APB) permettant l'affectation des lycéens à une formation dans l'enseignement supérieur. Les constatations opérées lors de ces contrôles ont révélé plusieurs manquements aux règles gouvernant la protection des données personnelles, conduisant ainsi la Présidente de la CNIL à mettre en demeure publiquement le ministère de l'enseignement supérieur, de la recherche et de l'innovation, le 28 septembre 2017.

Outre une information insuffisante des personnes concernées, il a été constaté que, s'agissant des formations non sélectives, un algorithme déterminait automatiquement, sans intervention humaine, les propositions d'affectation faites aux candidats, à partir des trois critères prévus par le code de l'Éducation : le domicile du candidat, sa situation de famille et l'ordre de préférence des vœux qu'il a formulés. Or, l'article 10 de la loi Informatique et Libertés interdit une telle prise de décision purement automatisée.

La procédure de droit d'accès ne permettait pas aux personnes d'obtenir des informations précises relatives à l'algorithme et à son fonctionnement, notamment la logique qui sous-tend le traitement APB ou le score obtenu par le candidat. En effet, l'article 39 de la loi Informatique et Libertés dispose que les personnes qui exercent leur droit d'accès doivent pouvoir obtenir « Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé ».

La CNIL n'a pas remis en cause le principe même de l'utilisation des algorithmes dans la prise de décision, notamment par les administrations. Cependant elle a rappelé les principes prévus par la loi : compte tenu des enjeux éthiques que soulèvent les algorithmes utilisés pour prendre une décision produisant des effets juridiques à l'égard d'une personne, leur utilisation des algorithmes ne peut exclure toute intervention humaine et doit s'accompagner d'une information transparente des personnes.

La réponse du ministère à cette mise en demeure a permis à la Présidente de la CNIL de considérer que les divers manquements avaient cessé et de clôturer la mise en demeure. Le ministère a, en effet, informé la Présidente de la fermeture de la plateforme APB et de la mise en place d'un nouveau dispositif dénommé « Parcoursup ».

Parallèlement la Commission a été saisie, pour avis, du projet d'arrêté autorisant la mise en œuvre de la première phase du nouveau traitement « Parcoursup », dédiée à la collecte des vœux des candidats pour l'entrée dans une formation de l'enseignement supérieur. La Commission sera en outre prochainement saisie pour avis sur le projet d'arrêté portant autorisation du dispositif permettant l'affectation des étudiants, sur la base des vœux ainsi recueillis.

La proposition de Règlement *ePrivacy*

Tout comme la directive 95/46/CE qu'il remplace, le règlement général sur la protection des données (RGPD) s'accompagne de textes dits « spéciaux » (ou *lex specialis*) qui viennent préciser l'application de la règlementation dans certains domaines spécifiques. C'est le cas notamment de la directive 2002/58/CE dite « *ePrivacy* » qui encadre les traitements réalisés dans le contexte des communications électroniques. Modifiée en 2009, cette directive va elle aussi faire l'objet d'une refonte et devenir un règlement à moyen terme. Cette évolution s'inscrit dans le cadre d'une stratégie plus globale, celle du marché unique numérique portée par la Commission européenne depuis mai 2015, qui donnera également naissance à un Code des communications électroniques européen (CCEE) réunissant les autres directives dites « Paquet Telecom »[1].

Le futur règlement *ePrivacy* sera intégré directement dans le droit des États membres, selon des conditions d'application identiques au RGPD. Il déclinera, dans le domaine des communications électroniques, les principes permettant de protéger le droit fondamental de toute personne au respect de sa vie privée et familiale, de son domicile et de ses communications, au sein de l'Union européenne.

À ce titre, le futur règlement adapte les principes déclinés par le RGPD au caractère particulièrement sensible des données de communication électroniques, lesquelles peuvent révéler des informations intimes sur les utilisateurs. Il peut non seulement recouvrir « les numéros appelés, les sites web visités, le lieu, la date, l'heure et la durée des appels passés par un individu, etc., qui permettent de tirer des conclusions précises sur la vie privée des personnes intervenant dans la communication électronique, comme leurs rapports sociaux, leurs habitudes et activités au quotidien, leurs intérêts, leurs goûts, etc. » mais également leurs « expériences personnelles et émotions jusqu'à leurs problèmes de santé, préférences sexuelles et opinions politiques ».

En tant que texte spécial, la règlementation *ePrivacy* n'a pas vocation à recopier le RGPD, mais à tenir compte du principe de confidentialité des communications électroniques pour préciser les conditions d'application de ce dernier. Le futur règlement *ePrivacy*, tout comme la directive *ePrivacy* aujourd'hui en vigueur, précise de ce fait les cas dans lesquels les traitements effectués dans ce domaine sont proportionnés ou nécessitent une base légale « forte ». À ce titre, la proposition de la Commission européenne, dans le prolongement de la directive de 2002, positionne le consentement au centre des préoccupations.

Par ailleurs, la proposition de texte permet d'égaliser les situations concurrentielles entre, d'une part, les fournisseurs d'accès internet principalement visés par la règlementation actuelle et, d'autre part, des acteurs dits « Over the top » proposant des services de contournement ; il s'agit des professionnels qui utilisent le réseau pour proposer des services équivalents du point de vue fonctionnel à ceux proposés par les opérateurs de télécommunications. Par exemple, un acteur qui permet aujourd'hui à deux utilisateurs de communiquer via un protocole de voix sur IP (ou VoIP) ou d'échanger dans le module de discussions au sein d'une application, d'envoyer et de recevoir des courriels, n'est pas couvert par la règlementation. Il le sera dans le cadre du futur texte, si la version actuellement discutée est maintenue. Du point de vue de l'utilisateur cette fois, cette évolution apparaît comme logique. En effet, le fait de passer classiquement un appel téléphonique ou d'appeler une personne via une application dédiée et installée sur un terminal (ordinateur, tablette, etc.) doit présenter les mêmes garanties en termes de confidentialité.

De même, et là où la directive « *ePrivacy* » laissait le soin aux législateurs nationaux de désigner les autorités de contrôle chargées de s'assurer de l'application de ses règles, la proposition de règlement affirme la compétence quasiment exclusive des autorités de protection des données en matière de protection de la vie privée dans les communications électroniques. Une coopération avec les autorités de régulation nationales (ARCEPs européennes) est toutefois prévue en tant que de besoin, notamment en cas de doute sur la qualification des acteurs concernés. La CNIL voit donc son rôle d'accompagnateur de la mise en conformité dans un écosystème en perpétuelle mutation conforté.

L'importance du futur Comité européen à la protection des données (l'actuel G29) est également accentuée puisqu'il pourra émettre des avis auprès de la Commission européenne sur d'éventuelles modifications et évolutions du règlement « *ePrivacy* » et établir, de sa propre initiative, des guides de bonnes pratiques ou des recommandations. Il constituera dès lors, comme le prévoit déjà le RGPD, le carrefour d'un circuit court et harmonisé de régulation au bénéfice des entreprises.

Enfin, la proposition de la Commission, tout comme la directive de 2002, encadre de nombreuses pratiques, telles que la prospection commerciale par voie électronique par exemple et dont les règles n'évolueront vraisemblablement pas.

De manière générale, il faut retenir que les deux grands volets du futur règlement *ePrivacy* s'inscrivent dans la voie tracée par l'actuelle directive. Il priorise par conséquent le principe de confidentialité des communications électroniques et le renforcement de la protection des terminaux.

« Le règlement *ePrivacy* priorise le principe de confidentialité des communications électroniques et renforce la protection des terminaux. »

1 Voir en ce sens « Le cadre actuel et le nouveau paquet télécom » sur le site de l'ARCEP.

INFOSPLUS

Agenda

La proposition de règlement *ePrivacy* a été publiée par la Commission européenne le 10 janvier 2017 et pourrait être adoptée en fin d'année 2018, sous réserve que les discussions entre la Commission, le Parlement européen et le Conseil de l'Union européenne aboutissent avant cette échéance.

UN OBJECTIF CLÉ : PROTÉGER LES COMMUNICATIONS ÉLECTRONIQUES

Dans la lignée de ce que prévoit l'actuelle directive de 2002, le principe reste la confidentialité des communications électroniques opposables aux seuls fournisseurs de services de communications électroniques. En clair, il s'agit des acteurs qui assurent l'acheminement de ces communications, à savoir les opérateurs de télécommunication et les fournisseurs de services équivalents (OTT ou services par contournement évoqués plus haut). Pour simplifier l'approche en la matière, la Commission européenne distingue deux notions, à savoir le contenu des communications électroniques à proprement parler et les métadonnées associées à ces communications.

Le principe de confidentialité s'entend ici de manière stricte, c'est-à-dire qu'il est interdit de traiter les données de communications électroniques, sans le consentement des utilisateurs et sauf à bénéficier de l'une des exceptions prévues dans le texte. Dans cette logique, les données de communications électroniques doivent être anonymisées ou effacées par les opérateurs une fois que ces derniers en ont assuré l'acheminement. Ces deux principes, déjà présents dans la directive de 2002 modifiée en 2009, sont reproduits dans la proposition de règlement.

> « La réutilisation des données pour d'autres fins que la fourniture du service attendu par l'utilisateur nécessitera son consentement. »

Dans le même temps, la proposition vise à favoriser la compétitivité des entreprises européennes. Comme le rappelle l'exposé des motifs de ce texte, il ne doit pas constituer un frein à l'innovation en empêchant les entreprises de développer de nouveaux produits et services. C'est pourquoi le législateur prévoit, pour chaque catégorie de données précitées, des cas pour lesquels elles peuvent être traitées :

- pour les communications électroniques, le traitement est possible lorsque cela est techniquement nécessaire au bon fonctionnement du réseau ou pour assurer sa sécurité ;

- pour les métadonnées, le traitement est possible :
  - pour assurer l'accès à Internet et le service universel (en bref et assez logiquement, lorsque le traitement est nécessaire pour assurer la communication) ;
  - pour calculer les paiements d'interconnexions (entre deux opérateurs) ou pour permettre la facturation des services utilisés par la personne et, partant, lutter contre la fraude « à l'usage et à l'abonnement » ;
  - lorsque l'utilisateur a donné son consentement *« pour un ou plusieurs objectifs précis, dont la fourniture de services spécifiques à son endroit, à condition que le traitement d'informations anonymisées ne permette pas d'atteindre les dits objectifs »* en priorisant les procédés d'anonymisation des données ou le consentement. Il s'agit ici, compte tenu de la grande sensibilité que peuvent revêtir les métadonnées, de prioriser les procédés d'anonymisation et de ne faire appel au consentement de l'utilisateur qu'en dernier recours.

- et enfin, pour le contenu des communications sur la base du consentement des utilisateurs et dans certains cas, après consultation de la CNIL.

Attention, cela ne signifie pas que les messages des utilisateurs de webmails vont subitement être effacés de la messagerie. La règlementation prévoit en effet expressément que les données de contenu peuvent être stockées par les utilisateurs finaux ou par un tiers mandaté par eux pour assurer le stockage ou tout autre traitement (par exemple, le fournisseur d'une messagerie électronique).

En dehors de ces exceptions qui recouvrent assez logiquement ce qu'un utilisateur pourrait attendre lorsqu'il se connecte à un réseau, la réutilisation des données pour d'autres fins que la fourniture du service attendu par l'utilisateur nécessitera son consentement.

À RETENIR

Contenu des communications et métadonnées

Si un utilisateur envoie un courriel à l'un de ses contacts, le contenu de l'échange (le texte rédigé) est qualifié de contenu. Les données associées à cet échange et qui le « décrivent », telles que son poids, l'horodatage de l'envoi et de la réception, éventuellement le serveur depuis lequel elles sont envoyées ou reçues, le type de communication, sa durée, etc., sont qualifiées de métadonnées.

PROTÉGER LES INFORMATIONS STOCKÉES OU ÉMISES PAR LES APPAREILS

Tout comme l'actuelle directive *ePrivacy*, la proposition de règlement prévoit comme principe le recueil du consentement des utilisateurs avant toute utilisation de traceur au sein des terminaux (téléphone, tablette, ordinateur, etc.). La notion de traceur s'entend ici au sens très large puisqu'il s'agit de toutes techniques permettant de suivre les utilisateurs : cookies, empreintes numériques (fingerprinting), pixels invisibles (web bugs), ce que la CNIL avait d'ores et déjà intégré dans le périmètre d'application de sa recommandation de décembre 2013 relative aux cookies et autres traceurs.

La proposition de la Commission, si elle peut être ajustéée sur certains aspects, prévoit un cadre global d'encadrement des traceurs très proche de celui actuellement en vigueur. Le consentement reste l'élément central, assorti d'exceptions classiques, à l'exemple des traceurs nécessaires pour accéder d'un point de vue technique aux sites web et de nouvelles exceptions telles que la possibilité pour ces mêmes sites d'effectuer des traitements de mesure d'audience, exception que la CNIL avait reconnue comme nécessaire dès 2013, dans ses recommandations.

La principale nouveauté de la proposition de règlement porte sur les modalités d'expression du consentement, signe de prise en compte des difficultés d'application de la règlementation actuelle. En effet, selon la Commission européenne, la multiplication des bandeaux d'information sur les sites web et l'absence réelle de choix a nui à l'objectif initialement fixé, à savoir permettre le recueil du consentement par site et par finalité, après information de l'internaute. Plus précisément, la Commission estime que *« la mise en œuvre de la directive « vie privée et communications électroniques » ne s'est pas avérée efficace pour ce qui est de responsabiliser l'utilisateur final. Aussi, pour atteindre le but recherché, est-il nécessaire d'appliquer le principe en centralisant le consentement dans des logiciels et en donnant aux utilisateurs des informations sur leurs paramètres de confidentialité. ».*

La consultation publique menée par la Commission européenne préalablement à la rédaction de la proposition de règlement permet de conforter cette idée. En effet, sur le thème *« solutions proposées au problème du consentement pour les cookies », « 81,2 % des particuliers et 63 % des pouvoirs publics soutiennent la solution consistant à imposer aux fabricants d'équipements terminaux l'obligation de commercialiser des produits dotés de paramètres de confidentialité activés par défaut, tandis que 58,3 % des entreprises sont favorables à la solution de l'autorégulation ou de la corégulation. ».*

Le G29, dans son avis 03/2016 relatif à l'évaluation et à la révision de la directive 2002/58 relevait également, en juillet 2016, la nécessité de changer d'approche en ce qui concerne l'expression des choix de l'utilisateur en impliquant les éditeurs de navigateurs ou de systèmes d'exploitation pour recueillir, via le paramétrage du logiciel, le consentement des personnes.

En pratique, le G29 et la CNIL ont souligné la nécessité d'intégrer dans le navigateur la possibilité d'émettre un signal indiquant aux sites consultés, le choix exprimé par l'utilisateur[2]. Ce signal pourrait s'appuyer sur le protocole *Do Not Track* (ou DNT) recommandé notamment par le G29.

INFOSPLUS

L'étude Eurobaromètre menée en amont de la proposition de règlement *ePrivaScy :*

- Pour 78 % des personnes interrogées, il est très important qu'on ne puisse accéder aux informations à caractère personnel contenues dans leur ordinateur, leur smartphone ou leur tablette qu'avec leur permission ;
- 72 % considèrent comme très important que la confidentialité de leurs courriels et de leur messagerie instantanée en ligne soit garantie ;
- 89 % conviennent, comme il a été suggéré, que les paramètres par défaut de leur navigateur devraient empêcher le partage de leurs informations.

Le rapport complet (en anglais) est disponible à l'adresse :
https://ec.europa.eu/digital-single-market/en/news/eurobarometer-*eprivacy*

2 *"When consent is the applicable legal basis, users must be provided with truly easy (user friendly) means to provide and revoke consent. The Working Party recommends rephrasing the requirements in the current Recital 66 of Directive 2009/136/EC. Instead of relying on website operators to obtain consent on behalf of third parties (such as advertising and social networks), manufacturers of browsers and other software or operating systems should be encouraged to develop, implement and ensure effective user empowerment, by offering control tools within the browser (or other software or operating system) such as Do Not Track (DNT), or other technical means that allow users to easily express and withdraw their specific consent, in accordance with Article 7 of the GDPR. Such tools can be offered to the user at the initial set-up with privacy-friendly default settings. Adherence to accepted technical and policy compliance standards must become a common practice. In addition, website operators should respect and adhere to browser control tools or other user preference settings."*

La position du Parlement européen est à ce jour très proche des attentes du G29, de la CNIL et du public.

Enfin, rappelons que dans tous les cas, ce consentement devra satisfaire les critères fixés par le RGPD, à savoir être « libre, spécifique et informé » et résulter d'un acte univoque, pour que ce dernier soit valide. Par exemple, un consentement obtenu sous la contrainte ou sans lequel l'utilisateur serait privé d'accès à un site web ne serait pas valide. De manière générale, que le consentement soit recueilli au niveau du navigateur, du système d'exploitation ou même de chaque site, il devra réunir l'ensemble de ces conditions.

La future réglementation comporte également des dispositions relatives à une pratique jusqu'alors peu connue mais dont l'essor ces dernières années est de plus en plus important, le *Wifi Tracking*.

INFOSPLUS

Do Not Track (DNT)

Le DNT est un signal envoyé par le navigateur de l'internaute lors de chaque appel d'une ressource sur le web (image, texte, publicité, etc.). Ce signal, qui peut prendre les valeurs 0 (j'accepte le traçage) ou 1 (je refuse le traçage), indique au destinataire la volonté de l'internaute. Le signal est géré automatiquement par le navigateur de l'internaute, à partir d'une valeur par défaut, d'une liste blanche de domaines et, éventuellement, de finalités acceptées par l'internaute[3]. Le DNT permet également aux éditeurs de signaler les tiers réalisant un traçage des internautes sur leur site et de demander un consentement pour leur compte à l'internaute, via une API du navigateur. Ce consentement peut être obtenu via une action positive de l'internaute, ou via les finalités qu'il a préalablement acceptées.

LE WIFI TRACKING

Véritable superposition des techniques numériques de suivi des personnes dans le monde physique, le *WiFi tracking* peut être défini comme l'ensemble des pratiques consistant à collecter des données émises par les appareils (téléphones portables, PDA, tablettes) des personnes de passage dans les espaces publics ou privés. Elles permettent par exemple de mesurer l'audience d'un panneau publicitaire ou la fréquentation de certaines zones, mais aussi d'analyser le flux des piétons entre deux points distants, ou encore de mesurer la fréquence de leurs visites, aussi appelée taux de répétition.

3 Le standard ne spécifie pas la partie permettant de gérer les finalités, mais prévoit des spécificités dites « régionales » qui peuvent être utilisées pour gérer une liste de finalités acceptées par l'internaute.

La CNIL a très tôt été saisie des problématiques liées à ce type de dispositifs

En 2014 tout d'abord dans le cadre d'un dossier dont la presse s'est largement fait l'écho. Une société spécialisée dans l'affichage publicitaire envisageait de mettre en place au sein d'un périmètre limité et sur l'esplanade de la Défense un système expérimental de mesure d'audience de dispositifs publicitaires. Le traitement consistait à compter le nombre des piétons passant à proximité des panneaux, à mesurer le nombre de fois où elles repassent devant ces panneaux et à suivre leurs parcours, afin d'optimiser au mieux l'affichage de messages publicitaires. Ce type de traitement étant soumis à autorisation, la CNIL a alors été saisie et a refusé la réalisation du traitement le 16 juillet 2015, en relevant que les données collectées n'étaient pas anonymisées et que les garanties envisagées n'étaient pas suffisantes, notamment en termes de transparence du traitement. En effet, le rôle de la CNIL est avant tout de s'assurer que ce type de dispositif s'accompagne de mesures protectrices permettant de garantir le respect de la vie privée des personnes au quotidien.

De nombreuses entreprises souhaitant s'engager sur cette voie sollicitent d'ailleurs la Commission pour s'assurer de la conformité de leurs traitements avec la règlementation. C'est en ce sens qu'a pu notamment être autorisé le traitement de mesure d'audience de dispositifs publicitaires sur la voie publique réalisé par la société Retency, intégrant des mesures techniques permettant d'anonymiser les données collectées dans des délais très courts.

Le RGPD fixe le cadre général des règles relatives à la protection des données. Comme vu précédemment, *ePrivacy* précisera les modalités d'application spécifique de ces règles dans le contexte des communications électroniques. Du fait de leur faible développement, les pratiques de *WiFi tracking* n'étaient pas explicitement prévues par la directive 2002. Cette absence est aujourd'hui corrigée par la proposition de règlement *ePrivacy*.

La proposition initiale de règlement paraît pouvoir être complétée. Là où le texte va dans le bon sens pour l'encadrement des traceurs de type cookies par exemple, il permet le *Wifi Tracking* à la suite d'une simple information préalable des utilisateurs, tout en réservant la possibilité pour le responsable de traitement de remplacer cette information par un logo (ou « standardized icons ») suffisamment explicite et dont la création passerait par un acte délégué de la Commission européenne.

« Le consentement doit être conforté comme la pierre angulaire de la protection des terminaux. »

Aussi, pour rehausser le niveau de « protection » des terminaux prévu ci-dessus et encadrer au mieux la captation passive de données émises par les appareils, le Parlement européen a proposé des modifications dans le sens de l'avis du G29 du mois d'avril 2017. La version de texte adoptée par le Parlement prévoit que ce type de traitement ne peut être effectué que :

- dans le seul but et pour la seule durée nécessaire à l'établissement de la connexion demandée par l'utilisateur ; ou
- si l'utilisateur a donné son consentement ; ou
- si les données sont anonymisées et si les risques sur la vie privée des personnes sont atténués (se limiter à une analyse statistique, limiter le suivi dans le temps et dans l'espace, mécanismes d'opposition, etc.).

Le Parlement européen a également ajouté des dispositions relatives à l'information préalable des personnes. Celle-ci doit être claire et intelligible, en précisant, a minima, la façon dont les données sont collectées, la finalité du traitement, l'identité du responsable du traitement, ainsi que toutes les informations prévues à l'article 13 du RGPD.

La proposition de règlement présente suffisamment d'éléments pour assurer la continuité des principes adoptés depuis la dernière réforme de la directive de 2002. À tout le moins, elle comporte les principaux éléments qui permettront de bâtir ce qui sera le futur de la protection de la vie privée dans les communications électroniques. Certains points paraissent devoir être soulignés dans la perspective des débats à venir.

Le consentement tout d'abord, doit rester et être conforté comme la pierre angulaire de la protection des terminaux. La proposition va dans ce sens en matière d'utilisation de traceurs. Il convient en outre de veiller à traduire dans la pratique ces principes, au bénéfice des utilisateurs. Le paramétrage du navigateur est à cet égard une novation à saluer qui intègre les principes de protection des données dès la conception et par défaut prévus par le RGPD.

« Le paramétrage du navigateur est une novation qui intègre les principes de protection des données dès la conception et par défaut prévus par le RGPD. »

Le projet de loi relatif à la protection des données personnelles

La CNIL a rendu le 30 novembre 2017 son avis sur le projet de loi relatif à la protection des données personnelles. Ce texte permettra de donner corps au Règlement européen et de la Directive du 27 avril 2016, qui sont une avancée majeure pour la protection des données.
La CNIL regrette le retard pris dans la préparation de ce projet de loi. Elle appelle, de toute urgence, à l'adoption de l'ordonnance prévue pour la réécriture du droit français de la protection des données afin de rendre le nouveau cadre juridique plus lisible pour les professionnels et les citoyens.

POURQUOI UN PROJET DE LOI RÉFORMANT LA LOI INFORMATIQUE ET LIBERTÉS ALORS QUE LE RÈGLEMENT EUROPÉEN EST DIRECTEMENT APPLICABLE AU 25 MAI PROCHAIN ?

Le 17 novembre 2017, la Commission a été saisie d'un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ce projet de loi a pour objet la mise en conformité du droit national avec le « paquet européen de protection des données » adopté par le Parlement européen et le Conseil le 27 avril 2016 qui se compose :

- d'un **Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard des données à caractère personnel,** qui constitue le cadre général de la protection des données et est directement applicable à compter du 25 mai 2018 ;

- d'une **Directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales,** d'enquête et de poursuites en la matière ou d'exécution de sanctions pénales, qui doit être transposée au plus tard le 6 mai 2018.

Il est assez remarquable de constater que la plupart des principes posés par le législateur il y a près de 40 ans dans la loi du 6 janvier 1978 restent valables. Cependant le nouveau cadre juridique du « paquet européen de protection des données » introduit un changement de paradigme.

Il repose en effet sur une logique de responsabilisation renforcée des acteurs, responsables de traitements et sous-traitants. Alors que la loi de 1978 reposait en grande partie sur une logique de « formalités préalables » (déclaration, autorisation, etc.), le Règlement repose sur une logique de conformité continue, tout au long du cycle de vie de la donnée, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur. En contrepartie de la réduction du contrôle en amont exercé via ces formalités, la CNIL voit ses pouvoirs de contrôle et de sanction renforcés par la possibilité d'infliger des amendes allant, dans les cas les plus graves, jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires pour une entreprise.
Le Règlement renforce également les droits des personnes en facilitant l'exercice de ceux-ci et en créant de nouveaux droits, comme le droit à la portabilité des données personnelles ou un droit à l'oubli propre pour les mineurs.
Enfin, pour permettre une application uniforme et cohérente du Règlement, le législateur européen a prévu un mécanisme de coopération renforcée entre les autorités de protection des données, qui devront adopter des décisions communes lorsque les traitements de données seront transnationaux, dans le cadre du mécanisme dit du « guichet unique ».

L'adoption du « paquet européen de protection des données » constitue donc une avancée majeure. Ces textes doivent permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Ils constituent également un standard international en matière de protection des données, notamment compte tenu du champ d'application élargi du Règlement via le critère de ciblage.

Ces changements nécessitent d'adapter la loi fondatrice du 6 janvier 1978, que le projet choisit symboliquement de ne pas abroger, tout en conservant son article 1er (« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle 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 »).

Le projet de loi modifie certains articles de la loi du 6 janvier 1978, avec un triple objectif :

- **Rendre compatible la loi avec le droit de l'Union (titre Ier du projet de loi).** Le nouveau cadre juridique du Règlement oblige le législateur à adapter les missions de la CNIL et à revoir les procédures applicables aux sanctions qui comportent désormais un aspect coopération internationale.

- **Exercer certaines des marges de manœuvre prévues par le Règlement (titre II).** Le Règlement comporte en effet plus d'une cinquantaine de renvois au droit national, permettant aux États membres de maintenir des formalités préalables à certains traitements, de poser des règles de fond propres ou de moduler les garanties offertes aux personnes. Il appartient au législateur national de décider si et dans quelle mesure il souhaite faire usage de chacune de ces marges.

- **Transposer les dispositions de la Directive (titre III).** Ce texte concerne plus spécifiquement les traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites ou d'exécution de sanctions pénales. Il nécessite de modifier la loi du 6 janvier 1978 pour transposer la directive.

« Le projet de loi va permettre l'application effective du règlement européen, qui représente un progrès majeur pour la protection des données personnelles des citoyens et la sécurité juridique des acteurs économiques. »

QUE DIT L'AVIS DE LA CNIL DU 30 NOVEMBRE 2017 ?

La CNIL, dans son avis, salue cette nouvelle étape et souligne que le projet de loi joue pleinement le jeu du Règlement et de l'harmonisation recherchée par celui-ci, en ne maintenant des dérogations nationales que lorsque celles-ci sont réellement justifiées, notamment en matière de données de santé.

Si, sur certains points, la Commission a pu exprimer une appréciation divergente et propose de positionner différemment le curseur (maintien d'un régime d'autorisation pour les données génétiques par exemple), elle estime, de manière globale, que le projet de loi semble faire un usage raisonnable de ces marges, ne conservant une spécificité nationale que par exception, dans les cas qui le justifient absolument. Il s'inscrit ainsi pleinement dans la logique du Règlement, cadre unique et harmonisé pour l'ensemble des citoyens et opérateurs de l'espace européen.

Par ailleurs, la Commission a souligné que le projet de loi remplissait globalement l'objectif principal qui lui était assigné, à savoir adapter le droit français au nouveau cadre européen pour en assurer la pleine effectivité pour les citoyens et les opérateurs dès le mois de mai 2018.

En particulier, concernant l'organisation et le fonctionnement de la CNIL, le projet de loi complète les missions de la Commission pour tenir compte du nouvel environnement juridique. Plus encore qu'aujourd'hui, cet environnement s'inscrit dans une logique d'accompagnement des acteurs, eux-mêmes davantage responsabilisés et donc davantage demandeurs de sécurité juridique. Il est prévu que la commission puisse édicter et publier de nouveaux instruments, le cas échéant de droit souple : lignes directrices, recommandations et référentiels destinés à faciliter la mise en conformité des acteurs privés et publics. Il est prévu en outre que la Commission puisse établir des règlements types de sécurité contraignants pour les traitements les plus sensibles (biométrie, génétique, santé, condamnations pénales).

Le projet de loi comporte en outre des précisions sur les pouvoirs de contrôle de la CNIL (sur l'opposabilité de certains secrets, sur la participation d'agents venus d'autres autorités aux contrôles de la CNIL, etc.). Il supprime la majorité des formalités préalables, à savoir l'obligation de déclaration ou d'autorisation auprès de la CNIL, à l'exception des traitements dans le domaine de la santé (soumis pour certains à demande d'autorisation) et les traitements relevant de la demande d'avis (ex : traitements biométriques pour le compte de l'État, traitements ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales).

Tout en soulignant ces apports majeurs, **la Commission relève dans son avis trois limites notables**.

En premier lieu, la Commission regrette le calendrier retenu pour l'adaptation du droit français.

Si elle a été associée en amont, par le ministère de la justice, aux réflexions sur cette entreprise législative, elle déplore d'avoir été saisie aussi tardivement du projet et de ne pas avoir disposé du délai nécessaire à l'examen, dans des conditions acceptables, d'un texte d'une telle portée. Surtout, la Commission souligne l'impératif de disposer d'un droit national conforme au 25 mai 2018, que le calendrier tardif d'adoption fragilise.

57

C'est le nombre de dispositions dans le Règlement qui renvoient au droit national, permettant au législateur national d'ajouter dans certaines hypothèses des règles de fond ou de procédure

En deuxième lieu, la Commission attire l'attention sur le manque de lisibilité des nouvelles dispositions du fait, notamment, du choix du projet de loi, consistant à n'opérer que les modifications « *a minima* » nécessaires à la mise en œuvre du Règlement et de la Directive, et à renvoyer la réécriture d'ensemble de la loi du 6 janvier 1978 à une ordonnance ultérieure.

Dans l'attente de cette ordonnance, ce choix créé une double difficulté de lecture. D'une part, la loi pourra induire en erreur le lecteur sur la portée de ses droits et obligations. En effet, des dispositions formellement inchangées et toujours en vigueur de la loi de 1978 ne seront en réalité plus applicables,

« Le projet de loi joue pleinement le jeu du Règlement et de l'harmonisation en ne maintenant que des dérogations nationales réellement justifiées.»

car substituées, dans leur champ, par les dispositions du Règlement (par exemple sur le consentement, la base légale des traitements ou la portée des droits reconnus aux personnes), tandis que la loi nationale ne comportera aucun écho à certains nouveaux droits ou nouvelles obligations posés par le Règlement.

D'autre part, la loi du 6 janvier 1978 ne donnera pas de grille de lecture permettant aux citoyens et aux responsables de traitement de comprendre les droits et obligations différenciés qui existeront demain dans les trois grands compartiments de la protection des données que seront le champ du Règlement (à savoir les fichiers « civils et commerciaux », mais également certains fichiers relevant de l'administration), celui de la Directive (traitements à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites) et, enfin, ce qui ne relève pas du champ du droit de l'Union ou relève du seul chapitre 2 du titre V du traité sur l'Union européenne (traitements intéressant la sûreté de l'État et la défense).

Un dernier enjeu de lisibilité tient aux difficultés de frontière, que le projet de loi ne saurait toutefois résoudre à lui seul, qui se poseront entre les différents régimes applicables aux traitements de données selon leurs finalités, parfois multiples, certains traitements pouvant relever du Règlement et de la Directive, d'autres relevant à la fois du champ de la Directive et du « hors-champ » du droit de l'Union.

Cet enjeu de lisibilité dépasse la seule structuration technique du texte. Il conditionne la pleine effectivité des droits des citoyens et des obligations des différents acteurs. Le choix fait est d'autant plus regrettable que la loi du 6 janvier 1978 constitue, par son objet et par son rayonnement aux niveaux européen et international, l'un des grands marqueurs du droit français, connu et pris comme standard. Dans l'attente de l'ordonnance, la CNIL publiera sur son site un « guide de lecture » visant à articuler la loi, une fois adoptée, et le RGPD.

En dernier lieu, la Commission regrette que, compte tenu notamment du calendrier retenu, et du choix de se contenter d'un exercice a minima d'adaptation du droit français aux deux textes européens de 2016, le projet de loi constitue à certains égards une occasion manquée de procéder à un réexamen global du droit de la protection des données en France, de compléter le dispositif législatif sur certains points et d'approfondir les droits des personnes pour les traitements entrant dans le champ de la Directive ainsi que pour ceux situés en dehors du champ du droit de l'Union.

Recherche médicale et protection des données

Depuis 1994, la CNIL est compétente pour autoriser les organismes, appelés aussi les promoteurs, qui souhaitent mener des études dans le domaine de la santé et, pour ce faire, collecter des données de santé et les analyser. Des dispositions spécifiques de la loi Informatique et Libertés fixent le cadre dans lequel la CNIL peut autoriser ces traitements et, ainsi, permettre à des personnes qui ne participent pas à la prise en charge habituelle des patients de pouvoir néanmoins analyser et étudier leurs données de santé.

Ces traitements reposent sur des protocoles de recherche variés, avec des méthodologies différentes (essais cliniques, études observationnelles, études avec entretiens, etc.).

LA MISE EN ŒUVRE PRATIQUE DU NOUVEAU CHAPITRE IX (RECHERCHE DANS LE DOMAINE DE LA SANTÉ)

La CNIL instruit les dossiers dont elle est saisie en veillant notamment à l'information des patients concernés, à la pertinence des données collectées (en portant une attention toute particulière à la collecte des données les plus sensibles - telles que les données génétiques ou l'origine ethnique) et à leur sécurité.

Les principes de respect du secret médical et de minimisation des données conduisent, par principe, à n'autoriser que les études pour lesquelles le promoteur ne reçoit qu'un code ou un numéro attribué aux patients, c'est-à-dire des données pseudonymisées. Le traitement des noms/prénoms en clair des personnes n'est autorisé que dans certains cas particuliers comme le suivi des personnes pour les études longues ou dans le cadre de certains registres. Dans ces cas précis, le promoteur ou son représentant doit veiller à assurer une stricte confidentialité des données, notamment en séparant les données directement identifiantes des données de santé. Le régime juridique des recherches en santé a connu des évolutions notables ces dernières années en raison de la publication de plusieurs textes législatifs et réglementaires dans des domaines différents :

- la création du système national des données de santé (SNDS) (voir encadré ci-contre) par la loi de modernisation de notre système de santé du 26 janvier 2016 et ses textes d'application : le décret du 26 décembre 2016 « SNDS », **les arrêtés de 2017 sur le référentiel de sécurité SNDS et sur les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études ;**
- la modification du décret d'application de la loi Informatique et Libertés pour permettre la mise en application de la loi de modernisation de notre système de santé ;
- l'entrée en vigueur du cadre juridique relatif aux recherches impliquant la personne humaine, avec la loi du 5 mars 2012 (dite loi « Jardé »), l'ordonnance de 2016 et deux décrets d'application (2016 et 2017) ;
- la loi du 7 octobre 2016 pour une République numérique.

Chacun de ces textes, dont la plupart a fait l'objet d'un avis préalable de la CNIL, a eu un impact sur les dispositions encadrant la recherche médicale au regard de la protection des données à caractère personnel.

La loi de modernisation de notre système de santé, qui prévoit la création de l'Institut national des données de santé (INDS) et du SNDS, opère une modification majeure des dispositions de la loi Informatique et Libertés en fusionnant ses chapitres IX et X.

Précédemment, le chapitre IX de la loi s'appliquait aux traitements de recherche dans le domaine de la santé et le chapitre X aux traitements ayant pour finalité l'évaluation, l'analyse des pratiques ou des activités de soins ou de prévention. Ce dernier concernait par exemple les études nécessitant un accès aux données hospitalières au niveau national (PMSI) et pour lesquels les données étaient considérées comme très indirectement identifiantes.

Le chapitre IX de la loi rassemble maintenant l'ensemble des dispositions de la loi en matière de recherche dans le domaine de la santé, et distingue :

- **les recherches impliquant la personne humaine,** définies par les dispositions du code de la santé publique, dont la réalisation nécessite l'obtention d'un avis favorable d'un comité de protection des personnes (CPP) et l'autorisation de la CNIL ;
- **les recherches n'impliquant pas la personne humaine** pour lesquelles les dossiers de demande d'autorisation doivent être adressés à l'INDS. Cet institut joue le rôle de secrétariat unique pour l'ensemble de ces demandes et assure leur transmission au Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES), successeur du Comité consultatif sur le traitement de l'information en matière de recherche (CCTIRS), qui émet un avis ; sur la base de ces éléments, la CNIL examine le dossier et délivre, le cas échéant, son autorisation.

Les dispositions du nouveau chapitre IX sont applicables depuis le 30 juin 2017, date d'installation du CEREES, et effectives depuis le 21 septembre 2017, date de sa première réunion. Depuis, l'INDS transmet à la CNIL les demandes ayant fait l'objet d'un avis favorable du CEREES, avec ou sans recommandations.

Une fois reçues par la CNIL, les demandes d'autorisation « recherche » sont instruites par un pôle dédié à la recherche au sein du service santé ; ce pôle a été créé spécifiquement, d'une part, afin d'assurer la transition vers l'application des nouvelles dispositions du chapitre IX et, d'autre part, d'optimiser l'instruction des dossiers notamment en termes de délai. L'examen des dossiers reçus porte en particulier, comme le prévoit la loi, sur l'existence d'une finalité d'intérêt public du projet, sur la durée de conservation des données et sur les dispositions prises pour assurer la sécurité et la garantie des secrets protégés par la loi.

En 2016, la CNIL avait reçu 1 161 demandes : 287 demandes « évaluation » et 874 demandes « recherche ».

En 2017, la CNIL a reçu 737 demandes d'autorisation au total, dont 156 réalisées en application des nouvelles dispositions de la loi Informatique et Libertés.

En 2017 la CNIL a reçu

737

demandes d'autorisation « recherche »

1 447

engagements de conformité aux méthodologies de référence

La diminution du volume de demandes « recherche » reçues s'explique par la publication de nouvelles méthodologies de référence en 2016.

Au total, au cours de l'année 2017, la Commission a délivré 391 autorisations « recherche » et 394 autorisations « évaluation ».

Abrogation du chapitre X de la loi Informatique et Libertés

L'entrée en vigueur du nouveau chapitre IX en juin 2017 a conduit à la suppression du chapitre X comme le prévoyait la loi de janvier 2016.

En conséquence, seules les demandes d'autorisation (ou de modification) relevant du chapitre X adressées la CNIL avant cette date ont pu être instruites. À ce jour, l'ensemble des demandes d'autorisation relevant du chapitre X ont été traitées par les services de la CNIL.

Les services de la CNIL ont également accompagné les responsables de traitement dans l'élaboration de modèles de dossiers. Saisie de près de 200 demandes similaires, la CNIL a par exemple été en mesure de délivrer dans des délais très réduits les autorisations attendues par les agences régionales de santé (ARS) et les établissements de santé pour accéder aux données du PMSI national.

Un renforcement du pouvoir de simplification de la CNIL

La loi de modernisation de notre système de santé a, dans l'esprit de « responsabilisation » porté par le RGPD, confié à la CNIL un pouvoir de simplification des démarches grâce à une palette d'outils spécifiques au secteur de la recherche dans le domaine de la santé.

Les méthodologies de référence (article 54-IV)

L'engagement de conformité à une méthodologie de référence permet à un promoteur de mettre directement en œuvre un traitement de données de santé à des fins de recherche, d'étude ou d'évaluation sans avis préalable du CEREES et sans autorisation spécifique de la CNIL[1].

5 532

engagements de conformité

3

méthodologies de référence reçues

À ce jour, **trois méthodologies de référence ont été établies par la CNIL :** une relative aux recherches nécessitant le consentement exprès de la personne (MR 001), une autre relative aux recherches portant sur des dispositifs médicaux de diagnostic in vitro (MR 002) et, enfin, une troisième relative aux recherches nécessitant une non-opposition (MR 003).

Depuis l'adoption de ces méthodologies de référence, 5 532 engagements de conformité ont été adressés à la CNIL (toutes MR confondues), dont 1 447 pour la seule année 2017.

Afin, d'une part, de prendre en compte les évolutions rappelées ci-dessus et, d'autre part, de fournir aux responsables de traitement des outils de simplification adaptés à leurs besoins, la CNIL a très rapidement pris l'initiative de procéder à l'actualisation de ses méthodologies de référence MR 001 et MR 003 et à la rédaction d'une nouvelle méthodologie (MR 004) applicable en matière de recherches n'impliquant pas la personne humaine.

Ces projets ont fait l'objet d'une large concertation avec les représentants des acteurs concernés en fin d'année 2017 pour une adoption prévue au début de l'année 2018.

L'homologation par la CNIL de conditions d'accès à des jeux de données agrégées ou des échantillons

Des jeux de données et échantillons peuvent être extraits de bases de données existantes. Afin de faciliter l'utilisation de ces « extraits », permettant de réaliser un grand nombre d'études au cours desquelles les risques de ré-identification sont limités, la CNIL peut homologuer des conditions d'accès allégées. Il s'agira plus particulièrement de simplifier le circuit de validation des demandes, en prévoyant des modalités d'instruction accélérées ou la suppression de l'intervention de certains acteurs.

Cette simplification pourrait par exemple concerner l'échantillon généraliste des bénéficiaires du SNIIRAM (EGB).

Les décisions uniques

La CNIL peut délivrer à un même demandeur une autorisation pour les traitements répondant à une même finalité, portant sur les mêmes catégories de données et ayant des catégories de destinataires identiques.

Des projets de mesure de simplification sont en cours d'élaboration, en collaboration avec l'INDS et le ministère de la santé, notamment pour l'accès à des échantillons de données issus de bases médico-administratives.

1 La saisine d'un CPP est cependant toujours requise s'agissant des recherches impliquant la personne humaine.

L'IMPLICATION DE LA CNIL DANS L'ÉLABORATION DU NOUVEAU DISPOSITIF

Cadre règlementaire : les avis de la CNIL

La CNIL a été amenée à se prononcer sur plusieurs projets de textes parus en 2017, notamment ceux dont la publication était essentielle à la mise en œuvre de la loi de modernisation de notre système de santé et du dispositif prévu par le législateur. Ces avis ont été l'occasion pour la Commission d'insister sur la nécessité de prévoir des garanties suffisantes pour permettre le respect des droits des personnes concernées.

Elle s'est par exemple prononcée sur :

- le décret relatif au dossier pharmaceutique ;
- le décret relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé (NIR-INS).

La Commission s'est également prononcée sur le projet de loi relatif à la protection des données personnelles qui a pour but d'adapter les dispositions législatives existantes au RGPD, et dont un chapitre est dédié aux traitements de données à caractère personnel dans le domaine de la santé.

Cette activité de conseil du Gouvernement est amenée à perdurer dans le cadre des futurs projets de texte dont elle sera prochainement saisie.

La CNIL, en lien avec tous les acteurs

Le rôle de la CNIL ne se limite pas à donner des avis sur des projets de texte ou autoriser des projets de recherche ; régulièrement sollicitée par les acteurs institutionnels du secteur de la santé, elle joue un rôle majeur dans l'accompagnement de ces acteurs et s'implique en amont dans les réflexions nationales relatives à l'utilisation des données de santé.

La collaboration étroite avec l'INDS

La loi prévoit des délais précis dans lesquels les demandes d'autorisation « recherche, étude ou évaluation » dans le domaine de la santé doivent être instruites. Ainsi, l'INDS, qui assure le secrétariat unique pour les recherches n'impliquant pas la personne humaine, dispose de sept jours pour saisir le CEREES qui, lui, dispose d'un mois pour rendre son avis. La CNIL dispose, quant à elle, d'un délai de deux mois renouvelable pour autoriser ou non le traitement.

Il est donc naturellement apparu nécessaire de concevoir et de mettre en place des procédures très opérationnelles, permettant une coopération efficace avec l'INDS afin de garantir un circuit fluide des dossiers. Ainsi, les équipes de la CNIL et de l'INDS se rencontrent très régulièrement afin d'échanger à la fois sur l'organisation générale du processus prévu par le chapitre IX, mais également de manière plus précise sur le contenu de certains dossiers. En effet, l'INDS est également chargé de rendre un avis sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation justifiant la demande de traitement.

Par ailleurs, la période transitoire entre l'arrêt de l'activité du CCTIRS et la mise en place du CEREES a conduit de nombreux responsables de traitement à saisir la CNIL sans avis préalable d'un comité compétent. Ces demandes, juridiquement non recevables, ont fait l'objet d'un accompagnement spécifique par les agents de la CNIL, en collaboration avec l'INDS, notamment afin d'expliquer les raisons pour lesquels le dossier ne pouvait être traité en l'État et d'envisager les solutions pour faire aboutir ces demandes.

La CNIL a également été sollicitée pour participer, en qualité d'observateur, aux réunions du comité d'expertise sur l'intérêt public (CEIP), chargé d'établir un avis préliminaire à celui rendu par l'INDS en matière d'intérêt public des finalités des traitements de données.

Les instances compétentes dans le nouveau dispositif

Les services de la Commission travaillent également en étroite collaboration avec la Commission nationale des recherches impliquant la personne humaine (CNRIPH), le ministère de la santé, le ministère de la recherche, l'INDS et le CEREES pour fluidifier et garantir la cohérence du nouveau dispositif (définition des recherches n'impliquant pas la personne humaine, répartition compétence CPP/CEREES, avis CPP préalablement à l'autorisation de la CNIL, etc.).

« La CNIL s'implique en amont dans les réflexions nationales relatives à l'utilisation des données de santé. »

La participation aux réunions du CSF santé

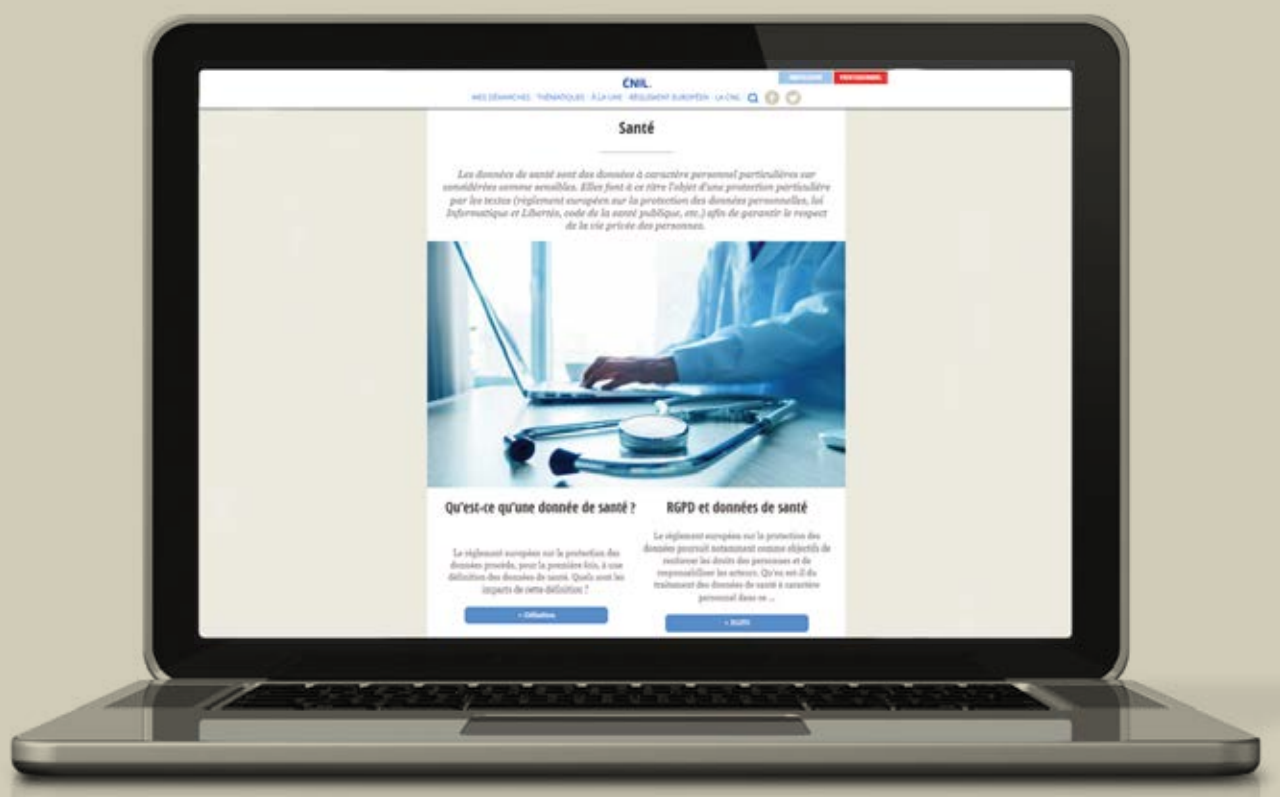
La CNIL a activement participé au groupe de travail « accès aux données de santé » du Comité stratégique de filière des industries et technologies de santé. Ce groupe de travail a pour mission de « promouvoir une démarche active visant à faciliter l'accès aux données de santé à des fins de santé publique, de recherche et de développement industriel » et a élaboré et publié un guide composé de fiches, présentant la gouvernance générale des accès au SNDS et les procédures de dépôts de dossiers, ainsi que des préconisations pour l'usage de ces données par les industriels des produits de santé.

L'accompagnement des responsables de traitement

La mission d'accompagnement de la CNIL auprès des responsables de traitement, notamment lors des permanences téléphoniques du service « santé », dans les réponses aux demandes de compléments ou encore dans l'instruction des dossiers est essentielle : les nouvelles procédures, même si elles ont vocation à simplifier les circuits et à fluidifier les échanges, nécessitent un important travail d'explication à destination de l'ensemble des acteurs concernés.

Par ailleurs, des réunions sont régulièrement organisées avec les acteurs de terrain organisés en réseaux ou fédérations sur les grandes thématiques de la recherche (par exemple : AFCRO, LEEM, AFCDP, club RSSI, FEHAP, GIRCI, CHU, etc.).

Au-delà de la participation des agents de la CNIL à des colloques ou de conférences destinées à présenter le nouveau cadre juridique, la CNIL a mis en ligne sur son site internet un module spécifique d'information concernant le traitement des données de santé dont une rubrique porte sur les traitements à des fins de recherche, d'étude ou d'évaluation.



FOCUS

Le système national des données de santé (SNDS)

Le SNDS regroupe, en une seule base des bases médico-administratives qui existent depuis de nombreuses années : le SNIIRAM (base de l'assurance maladie), le PMSI (données hospitalières), le CépiDC (base gérée par l'INSERM comprenant les causes médicales de décès). Viendront prochainement s'y greffer des données liées au handicap issues des maisons départementales des personnes handicapées et des données provenant des mutuelles.

L'objectif du législateur, en janvier 2016, est d'ouvrir l'accès à ces données afin que celles-ci puissent être utilisées à des fins de santé publique et de recherche dans l'intérêt de la collectivité.

Le SNDS ne contient aucune donnée directement identifiante concernant les personnes physiques (pas de noms/prénoms ou numéro de sécurité sociale). Mais, même si les données contenues dans le SNDS sont dites « pseudonymisées », il s'agit tout de même de données à caractère personnel sensibles ; à ce titre, leur accès est très encadré.

Un référentiel fixe ainsi les conditions de sécurité devant encadrer leur accès et leur traitement (gestion des utilisateurs, sécurité des systèmes d'information, etc.). Certains organismes publics disposent d'un accès permanent à certaines données dans le cadre de leur mission. Pour les autres organismes, une autorisation spécifique (recherche) doit être demandée auprès de la CNIL.

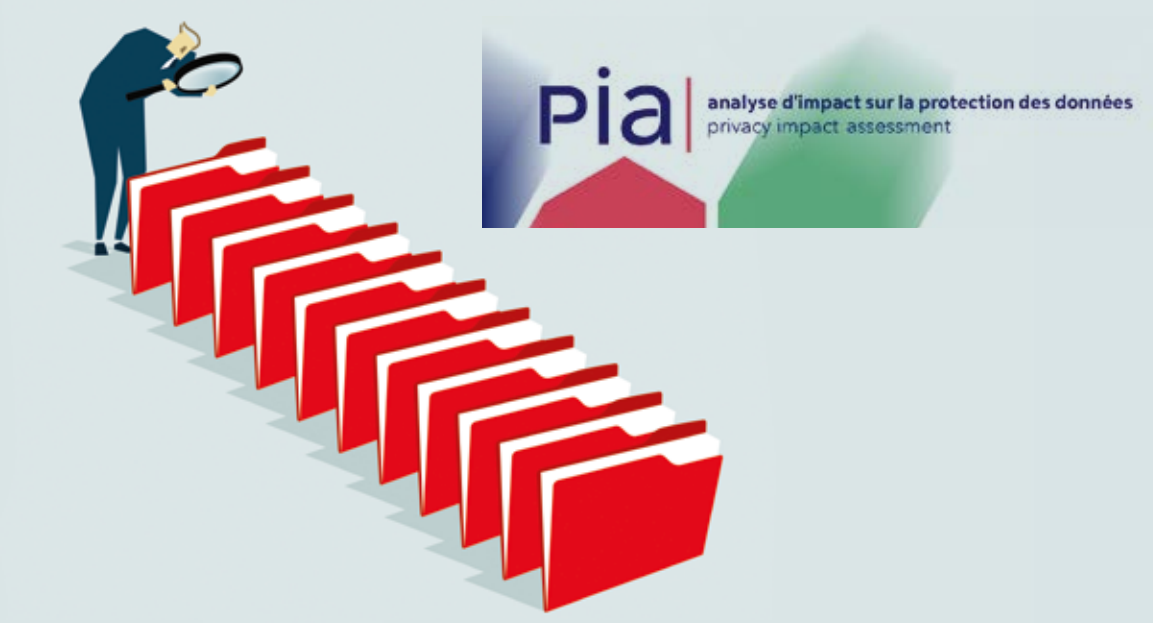
Une transparence est prévue par les textes, puisque l'INDS mettra à disposition du public l'autorisation de la CNIL, le protocole et les résultats de la recherche qui aura été autorisée.

La loi prévoit l'interdiction d'utiliser les données contenues dans le SNDS à des fins de promotion des produits de santé et à des fins d'exclusion de garanties des contrats d'assurance ou la modification des cotisations et des primes d'assurance. L'accès à ces données est donc limité pour les assureurs ou les laboratoires pharmaceutiques, qui doivent notamment faire appel à un bureau d'études ou un laboratoire de recherche.

Lorsque le traitement de données ne porte que sur des données du SNDS, les personnes sont informées de la réutilisation possible de leurs données à des fins de recherche sur le site Internet des hôpitaux, des organismes d'assurance maladie, des mutuelles et par le biais d'affiches dans les locaux et/ou via des documents remis. Les personnes disposent d'un droit d'opposition sauf pour les traitements de données nécessaires à l'exercice des missions des services de l'État et de certains établissements publics telles que, par exemple, le suivi d'une épidémie ou la surveillance sanitaire.

Les analyses d'impact relatives à la protection des données (PIA) et la notification de violation de données

Le Règlement européen prévoit que, lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, une analyse d'impact sur la protection des données doit être menée. La CNIL met à disposition des professionnels un logiciel open source pour faciliter la conduite et la formalisation d'analyses d'impact et a entièrement actualisé les guides pratiques. Par ailleurs, en cas de violation de données à caractère personnel, le responsable du traitement doit la notifier, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à l'autorité de protection des données compétente. En cas de risque élevé pour les personnes concernées, le responsable de traitement doit également informer, en des termes clairs et simples, les utilisateurs touchés par l'indicent, sauf si le responsable a pris préalablement ou postérieurement à la violation des mesures techniques ou organisationnelles appropriées.



LES ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

L'article 35 du règlement européen sur la protection des données rend obligatoire la réalisation d'une analyse d'impact relative à la protection des données (AIPD) pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Il y a ici une reconnaissance officielle de la nécessité, pour protéger efficacement les données, du recours à ce processus dont la CNIL recommandait l'usage dès 2015 via la publication de son premier guide PIA.

À RETENIR

Point sur les différentes terminologies

Plusieurs termes, utilisés de manière interchangeable en fonction des contextes, désignent le processus décrit dans l'article 35 du RGPD et dans les lignes directrices du G29 :

- Privacy Impact Assessment **(PIA)**
- Data Protection Impact Assessment **(DPIA)**
- Étude d'Impact sur la Vie Privée **(EIVP)**
- Analyse d'Impact relative à la Protection des Données **(AIPD)**

La CNIL utilise majoritairement l'acronyme PIA pour désigner ces analyses d'impact.

Pourquoi réaliser un PIA ?

Le recours à ce processus va permettre à un organisme d'évaluer la nécessité et la proportionnalité d'un traitement et de traiter les risques sur les droits et libertés des personnes concernées. Un risque sur la « vie privée » est un scénario décrivant un événement redouté et toutes les menaces qui le rendent possible. Il s'agit donc ici d'envisager les évènements redoutés tel qu'un accès illégitime aux données, les menaces permettant la réalisation de cet évènement tel qu'un défaut de sécurité et enfin l'impact sur les personnes concernées qui sera estimé en termes de gravité et de vraisemblance. Les différentes mesures prises au cours de l'analyse devront réduire cet impact à un niveau acceptable.

Au-delà de l'obligation légale, les lignes directrices soulignent l'importance de ce processus qui permet aux responsables de traitement de concevoir des traitements conformes aux exigences du règlement mais aussi de démontrer cette conformité.

Quand réaliser un PIA ?

Pour aider les responsables de traitement à respecter leurs obligations et garantir une interprétation cohérente de l'article 35, le groupe des CNIL européennes (G29) a adopté le 4 octobre 2017 des lignes directrices relatives à l'AIPD qui distinguent :

- d'une part les traitements qui n'auront pas à faire l'objet d'un PIA et
- d'autre part, tous les autres traitements qui présentent un risque inhérent élevé pour les droits et libertés des personnes concernées et devront de ce fait être soumis à un PIA. Pour identifier ces opérations de traitement, le G29 liste **9 critères à prendre en considération** tels que les activités de profilage et de prédiction ou les traitements à grande échelle ou encore ceux portant sur des données sensibles (ex. santé, infractions). **Plus un traitement remplira de critères, plus la nécessité d'une analyse sera impérative. Pour autant un seul critère peut parfois suffire**.

Pas de PIA nécessaire	PIA nécessaire
• le traitement n'est pas susceptible d'engendrer un risque élevé ; • un PIA similaire existe déjà ; • le traitement a été autorisé ou déclaré avant mai 2018 et n'a pas subi de modifications ; • il figure dans la liste (à venir), prévue par l'article 35.4. du RGPD, des traitements qui ne requièrent pas d'analyse. - quand le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public (art 6.1.c 6.1.e), sous réserve que les conditions suivantes soient remplies : a) qu'il ait une base juridique dans le droit de l'UE ou le droit de l'État membre ; b) que ce droit règlemente cette opération de traitement ; c) et qu'un PIA ait déjà été mené lors de l'adoption de cette base juridique ;	• les traitements qui présentent un risque inhérent élevé pour les droits et libertés des personnes concernées. Pour identifier ces opérations de traitement, le G29 liste 9 critères à prendre en considération tels que les activités de profilage et de prédiction ou les traitements à grande échelle ou encore ceux portant sur des données sensibles (ex. santé, infractions).

À RETENIR

Liste des 9 critères du G29

- **évaluation/scoring** (y compris le profilage) **;**
- **décision automatique avec effet légal ou similaire ;**
- **surveillance systématique ;**
- **collecte de données sensibles ;**
- **collecte de données personnelles à large échelle ;**
- **croisement de données ;**
- **personnes vulnérables** (patients, personnes âgées, enfants, etc.) **;**
- **usage innovant** (utilisation d'une nouvelle technologie) **;**
- **exclusion du bénéfice d'un droit/ contrat.**

Comment réaliser un PIA ?

Il existe différentes méthodologies pour réaliser un PIA. Aussi, dans un souci de cohérence, le G29 s'est accordé sur des critères communs d'acceptabilité. Les analyses devront donc *a minima* contenir :

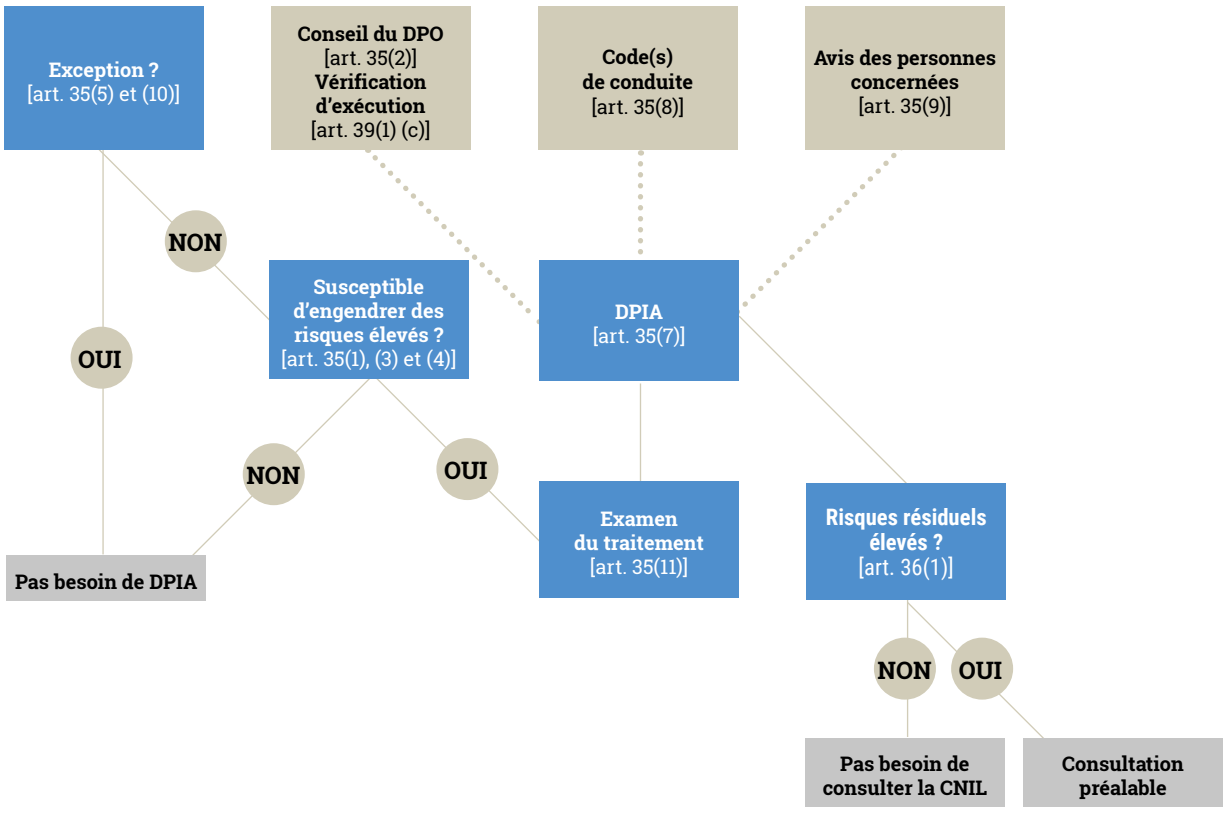
- une description systématique des opérations de traitement envisagées et les finalités du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques sur les droits et libertés des personnes concernées et ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

L'organisme porte la responsabilité de cette démarche mais l'exercice nécessite d'impliquer des parties prenantes telles que le délégué à la protection des données, les sous-traitants, les métiers, la direction informatique. Il s'agit donc d'une réflexion en commun menée par les personnes impliquées dans un projet qui auront chacune vocation à apporter leur pierre à cet édifice.

À l'issue de ce travail, la consultation de l'autorité de contrôle sera obligatoire **uniquement lorsque le responsable de traitement ne sera pas parvenu à réduire les risques pour les personnes concernées à un niveau acceptable**.

Le règlement ne rend pas la publication du PIA obligatoire, pour autant les lignes directrices encouragent, comme vecteur de confiance et gage de transparence la publication d'un résumé ou d'une déclaration relative à la réalisation d'un PIA.

Les principes de base adoptés par le RGPD en ce qui concerne les PIA



LA MÉTHODE PIA DE LA CNIL

Consciente des enjeux de sécurité majeurs existants autour de la protection des données personnelles, la CNIL travaille depuis 2010 sur la gestion des risques de sécurité. Elle a publié dès 2012 des guides sécurité à destination des responsables de traitement.

La CNIL a ensuite proposé en 2015 une méthode d'analyse des risques qu'un traitement de données personnelles peut engendrer sur la vie privée et les libertés des personnes concernées. Cette méthode, assortie de modèles et d'exemples d'analyse pour des objets connectés, a été mise à jour pour tenir compte du RGPD, entrant en vigueur en mai 2018, ainsi que des lignes directrices sur l'analyse d'impact relative à la protection des données, publiées en 2017 par le G29. Elle a été déclinée dans un logiciel permettant de la dérouler facilement et de produire le rapport PIA exigé par le RGPD pour les traitements susceptibles d'engendrer des risques élevés sur les droits et libertés des personnes concernées.

EXEMPLES DE PIA

Afin de faciliter la prise en main de sa méthode PIA, la CNIL a produit deux exemples très détaillés qui seront eux aussi publiés à destination des responsables de traitement :

- un modèle générique de PIA pour un objet connecté qui reprend tous les points de contrôle et les illustre au travers du cas d'un jouet connecté. Chacun de ces points est complété par des conseils sur les mesures juridiques et techniques adaptées au contexte d'un objet connecté ;
- un exemple fictif de PIA complet pour un objet de bien être qui montre le contenu concret d'un rapport de PIA finalisé et conforme aux lignes directrices du G29.

Mise à jour des guides d'analyse d'impact relative à la protection des données

La CNIL proposera en mars 2018 une révision de sa méthode PIA. Celle-ci sera restructurée pour s'adapter aux exigences du RGPD et pour la rendre encore plus opérationnelle. Ces modifications comprennent :

- **une révision du déroulé de la méthode** afin d'y incorporer le vocabulaire et les références du RGPD et pour l'adapter au découpage du rapport PIA défini dans les lignes directrices du G29 sur l'analyse d'impact relative à la protection des données ;
- **de nouveaux tableaux présenteront les points à contrôler** pour le respect de l'ensemble des principes juridiques et des bonnes pratiques de sécurité ;
- **un tableau de synthèse** permettant de visualiser la conformité globale du traitement.

En parallèle, **un WIKI sera mis à la disposition du public et contiendra les bases de connaissances et le catalogue des bonnes pratiques** afin d'en simplifier l'exploration et d'en rendre la lecture plus accessible. Ce mode de publication, nouveau pour la Commission, permettra à celle-ci de mettre à jour plus fréquemment ces éléments de références.

Le logiciel PIA : outiller les responsables de traitement et les accompagner dans leurs démarches de conformité

Soucieuse d'accompagner au mieux les responsables de traitements dans leurs démarches de conformité, en particulier ceux peu familiers avec la règlementation et ne disposant pas des outils et méthodes nécessaires pour se conformer aisément, la CNIL a développé un outil PIA sous licence libre et disponible gratuitement au téléchargement sur cnil.fr.

Solution « prête à l'emploi », se lançant facilement sur un poste de travail (Windows, MacOS ou Linux), ou bien se déployant sur les serveurs d'entreprises, le logiciel a été conçu pour offrir une interface simple et ergonomique pour ses utilisateurs tout en leur permettant d'industrialiser autant que possible la réalisation des analyses d'impact. L'outil PIA s'articule autour de trois axes :

1 **une interface didactique** qui permet de gérer simplement ses analyses et de dérouler clairement la méthode PIA conçue par la CNIL afin de n'en oublier aucune étape. Cette interface est complétée par des outils de visualisation permettant de comprendre rapidement l'État des risques du traitement étudié ;

2 **une base de connaissance** juridique et technique contextuelle, accessible à tout moment de la réalisation du PIA affichant les contenus des guides PIAs pertinents par rapport aux éléments de l'analyse d'impact en cours ;

3 **une approche modulaire** permettant d'adapter l'outil à des besoins spécifiques, soit en créant des templates d'analyse, soit en ajoutant de nouvelles fonctionnalités à l'outil en modifiant son code source.

Sorti en Novembre 2017 dans une version beta, la première version officielle de l'outil sera disponible pour l'été 2018. Entre ces deux dates, l'outil sera régulièrement mis à jour, prenant en compte les retours d'expérience reçus de la part des utilisateurs. Outil ouvert, les utilisateurs sont aussi invités à participer directement à son amélioration.

Un mois après sa publication, le logiciel PIA comptabilisait plus de

10 000

TÉLÉCHARGEMENTS

À ce titre, plusieurs traductions (italien, néerlandais, polonais, tchèque) ont été proposées par la communauté d'utilisateurs et ajoutées à l'outil. Il est aussi possible d'envisager d'autres formes de contribution à l'outil, par exemple en développant de nouvelles fonctionnalités.

DERNIÈRE MINUTE

L'outil PIA, publié en version beta en novembre 2017, est en constante amélioration grâce aux nombreuses contributions de ses utilisateurs. La CNIL a publié le 29 janvier 2018 une nouvelle version beta de son logiciel PIA.

Plusieurs bugs ont été corrigés, de nouvelles fonctionnalités sont disponibles ainsi que quatre nouvelles langues.

LES NOTIFICATIONS DE VIOLATION DE DONNÉES

L'entrée en application du Règlement général sur la protection des données (RGPD), le 25 mai 2018, généralise l'obligation de notifier les violations de données personnelles à tous les responsables de traitement. Une obligation qui participe au mouvement de responsabilisation des acteurs porté par le RGPD et qui leur demande d'assumer auprès des autorités et des personnes concernées, l'impact potentiel induit par une violation et de justifier du déploiement de mesures visant à le limiter au maximum. Car au-delà des conséquences directes pour les responsables de traitement, de telles violations de données personnelles peuvent engendrer d'importants risques et dommages pour les personnes. Il est donc primordial de tout mettre en œuvre afin de limiter ces impacts.

Les notifications de violation avant le RGPD

Si l'entrée en application du RGPD généralise cette obligation de notification des violations de données personnelles, celle-ci est déjà prévue à l'article 34 bis de la loi 78-17 du 6 janvier 1978 modifiée depuis 2011 et la transposition en droit français des directives « Paquet télécom ». Néanmoins, cette obligation de notification s'applique actuellement aux fournisseurs de services de communications électroniques déclarés auprès de l'ARCEP uniquement, et ce dans le cadre de leur activité de fourniture de services de communications électroniques. Une centaine de notifications ont été recensées par la CNIL dans ce cadre, et d'autres ont également été envoyées par des organismes non soumis aux dispositions de l'article 34 bis.

Dans une démarche d'accompagnement des responsables de traitement, les services de la CNIL, après analyse des risques engendrés par la violation et des réactions de l'organisme face à celle-ci, émettent, au besoin, des préconisations, s'agissant notamment de la nécessité ou non de notifier les personnes concernées, ainsi que de perfectionner les garanties de sécurité et de confidentialité mises en œuvre par l'organisme.

Qu'est-ce qu'une notification au sens du RGPD ?

Le RGPD définit dans son article 4 une violation de données comme étant « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

Une violation de données se définit donc comme tout incident, d'origine malveillante ou non, se produisant de manière intentionnelle ou pas, ayant comme conséquence une perte de disponibilité, d'intégrité ou de confidentialité de données personnelles.

Quand et comment notifier ?

Les articles 33 et 34 font apparaitre, quant à eux, différents niveaux s'agissant des violations et des obligations en découlant qui se distinguent en trois cas :

	Cas 1 : les violations n'engendrant pas de risques sur les personnes	**Cas 2 : les violations engendrant un risque sur les personnes**	**Cas 3 : les violations engendrant un risque élevé sur les personnes**
Documentation en interne par l'organisme sous forme d'un registre interne des différentes violations dont il est victime	X	X	X
Notification à l'autorité de contrôle, c'est-à-dire la CNIL en France, si possible en 72 h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

Des exceptions à l'obligation d'information des personnes concernées existent néanmoins lorsque :

- les données à caractère personnel affectées par ladite violation étaient protégées par des mesures de protection techniques et organisationnelles appropriées de sorte qu'elles étaient, avant la violation, incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès. Il peut s'agir d'une mesure de chiffrement dont la clé utilisée n'a été compromise dans aucune violation et a été générée de façon à ne pas pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser ;

- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser, par exemple des mots de passe d'employés ont été subtilisés, n'ont pas été utilisés et ont été réinitialisés ;

- elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt recommandé de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Dans le cas où l'organisme fait appel à un ou plusieurs sous-traitants impliqués dans la violation, ces derniers doivent prévenir dans les meilleurs délais le responsable de traitement après avoir pris connaissance de ladite violation afin que ce dernier puisse remplir ses obligations. Afin de guider les organismes au mieux et de faire en sorte que les différentes autorités européennes de protection des données aient la même interprétation du niveau de risque, ces dernières ont élaboré des guidelines adoptées en février 2018 qui permettront d'éclaircir ces concepts.

La CNIL travaille actuellement à la mise en place d'un téléservice qui permettra, aux organismes touchés par une violation de la notifier, de manière sécurisée, les informations nécessaires.

Quels sont les éléments devant figurer dans une notification ?

L'article 33 du RGPD décrit *a **minima*** les informations que doivent contenir une notification à l'autorité de protection des données et comprend :

- **des informations sur la nature de la violation de données à caractère personnel ;**
- **les coordonnées de la personne à contacter afin d'obtenir plus d'informations sur la violation** (en l'espèce le DPO ou tout autre personne en charge) ;
- **les conséquences probables de la violation** pour les personnes impactées ;
- **les mesures prises, ou à prendre, afin de remédier à la violation** et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- **les catégories et le nombre approximatif des personnes concernées ;**
- **les catégories et le nombre approximatif d'enregistrements concernés.**

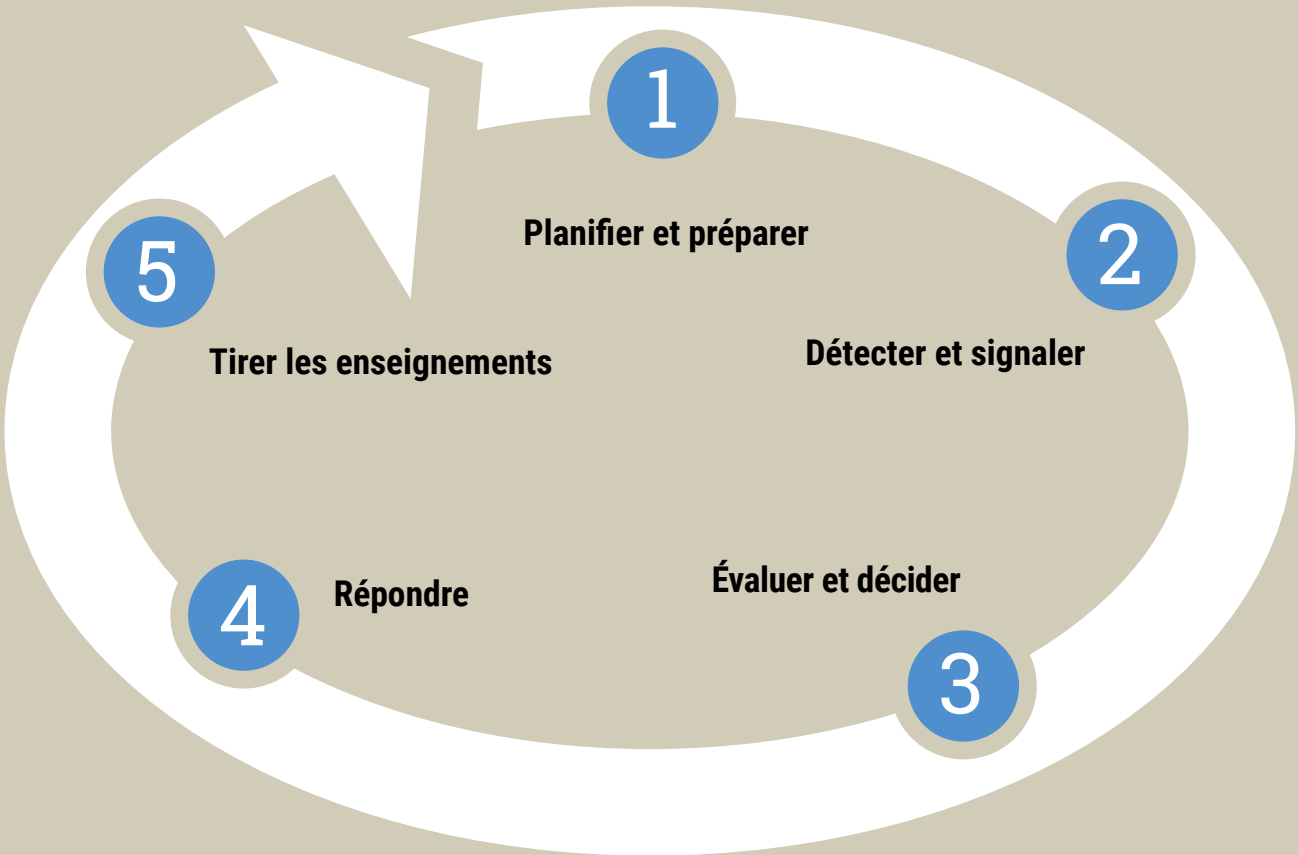
Les quatre premiers de ces points doivent être communiqués en des termes clairs, simples et compréhensibles par tous aux personnes concernées s'il est nécessaire d'informer ces dernières de la violation.

Toute violation devant être documentée en interne, il est nécessaire que cette documentation contienne, *a minima*, les mêmes informations que celles présentées ci-dessus.

COMMENT S'ORGANISER POUR GÉRER SES RISQUES ET SES INCIDENTS DE SÉCURITÉ ?

L'incident de sécurité n'arrive pas qu'aux autres et, de plus en plus, celui-ci affecte des données personnelles devenant de facto une violation de données personnelles. Il est possible de gérer cette situation sereinement dès lors que l'on est préparé en amont. Ainsi, il apparait essentiel que les organismes adaptent ou mettent en place un processus de gestion des incidents de sécurité dans le but d'être capables de détecter ces incidents, de les gérer et, le cas échéant, d'être en mesure de remplir leurs obligations légales.

Un processus classique de gestion des incidents en cinq étapes se base sur la norme ISO/IEC 27035



« Une violation de données est la matérialisation d'un risque que l'on a imaginé et essayé d'empêcher en procédant à une étude d'impact et en déployant des actions et solutions techniques ou organisationnelles. »

1

Planifier et préparer

il s'agit ici, en amont de la survenance d'un incident, **de formaliser et de tester les procédures internes de gestion des incidents** en créant un annuaire des parties impliquées et de ces procédures ;

2

Détecter et signaler

il faut être capable, en s'appuyant sur un travail de veille, **de détecter un évènement de sécurité** et de faire en sorte que les alertes soient traitées correctement afin d'être en mesure d'adopter la posture adéquate ;

3

Évaluer et décider

après avoir évalué les informations remontées et déterminé si l'évènement de sécurité est un incident avéré, il convient de **qualifier l'incident**, notamment dans le but de déterminer si ce dernier est une violation de données et de déterminer le risque engendré pour les personnes concernées. Dans le cas où la violation touche un traitement qui a fait l'objet d'un PIA, l'analyse ainsi réalisée peut être utilisée pour faciliter l'estimation de la gravité de la violation en termes de risque.

4

Répondre

il convient de déterminer et de mettre en place les mesures techniques ou organisationnelles permettant **de résorber l'incident et de notifier la violation** si cette dernière doit l'être, en fonction du risque engendré ;

5

Tirer les enseignements

le retour d'expérience est maintenant à capitaliser afin **d'empêcher que l'incident se reproduise**. Les lacunes sécuritaires et organisationnelles sont identifiées et il convient de les corriger pour réduire le risque d'incident ou en atténuer les effets le cas échéant. Il convient également de revoir les risques et de mettre à jour les PIA en conséquence.

Vers une propriété sur les données personnelles ?

Les derniers mois ont été l'occasion pour la CNIL de voir réapparaître dans le débat public des positionnements en faveur de l'attribution de droits de propriété sur les données personnelles. La CNIL estime qu'il ne s'agit pas de la voie à suivre car de tels droits ne permettraient aucunement d'accroître le retour vers l'individu de la valeur créée à partir de ses données, et fragiliseraient le cadre historique de protection des données. Elle voit en revanche dans l'application du RGPD une occasion de renforcer les droits d'usage, y compris exercés collectivement, des personnes sur leurs données.

LA PROPRIÉTÉ DES DONNÉES : UNE RÉPONSE À L'ASYMÉTRIE ENTRE LES INDIVIDUS ET CEUX QUI TRAITENT LEURS DONNÉES ?

L'idée d'instituer un droit de propriété sur les données personnelles est revenue dans le débat public. Elle part principalement du constat d'une asymétrie, qui est réelle entre l'individu et ceux qui traitent ses données. Les bases de données personnelles sont au fondement des modèles économiques de nombreux acteurs, au premier rang desquels figurent les géants du Web, et permettent à ceux-ci une création de valeur considérable. L'individu reçoit, en retour, une part de cette création de valeur : il bénéficie par exemple sur l'Internet, grâce à la collecte de ses données personnelles, de services gratuits qui se personnalisent de jour en jour. Mais au vu des profits substantiels réalisés grâce à l'usage de ses données, ce retour sur « investissement » vers l'individu peut raisonnablement apparaître comme insuffisant.

Pour les tenants de cette proposition, la reconnaissance de droits de propriété serait l'une des réponses à cette asymétrie, en permettant aux personnes de ne plus être « dépossédées » de leurs données, d'être pleinement incluses dans la chaine de valeur.

L'idée peut apparaître à bien des égards comme attrayante : chaque individu pourrait se voir rémunéré pour ses données ou choisir celles qu'il souhaite préserver en payant le prix de cette confidentialité. C'est la perspective d'un *empowerment* qui prendrait corps sur une communauté d'individus désormais financièrement intéressés à la gestion de leurs données.

Si l'on peut partager le constat de départ, la réponse à la problématique identifiée ne doit, pour la CNIL, pas passer par l'instauration de droits de propriété.

Une telle proposition serait en effet susceptible de renforcer les déséquilibres économiques au détriment des personnes. D'un point de vue économique tout d'abord, il est douteux que cet instrument puisse réellement déboucher sur un rééquilibrage des rapports de force.

D'abord, très peu de données personnelles, prises à l'échelle individuelle, seraient susceptibles de constituer un actif profitable pour les personnes. La valeur monétaire d'une donnée fournie à un service ne se révèle véritablement que dans son traitement, lorsqu'elle est agrégée à celles d'autres d'utilisateurs.

Surtout, si un « marché de la donnée » parvenait à émerger, l'histoire et la théorie économiques démontrent que la reconnaissance de droits de propriété bénéficierait aux acteurs les plus forts, en l'occurrence ici les « demandeurs » de données, les grands groupes, relativement concentrés, qui voient dans la collecte de données une opportunité immense, et non aux « offreurs » de données, les individus, nombreux et éparpillés. Quel que soit le titulaire initial du droit, le marché permettrait de les attribuer *in fine* aux agents économiques les mieux à mêmes d'en tirer profit. Dès lors, alors que les individus consentent déjà aujourd'hui massivement à l'utilisation de leurs données personnelles, le risque est celui d'une dépossession massive par les personnes de leurs données pour l'accès aux plateformes, sans la contrepartie escomptée en termes de « prise de pouvoir » économique.

Par ailleurs, cette proposition est contraire au cadre historique de protection de données. D'un point de vue plus philosophique, il faut mesurer qu'une telle évolution irait à contre-courant des principes et valeurs qui sous-tendent depuis quarante ans le droit des données personnelles.

> « Cette proposition serait susceptible de renforcer les déséquilibres économiques au détriment des personnes. Elle est aussi contraire au cadre historique de protection des données. »

La loi Informatique et Libertés entendait répondre aux défis posés par l'avènement de l'informatique en consacrant des droits attachés à la personne. Chaque individu doit pouvoir disposer d'une vie privée. La loi repose donc sur un ancrage, qui est une conception éthique et humaniste d'un droit qui se situe à l'essence même de la personne, fondamental pour sa dignité et le libre développement de sa personnalité indépendamment de toute considération marchande.

Dans un univers numérique en expansion, le cadre normatif a d'ailleurs été modifié par la loi du 7 octobre 2016 pour une République numérique afin d'affirmer le principe d'autodétermination informationnelle, clé de lecture visant à donner un contenu plus positif aux grands principes de la loi Informatique et Libertés : « 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. » (art. 1er de la loi du 6 janvier 1978 modifiée).

« La reconnaissance de droits inaliénables sur les données nous concernant est une pierre angulaire du droit européen. »

La reconnaissance de droits inaliénables sur les données nous concernant (droit d'accès, d'opposition, de rectification, etc.), abstraction faite de toute considération de propriété, est donc une pierre angulaire du droit français et du droit européen. Le renforcement de ces droits vise à rendre possible le libre épanouissement de la personne dans cet univers qui se complexifie et dans lequel la donnée circule de plus en plus entre une multitude d'acteurs.

LA PROPRIÉTÉ DES DONNÉES EST PEU COMPATIBLE AVEC L'EXERCICE DES DROITS DES PERSONNES

Enfin, l'approche de la patrimonialisation des données personnelles semble peu compatible avec le plein exercice des droits reconnus aux personnes. Il est peu envisageable, d'un point de vue juridique et opérationnel, de faire coexister une propriété sur les données avec l'approche centrée sur les droits. En effet, la donnée à caractère personnel, dès lors qu'elle est considérée comme étant à l'essence même de la personne, ne peut être librement transférable, soumise aux possibilités de cessibilité et d'expropriation intrinsèques au concept de propriété. Un individu ne serait plus libre dans le choix de l'utilisation de ses données dès lors qu'il les aurait vendues et qu'il ne serait plus en capacité de révoquer son consentement.

En outre, l'attribution de droits de propriété clairement définis et exclusifs sur les données personnelles peut se heurter à la nature même de certaines données : par exemple, les données génétiques (qui ont fait l'objet d'une publication en 2017) sont pluripersonnelles au sens qu'elles concernent aussi ascendants et descendants. Ces données personnelles « embarquent » en quelque sorte des tiers.

La logique de propriété amoindrirait donc les standards généraux de protection des personnes. Les atteintes au droit de propriété étant aujourd'hui strictement encadrées par le droit, la liberté de décider comment disposer de ses données pourrait devenir la règle, la protection des libertés publiques ne devenant plus que l'exception (des principes clés tels que la nécessité de justifier une finalité en amont d'une collecte ou l'existence d'un droit d'opposition seraient inévitablement vidés de leur substance).

« L'approche de la patrimonialisation des données personnelles semble peu compatible avec le plein exercice des droits reconnus aux personnes. »

RENFORCER LES DROITS D'USAGE POUR UN MEILLEUR RETOUR VERS L'INDIVIDU

Un renforcement du cadre juridique actuel, sans en changer les soubassements, peut contribuer à résoudre l'asymétrie de pouvoir soulignée précédemment. Le RGPD constituera une étape importante vers cet objectif.

Le RGPD renforce en effet les droits individuels, d'abord en imposant aux professionnels d'obtenir expressément le consentement des personnes quant à l'utilisation de leurs données, en mettant à leur disposition une information claire, intelligible et aisément accessible. Il s'agit d'un prérequis indispensable pour une plus grande maîtrise, cette disposition correspondant plus aux attentes des citoyens et consommateurs que la promesse illusoire d'un retour monétaire.

En outre, le nouveau droit à la portabilité permettra 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. Grâce à ce droit, une personne pourra reprendre du pouvoir en migrant vers des services moins « prédateurs » de ses données.

Le RGPD annonce plusieurs perspectives novatrices qui permettront de mieux prendre en compte la dimension collective des données personnelles. Les moyens d'action collective sont amenés à être facilités et encouragés. Le Règlement prévoit en effet un droit à réparation pour toute personne ayant subi un dommage matériel ou moral. Le projet de loi relatif à la protection des données personnelles, encore en discussion au Parlement, devrait permettre à l'avenir aux victimes desdits dommages d'obtenir une réparation de leur préjudice au travers d'actions collectives initiées par des acteurs associatifs. Le droit à la portabilité pourrait également à terme être envisagé comme un moyen pour des communautés de personnes de gagner en maîtrise collectivement, en contribuant à des missions d'intérêt général choisies par la mise à disposition de données à des acteurs publics (cette « portabilité citoyenne » constitue l'un des scénarios développés dans le cahier « Innovation et Prospective » publié en 2017 par la CNIL sur la smart city).

Enfin, l'entrée en application du RGPD doit être mise en perspective avec les des actions d'information du public et d'Éducation au numérique conduites par la CNIL depuis plusieurs années aux côtés d'autres acteurs. Faire monter le degré de conscience collective des enjeux numériques permet en effet aux citoyens de mieux exercer leurs droits, et ainsi de contribuer à un rééquilibrage des pouvoirs.

À travers le RGPD, l'Europe a posé les bases d'un cadre qui permettra à chacun de gagner en maîtrise. Il appartient à l'ensemble des parties prenantes – citoyens, responsables de traitement, régulateur – de faire désormais vivre ce cadre pour concrétiser cette évolution.

Plus de **droits** pour vos **données !**

1 Des données à emporter !

Je peux récupérer les données que j'ai communiquées à une plate-forme et les transmettre à une autre (réseau social, fournisseur d'accès à internet, site de streaming, etc.)

2 Plus de transparence

Je bénéficie de plus de lisibilité sur ce qui est fait de mes données et j'exerce mes droits plus facilement (droit d'accès, droit de rectification).

3 Protection des mineurs

Les services en ligne doivent obtenir le consentement des parents des mineurs de moins de 13 ans avant leur inscription.

4 Guichet unique

En cas de problème, je m'adresse à l'autorité de protection des données de mon pays, quelque soit le lieu d'implantation de l'entreprise qui traite mes données.

5 Sanction renforcée

En cas de violation de mes droits, l'entreprise responsable encoure une sanction pouvant s'élever à 4% de son chiffre d'affaires mondial.

Illustration : Martin Vidberg

6 Consécration du droit à l'oubli

Je peux demander à ce qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à ma vie privée.

Nouveau Réglement européen sur la protection des données personnelles

Après quatre années de débats, l'Union européenne a finalisé le projet de règlement sur le protection des données personnelles qui doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Le règlement, qui sera adopté au premier semestre 2016, renforce les droits des citoyens européens et leur donne plus de contrôle sur leurs données personnelles. Il simplifie les formalités pour les entreprises et leur offre un cadre juridique unifié. Il sera applicable en 2018 dans tous les pays de l'UE.

ARTICLE 29 Data Protection Working Party

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

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.

Carina
Responsable de l'éducation au numérique

Le pôle « éducation au numérique » a pour mission de diffuser et promouvoir une « culture citoyenne du numérique » auprès de tous les publics, et notamment des plus jeunes. Pour cela, il s'appuie sur la force de frappe que représente le collectif educnum, composé de têtes de réseaux disposant de relais sur l'ensemble du territoire. Sur le site www.educnum.fr, le pôle valorise les actions du collectif et propose aux enseignants et aux éducateurs des ressources pédagogiques variées (affiches, vidéos, ateliers, fiches pratiques…). Sensibiliser les jeunes, c'est aussi former les « formateurs » : enseignants et cadres de l'éducation nationale, ambassadeurs des droits de l'enfant, community managers des clubs de football qui démultiplient nos messages.

Le pôle interagit également avec près de 60 autorités de protection des données à l'international.

Pour exercer ses missions, le pôle travaille en lien avec différents services de la CNIL : communication, expertise, prospective, service international, juristes… Variété de nos actions, interface avec de nombreux interlocuteurs, sens de la pédagogie, créativité et réactivité rendent notre travail chaque jour passionnant !

L'EFFET RGPD SUR CNIL.FR ET LES RÉSEAUX SOCIAUX

4 454 862
visiteurs sur cnil.fr en 2017

+59%
de visiteurs par rapport à 2016

93
actualités et communiqués publiés en 2017

Le site cnil.fr

Cnil.fr a connu un bond spectaculaire de son audience en 2017 (+59 %). Ce gain de visites s'explique principalement par les consultations des contenus sur le règlement européen sur la protection des données. Site de référence sur le RGPD, une vingtaine de documents ont été mis en ligne sur le sujet durant l'année 2017.
Ils proposent notamment une méthodologie pour se préparer au RGPD, une FAQ en français facilitant la lecture aux non-spécialistes des lignes directrices du G29, des outils pour se mettre en conformité (Outil PIA, modèle de registre).

Une rubrique « Règlement européen » a spécialement été créé pour regrouper ces contenus à destination des professionnels en phase de préparation.

En 2018, une refonte éditoriale plus profonde et la revue de l'intégralité des contenus du site sont prévues pour prendre en compte, dans l'ensemble du site, les nouvelles règles applicables à partir de mai 2018.
Le site de la CNIL est également plébiscité par les particuliers en recherche de conseils et de bonnes pratiques pour maîtriser leur vie privée ou leur e-réputation. Les conseils de la CNIL pour la création d'un bon mot de passe est d'ailleurs l'article le plus lu du site pour l'année 2017 (53 412 visites).

Quelques chiffres sur les statistiques du site cnil.fr

Le top 3 des actualités les plus consultés publiées en 2017 :

« Les conseils de la CNIL pour un bon mot de passe / 27-janv-17 »
53 412
consultations

« Comment se préparer au règlement européen sur la protection des données ? / 15-mars-17 »
35 989
consultations

« Règlement européen sur la protection des données : un guide pour accompagner les sous-traitants / 29-sept-17 »
16 195
consultations

Le top 3 des communiqués les plus consultés publiés en 2017 :

« Éthique et numérique : les algorithmes en débat / 23-janv-17 »
14 280
consultations

« Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers / 27-janv-17 »
12 212
consultations

« Facebook sanctionné pour de nombreux manquements à la loi informatique et libertés / 16-mai-17 »
11 926
consultations

Le top 3 des documents les plus téléchargés en 2017 :

« Se préparer en 6 étapes »
17 158
consultations

« Modèle de registre »
15 422
consultations

« Modèle de fiche à porter au registre »
10 286
consultations

FOCUS

Educnum

96 163
visiteurs

LINC

57 775
visiteurs
(+ 20 000 visiteurs)

Les réseaux sociaux

La taille de la communauté @CNIL* sur Twitter a atteint les 100 000 followers alors même que le mot RGPD ne cesse de prendre de l'importance dans les conversations. Cette année, ce sont surtout les professionnels qui ont interpellé la CNIL sur les réseaux sociaux. Parmi leurs préoccupations, les moyens à mettre en œuvre pour assurer la conformité de leur entreprise ou de leur association. La CNIL a donc fait appel au youtuber CookieConnecté pour expliquer les changements qu'implique cette nouvelle réglementation.

Sa vidéo s'est très vite classée en tête de visionnage des contenus RGPD sur YouTube !**

***Nombre de followers au 20/02**

93 500
CNIL

1 500
CNIL version anglaise

2 600
LinCNIL

2 100
Educnum

28 385
fans

18 360
abonnés sur LinkedIN

**** : le visionnage de cette vidéo a atteint 10 000 vues en 2 semaines (TOP 3) ce qui en fera certainement la plus vue sur le thème RGPD dans quelques semaines.**

La CNIL partenaire de l'exposition Terra Data

Pour la première fois, la Cité des sciences a organisé, du 4 avril 2017 au 7 janvier 2018, une exposition intereactive autour des données, « Terra Data, nos vies à l'ère du numérique ». À l'ère du big data, des algorithmes et des réseaux, il s'agissait, dans une démarche pédagogique et interactive, de donner les clés de déchiffrement du monde numérique qui est en train de se bâtir.
Un parcours de découverte original, avait été conçu autour de quatre temps :

- Les données, qu'est-ce que c'est ?
- Les données, comment les traite-t-on ?
- Les données, qu'est-ce que ça change ?
- Les données, où ça nous mène ?

L'exposition a rencontré un vif succès avec près de **165 000 visiteurs**. Les ateliers de médiation organisés au sein de l'exposition ont permis à près de 7 000 visiteurs et notamment à de nombreuses classes d'enrichir leurs connaissances du sujet. Une itinérance de l'exposition est envisagée.

La CNIL, en tant que régulateur des données personnelles, a été associée dès la conception de cette exposition. Elle a ainsi participé au comité scientifique et culturel et apporté son conseil juridique pour la mise en place d'un suivi du parcours du visiteur via le wifi et la reconnaissance faciale.

Elle a également mis à disposition plusieurs ressources parmi lesquels le dispositif multimédia sur les droits Informatique et Libertés et son application cookieviz (qui permet de visualiser en temps réel le dépôt et la lecture des cookies) et contribué à la conception d'une frise chronologique graphique qui retrace la numérisation croissante des activités et rappelle les enjeux clés pour les libertés et la vie privée.

Enfin, la CNIL a participé à différentes manifestations en marge de l'exposition et notamment à une projection débat intitulée « Big data et recommandations : menace ou opportunité ? » le 30 mai à la Cité des sciences et de l'industrie.

INFOSPLUS

Le service Besoin d'aide ? en 2017

513 Questions/Réponses publiées

178 974 Consultations des Questions/Réponses

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

- Comment faire une déclaration à la CNIL ?
- Faut-il déclarer un site web à la CNIL ?
- Opt-in, opt-out, ça veut dire quoi ?
- Ma dette est forclose et je suis toujours fiché au FICP (Fichier national des Incidents de remboursement des crédits). Que peut faire la CNIL ?
- Une demande d'autorisation, c'est quoi ?
- Règlement européen sur la protection des données : que faut-il savoir ?
- Mentions légales sur un site internet, est-ce obligatoire ?
- Déclarer à la CNIL, c'est obligatoire ?
- La CNIL, c'est quoi ?
- Comment faire supprimer des informations me concernant diffusées sur internet ?

LES RÉPONSES AUX PUBLICS

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

En 2017, le volume d'activité du service s'est fortement accru. Les usagers privilégient de plus en plus l'envoi de leurs demandes par voie électronique démontrant ainsi que le service « Besoin d'aide », disponible 24h/24 sur www.cnil.fr, répond véritablement à leurs besoins et attentes.

La CNIL a notamment optimisé le référencement des Questions/Réponses du service en ligne « Besoin d'aide » par les moteurs de recherche. En effet, le langage, moins institutionnel et plus courant, utilisé par ce service permet de faire venir sur le site de la CNIL des publics qui s'intéressent à des sujets de protection des données mais ne connaissent pas ou n'identifient pas nécessairement la CNIL.

Il est à noter que pour la première fois, on constate une hausse significative (+21 %) des sollicitations reçues par voie électronique alors que le nombre d'appels téléphoniques adressés à la Commission a baissé (-16,3 %). Ceci résulte de la mise en place d'un nouveau serveur vocal interactif en octobre 2017 qui organise l'accès direct aux permanences sectorielles (santé, international, CIL).

Cette modification a ainsi permis de limiter les réitérations d'appels et de faire diminuer le temps d'attente au téléphone, renforçant la qualité du service rendu par la CNIL à ses usagers.

Le courrier postal continue sa baisse, régulière depuis 2015.

17 231
courriers postaux

155 281
appels reçus
(-6,8 % par rapport à 2016)

67 128
appels pour la permanence téléphonique
(-16,3 % par rapport à 2016)

14 701
requêtes reçues par voie électronique
(+21 % par rapport à 2016)

12 500
Téléchargements pour la liste article 31

Anticiper le RGPD

De nombreuses Questions/Réponses dédiées au RGPD sont disponibles dans Besoin d'aide.
Depuis août 2017, la liste des traitements déclarés à la CNIL (article 31) est en ligne pour répondre aux très nombreuses demandes des professionnels désireux de cartographier leurs traitements de données et de préparer ainsi leur mise en conformité avec les dispositions du RGPD.

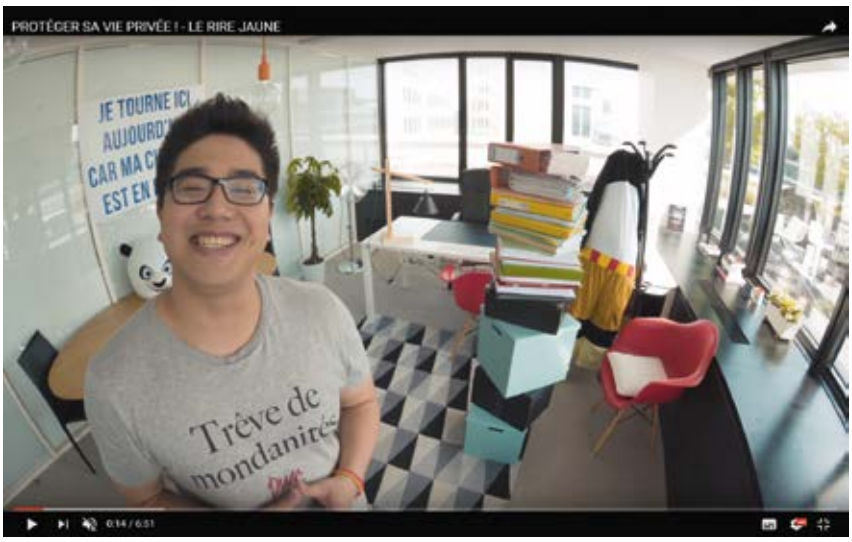
DES RESSOURCES PÉDAGOGIQUES POUR LES JEUNES PUBLICS

Les plus jeunes sont nés avec le numérique et en maîtrisent plutôt bien les usages mais ils ne sont pas toujours conscients des conséquences que peuvent avoir leurs publications en ligne sur leur vie d'adulte ou sur celle des autres. C'est pourquoi il est essentiel de les sensibiliser à l'importance d'adopter les bons réflexes pour protéger leur vie privée en ligne et celle d'autrui. Dans le cadre de sa mission d'éducation au numérique, la CNIL a choisi de développer en 2017 des actions et des contenus plus spécifiquement en direction des publics jeunes.

Sensibiliser les jeunes à la protection de leur vie privée en ligne

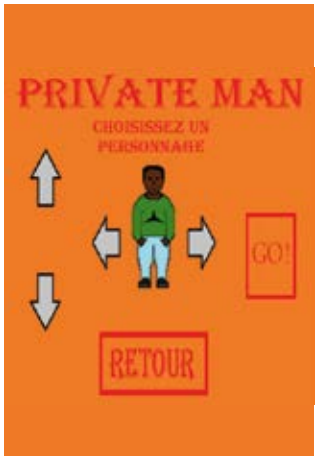
En 2017, la CNIL, en partenariat avec la MGEN, a réalisé une vidéo avec le Youtubeur Le Rire Jaune. Intitulée « Protéger sa vie privée en 6 étapes », la vidéo illustre de façon décalée et humoristique différents moyens de protéger ses données et sa vie privée sur internet : créer des mots de passe robustes, bien vérifier la confidentialité des contenus postés sur les réseaux, séparer les contenus professionnels des contenus plus personnels... le Rire Jaune fait passer de façon simple des messages clés, essentiels à une bonne utilisation d'Internet. La vidéo a rencontré un grand succès, puisqu'elle a enregistré près de 4 millions de vues. Cette action a été soutenue par le collectif EDUCNUM.

La CNIL a actualisé et réédité le quiz Les Incollables, « Ta vie privée, c'est secret », qui permet à chacun de tester ses connaissances sur les questions clés liées au numérique et aux données personnelles. Le quiz a été envoyé à tous les centres de documentation et d'information des collèges à la rentrée scolaire de septembre 2017, avec l'aide du ministère de l'Éducation nationale. Un module web a également été réalisé.



Les Trophées EDUCNUM

La CNIL et le Collectif ont lancé, en novembre 2016, la 3ème édition des Trophées EDUCNUM.
Les étudiants de 18 à 25 ans ont proposé des projets pédagogiques pour sensibiliser les collégiens (10-14 ans) aux bons usages du web. Le concours a bénéficié une nouvelle fois du soutien du ministère de l'Éducation nationale. France Télévisions et France TV éducation ont relayé la communication sur le concours, via leurs sites et leurs réseaux sociaux. Le Grand prix du jury a été attribué à des étudiants en Master « Propriété intellectuelle et droit du numérique » à l'université Paris Sud, pour un livre-jeu « *Defeat the hacker* » destiné à sensibiliser les collégiens aux bons usages d'Internet.

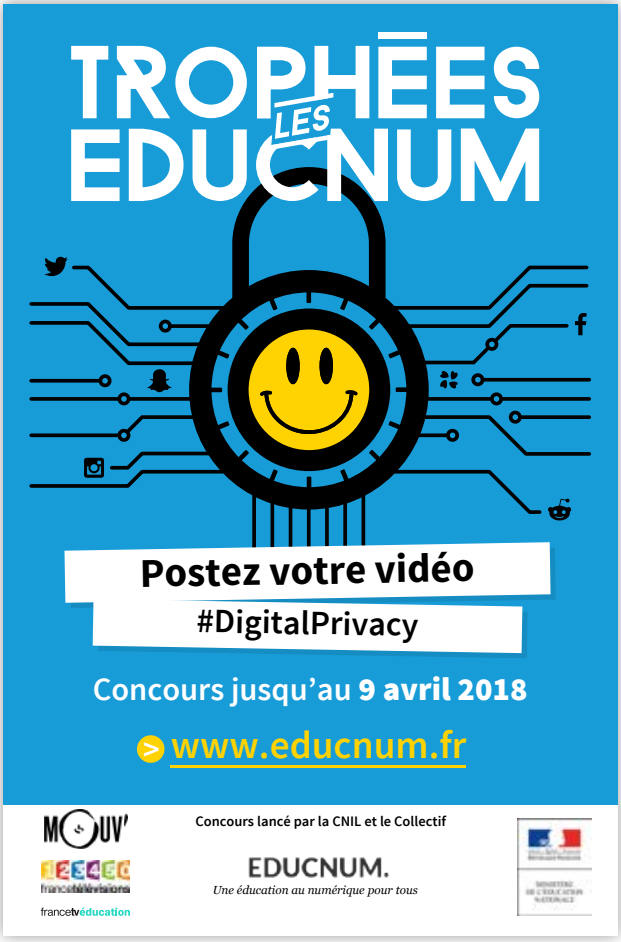


Le Prix Coup de cœur du jury a été attribué à un étudiant en BTS « Services informatiques aux Organisations » au lycée Simone Weil de Saint Priest en Jarez, pour « *Privateman* », une application sous forme de jeu vidéo mettant en scène un super héros chargé de protéger la vie privée des utilisateurs sur Internet.

En plus de la dotation financière qui leur a été allouée, les lauréats ont bénéficié d'une aide pour diffuser et faire connaître leur projet : l'Association AXA Prévention a mis en relation les lauréats du Grand Prix du jury avec les éditions Michel Lafon, pour étudier la faisabilité d'une large diffusion ; le ministère de l'éducation nationale a valorisé le Prix coup de cœur « *Privateman* » sur son site eduscol et ses réseaux sociaux.

La cérémonie de remise des prix a eu lieu à la Cité des Sciences et de l'Industrie le 15 juin 2017 et a été suivie d'une visite privée de l'exposition « Terra Data, nos vies à l'ère du numérique ».

De plus, la CNIL, le ministère de l'Éducation nationale et la MGEN ont organisé la 3ème édition des Trophées des classes « pour un usage responsable d'Internet ».



Des classes du 1er et du second degré ont proposé des projets sur l'un des trois sujets du concours : respect des droits des personnes, protection de la vie privée, traces laissées sur Internet, vérification des sources.

Le référentiel international de formation des élèves à la protection de la vie privée

La CNIL a poursuivi les travaux engagés avec le ministère de l'éducation nationale et l'association Savoir Devenir, spécialisée en expertise pédagogique, afin de décliner le référentiel par types de ressources et tranches d'âge à intégrer dans les programmes scolaires.

Des expérimentations en classe ont permis de tester le référentiel dans des séquences pédagogiques sur les thématiques des droits et devoirs sur Internet, la traçabilité et la sécurité lors de la navigation sur le web ou encore la lutte contre le cyber-harcèlement.

À l'occasion du *Safer Internet Day* en février 2017, les retours très positifs des écoles ayant utilisé le référentiel pour structurer la réflexion sur ces nombreuses thématiques de la protection des données constituent un réel encouragement pour la CNIL et ses homologues internationaux à continuer de produire en 2018, des scénarios pédagogiques de cours tout comme à illustrer des cas concrets d'apprentissage des compétences du référentiel mixées avec d'autres matières et pratiques quotidiennes de classes.

La déclinaison du référentiel s'est poursuivie en coopération avec les partenaires éducatifs en France comme dans d'autres pays, qui ont dégagé des moyens humains et financiers à cet effet (des outils en ligne sont en cours de développement pour faciliter l'accès par les enseignants au référentiel).

Le référentiel a par ailleurs été traduit dans six autres langues, Albanais, Catalan, Espagnol, Hongrois, Italien et Polonais, en plus du français et de l'anglais.

PROTÉGER
les citoyens

La CNIL continue à recevoir via son service de plaintes en ligne un nombre croissant de plaintes pour non-respect de la loi Informatique et Libertés. C'est un nombre record pour 2017, car la barre des 8 000 plaintes a été franchie avec 8 360 plaintes reçues.
Le plus souvent, la CNIL intervient auprès du responsable du fichier pour l'informer des faits portés à sa connaissance (manquement soulevé par le plaignant) et des textes applicables, afin qu'il se mette en conformité et respecte les droits des personnes. Les plaintes les moins complexes font l'objet d'un traitement rapide par le service de relations avec le public. Les plaintes plus complexes, nécessitant souvent plusieurs actes d'instruction auprès des responsables de fichiers, sont orientées vers le service des plaintes.

Névine
Juriste au service des plaintes

Je traite avec mes collègues les plaintes reçues par la CNIL en matière de protection des données personnelles sur le secteur Travail - Social – Santé - Éducation - Transport. Nos domaines d'intervention concernent notamment des questions portant sur la collecte et le traitement des données personnelles des employés, des patients, des élèves, des usagers d'associations ou d'administrations à vocation sociale et des usagers des transports.

Nous rappelons aux organismes la législation applicable et, en particulier, les droits (droits d'accès, d'opposition et de rectification) des personnes concernées par des traitements tels que les fichiers de recrutement, les dossiers médicaux, les dispositifs de vidéosurveillance, de géolocalisation, de biométrie, d'écoute et d'enregistrement des appels téléphoniques, etc.

Les plaintes adressées à la CNIL en la matière révèlent régulièrement une méconnaissance de la loi Informatique et Libertés par les structures dépourvues de services juridiques et de Correspondant Informatique et Libertés. Il arrive que des responsables de fichiers ne respectent pas le cadre fixé par la loi en filmant de manière permanente des employés à leur poste de travail, ou en ne sécurisant pas suffisamment les données qu'ils traitent.

Dans nos courriers d'instruction nous rappelons les règles applicables et les bonnes pratiques. Nous participons ponctuellement aux opérations de contrôles en ligne, sur place ou sur audition des organismes mis en cause et proposons des mesures correctrices.

EN 2017, LA CNIL A REÇU 8 360 PLAINTES : UN NOMBRE RECORD

- **1 580 plaintes peu complexes** ont fait l'objet d'un traitement rapide par le service des relations avec les publics (SRP).

Par cette voie, les plaignants ont obtenu une réponse rapide à leur demande, portant notamment sur :

- les droits et obligations résultant de la loi Informatique et Libertés ;
- les modalités d'exercice des droits et les démarches préalables requises ;
- l'orientation vers les organismes à même de répondre au mieux à la demande ;
- l'information sur des procédures judiciaires pendantes.

- **6 780 plaintes plus complexes** sont orientées vers le service des plaintes et font l'objet d'une instruction plus poussée. Dans ce cas, plusieurs échanges peuvent avoir lieu avec le responsable des fichiers. Dans certains cas, des contrôles peuvent être décidés, suivis éventuellement d'une mise en demeure ou d'une sanction.

Cette année, les plaintes concernent principalement les secteurs internet/téléphonie et commerce qui représentent à eux deux 52 % des plaintes reçues.

- **27 % des plaintes concernent la diffusion de données sur internet**

Les demandes de suppression de données et de contenus diffusés sur internet (nom, coordonnées, commentaires, photos, vidéos, comptes etc.) restent importantes, ce qui traduit une préoccupation majeure du public. Pour exercer ses droits, l'internaute doit d'abord s'adresser au responsable du site pour demander la suppression des informations. Ce n'est qu'en cas de refus ou d'absence de réponse que la CNIL peut intervenir.

En 2017, la CNIL a reçu **335 demandes de déréférencement**. Cette procédure, couramment appelée « droit à l'oubli », permet de demander à un moteur de recherche de supprimer certains résultats de recherche associés à ses nom et prénom. Le moteur de recherche peut refuser de donner une suite favorable à ces demandes s'il considère que l'intérêt des internautes à disposer de cette information est prépondérant. Il est possible de contester le refus du moteur de recherche auprès de la CNIL.

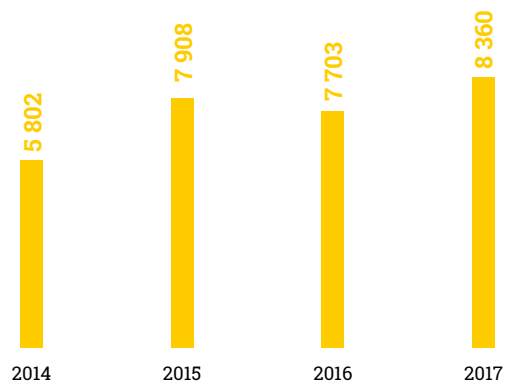
Pour apprécier le bien-fondé d'une demande, la CNIL met en balance les droits fondamentaux de la personne avec l'intérêt du public à avoir accès au contenu à partir des nom et prénom du plaignant. La CNIL prend notamment en compte le caractère récent du contenu en cause, sa pertinence, son caractère exact, journalistique ou légal et le rôle joué par la personne dans la vie publique.

Histoire vécue...

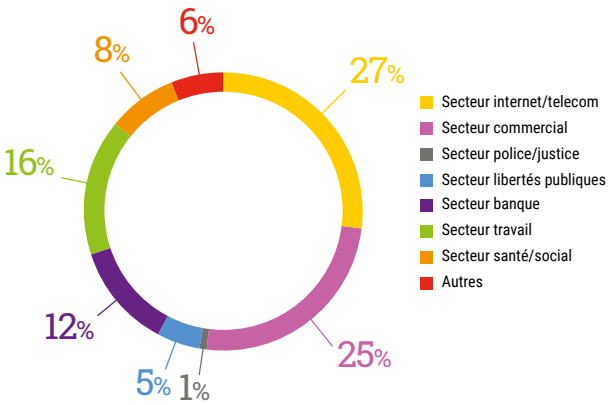
LA MAMAN DE ZOÉ a saisi la CNIL pour obtenir la suppression d'une vidéo dans laquelle sa fille mineure apparaissait. Elle a contacté le site diffusant la vidéo sans succès. Après intervention de la CNIL, le site a procédé à la suppression de la vidéo.

JULIE a contacté la CNIL pour contester le refus d'un moteur de recherche de supprimer plusieurs résultats associés à ses nom et prénom, qui renvoient vers des sites américains diffusant des photos anthropométriques (« Mugshot ») et des informations concernant des arrestations. Ces sites ne précisent pas les faits à l'origine des arrestations. Or, Julie avait été arrêtée pour un simple problème de visa ne relevant pas de sa responsabilité et qui avait été rapidement résolu.
Le moteur de recherche avait refusé le déréférencement, considérant que les informations concernaient des infractions pénales et qu'aucun élément n'attestait qu'elles étaient inexactes ou obsolètes.
La CNIL est intervenue auprès du moteur de recherche car les informations publiées ne participaient à aucun débat d'intérêt général. Julie n'est pas une personne publique et l'association de ces résultats de recherche à ses nom et prénom lui causait un fort préjudice. De plus, Julie ne pouvait pas exercer son droit d'opposition auprès des sites sources, hébergés aux États Unis. Face à ces arguments, le moteur de recherche a accepté de revenir sur son refus et de procéder au déréférencement des liens hypertextes.

Évolution du nombre de plaintes depuis 2014



Répartition des plaintes par secteur d'activité 2017



- **25 % des plaintes concernent le secteur commerce/marketing**

Le secteur commerce/marketing reste l'un des plus concernés par les plaintes, notamment pour la prospection commerciale par courriel, téléphone ou voie postale.

Pour agir plus efficacement contre le spam, la CNIL a changé ses méthodes d'instruction et renforcé sa collaboration avec l'association Signal spam.

L'instruction au cas par cas des plaintes ne donnant pas de résultats satisfaisants, la CNIL est passée à un traitement collectif fondé sur la centralisation des signalements auprès de la plateforme Signal spam (https://www.signal-spam.fr/) afin d'avoir une vision plus globale du phénomène. Ce nouveau dispositif permet à la CNIL de mieux identifier les principaux organismes à l'origine de ces spams pour mener des actions de contrôle et des actions répressives ciblées. Aidez-nous à lutter contre le spam en les signalant auprès de la plateforme Signal spam (https://www.signal-spam.fr/) !

Histoire vécue...

MARIE souhaite commander une table sur un site de vente en ligne. Lorsqu'elle se rend sur son compte client, elle s'aperçoit que, bien qu'elle soit une cliente fidèle, elle n'a pas acheté tous les articles qui s'affichent dans son compte. Elle remarque aussi que ces articles n'ont pas été livrés à Lyon, la ville où elle réside, mais à Lille. Marie contacte alors le site de vente en ligne pour faire part de son étonnement et demander la rectification de ces informations erronées, mais elle ne reçoit aucune réponse. Marie saisit la CNIL, qui décide de mener un contrôle sur le site concerné. La CNIL constate que deux comptes clients ont été mélangés et que les commandes d'une tierce personne ont été associées au compte client de Marie. La CNIL met alors la société en demeure de rectifier ces informations et d'assurer la sécurité et la confidentialité des données de ses clients. Cette mise en demeure a été clôturée à la suite d'une mise en conformité de la société concernée.

Outre la publicité, les motifs de plainte auprès de la CNIL sur ce secteur sont variés : conservation des coordonnées bancaires, accès au dossier client, enregistrement de données relatives aux clients non pertinentes ou excessives, défaut de confidentialité des données, jouets connectés, etc.

- **16 % des plaintes concernent les ressources humaines**

Le nombre de plaintes reçues sur le secteur travail/ressources humaines augmente (+ 2 % par rapport à 2016). Les demandes émanent de salariés, de syndicats ou d'inspecteurs du travail. Elles concernent principalement par ordre décroissant les dispositifs de vidéo, de géolocalisation, l'accès au dossier professionnel, la messagerie professionnelle et la sécurité des données.

Histoires vécues...

PASCAL a changé d'employeur depuis 8 mois mais constate que son ancienne messagerie professionnelle est toujours active. Après intervention de la CNIL, la messagerie électronique de Pascal a été fermée et la société a mis en place une procédure automatique informant l'expéditeur du message que le salarié est parti et l'invitant à contacter la société via une autre adresse électronique.

Dans la cadre du plan d'urgence sanitaire et de crise dit « plan blanc » (attentat, crash, épidémie), le personnel hospitalier doit pouvoir être mobilisé pour la mise en place de cellules de crise. Afin de pouvoir être contactée, **LEÏLA** a communiqué, comme tous ses collègues hospitaliers, ses coordonnées aux ressources humaines pour alimenter le fichier « Plan blanc ». Cependant, elle constate rapidement que ses coordonnées téléphoniques sont utilisées par le centre hospitalier pour l'appeler pendant ses heures de repos afin de lui demander de remplacer des collègues absents. Leïla sollicite en vain la suppression de son numéro de portable de son dossier professionnel. Après intervention de la CNIL, son numéro de téléphone a été strictement cantonné au fichier « Plan blanc » et supprimé de son dossier professionnel.

- **12 % des plaintes concernent le secteur banque/crédit**

Les plaintes sur le secteur bancaire/crédit ont augmenté de 3 % par rapport à 2016. Il s'agit principalement de contestations d'inscription ou d'absences de levée d'inscription au fichier des incidents de crédit et de paiement (FICP) ou au fichier central des chèques (FCC).

Histoire vécue...

GISLAINE saisit le tribunal d'instance pour contester le bien-fondé de son inscription au FICP. Le tribunal juge cette inscription illégale et ordonne la levée de l'inscription. Or, l'établissement bancaire ne s'exécute pas.
L'intervention de la CNIL auprès de l'établissement a finalement permis une prise en compte du jugement et une levée de l'inscription de Gislaine au FICP.

- **8 % des plaintes concernent le secteur santé/social**

Les plaintes sur le secteur santé/social ont augmenté et représentent cette année 8 % des plaintes (+ 5 %). Le plus souvent les personnes ne parviennent pas à obtenir l'accès à leur dossier personnel (dossier médical, dossier CAF, Pôle emploi, etc.).

Histoire vécue...

Malgré ses demandes répétées, **MARYSE** n'arrive pas à accéder à son dossier dentaire afin de poursuivre ses soins en province. L'intervention de la CNIL auprès du dentiste lui a permis d'obtenir une copie des éléments qu'elle demandait à son ancien dentiste.

- **5 % des plaintes concernent le secteur libertés publiques/collectivités**

De nombreuses plaintes reçues en 2017 sur ce secteur sont directement liées aux élections législatives et présidentielles. La CNIL a reçu 673 sollicitations, dont 131 plaintes relatives à l'absence de prise en compte du droit d'opposition exercé par le plaignant (désinscription non valide), à la réception de messages de prospection politique non désirés (courriels, automates d'appels, appels téléphoniques), aux difficultés relatives à l'exercice du droit d'accès, à l'utilisation détournée de fichiers d'associations et aux défauts de sécurité. En 2017, la CNIL a également reçu une centaine de plaintes relatives à des demandes d'opposition concernant des articles de **presse** (retrait de l'article, anonymisation, désindexation).

Les personnes rencontrent des difficultés à exercer leur droit d'opposition auprès des organes de presse (absence de réponse, refus non motivé, etc.). La CNIL rappelle régulièrement aux organes de presse qui sont saisis de telles demandes qu'ils peuvent le cas échéant refuser la demande mais doivent motiver leur refus.

Histoire vécue...

Il y a 8 ans, **TOM** s'est retrouvé impliqué dans un accident qui a fait l'objet d'un article dans la presse régionale. Cet article disponible, à la saisie de ses nom et prénom, dans les archives web du journal, lui porte préjudice dans ses recherches d'emploi. Il demande au journal la suppression de l'article mais sa demande reste sans réponse. Tom saisit la CNIL qui relaie sa demande et obtient l'anonymisation de l'article.

La CNIL a reçu deux plaintes portant sur l'impossibilité de s'opposer à la numérisation de la prise d'empreintes digitales pour la carte nationale d'identité, alors que cette possibilité est prévue par le décret du 9 mai 2017 relatif aux « titres électroniques sécurisés ». Interrogé sur ce point, le ministère de l'Intérieur a indiqué que les demandes de titres avaient été faites peu de temps après la parution du décret et que depuis une circulaire avait été diffusée pour rappeler cette possibilité et préposer des formulaires de recueillir l'opposition.

FOCUS

Les compteurs communicants

De nombreuses personnes, associations et maires ont saisi la CNIL de plaintes relatives aux compteurs communicants d'électricité, faisant état de leurs inquiétudes quant aux risques d'atteinte à la vie privée liés au déploiement des compteurs Linky.

La CNIL suit ce sujet avec attention depuis de nombreuses années. Elle a émis des recommandations concernant les traitements des données de consommation détaillées collectées par les compteurs communicants, les 15 novembre 2012 et 30 novembre 2015. Afin d'accompagner les acteurs du secteur, la CNIL a également élaboré un Pack de conformité sur les compteurs communicants (édition mai 2014).

Par ailleurs, afin de vérifier la conformité de ces traitements à la loi Informatique et Libertés, des contrôles ont été menés en 2016. Ces investigations ont conduit la CNIL à publier sur son site en novembre 2017 un communiqué intitulé « Linky, Gazpar : quelles données sont collectées et transmises par les compteurs communicants ? ».

Ce communiqué répond aux principales interrogations des particuliers, associations, maires sur les mesures prévues pour garantir la maîtrise des données sur les compteurs communicants. La généralisation de ces compteurs résulte d'une obligation légale de modernisation des réseaux qui répond à des directives européennes. Certaines données sont collectées par défaut (consommation globale du foyer sur une journée). D'autres le sont après accord de l'abonné (la collecte de données de consommation fines). L'accès aux données de consommation par le consommateur s'effectue dans son espace sécurisé accessible sur internet.

La CNIL reste vigilante sur le respect effectif de ces principes.

40 ans !

136 **plaintes en 1981**

478 **plaintes en 1988**

2 671 **plaintes en 1998**

8 360 **plaintes en 2017**

LE DROIT D'ACCÈS INDIRECT : UN NOUVEL INFLÉCHISSEMENT DU NOMBRE DE DEMANDES SANS DOUTE PROVISOIRE

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.

4 039 personnes se sont adressées à la CNIL en 2017 pour exercer leur droit d'accès indirect, ce qui confirme, pour la seconde année consécutive, l'infléchissement de la progression des demandes en ce domaine. Cette évolution s'explique par la conjonction de plusieurs facteurs :

- la mise en place en 2016 d'un droit d'accès direct des héritiers au fichier FICOBA (fichier des comptes bancaires et assimilés) de l'administration fiscale dans le cadre des successions. Le nombre de demandes de droit d'accès indirect à ce fichier, formulées par les particuliers pour l'obtention des données relatives à l'identification de leurs propres comptes, n'en demeure pas moins important (1 729 en 2017) ;
- la modification en décembre 2016 de l'article R.40.29 du code de procédure pénale afin de permettre aux services de police français d'échanger des informations, issues du Traitement d'Antécédents Judiciaires (TAJ), avec les services de police étrangers dans le cadre d'enquêtes administratives pour l'accès à certains emplois (sécurité privée...). Ces échanges sont depuis lors mis en œuvre avec les autorités suisses, par l'intermédiaire du centre de coopération policière et douanière de Genève. Ils ont permis de réduire progressivement, au cours de l'année 2017, le nombre de demandes de droit d'accès indirect à ce fichier émanant de ressortissants français souhaitant travailler dans ce pays qui s'étaient vus imposer cette démarche préalable auprès de la CNIL pour garantir la recevabilité de leur candidature ;
- le nombre plus restreint de mesures (assignations à résidence, perquisitions administratives...) dans le cadre des prolongations successives de l'état d'urgence jusqu'au 1er novembre 2017.

Cette évolution ne préjuge nullement de l'avenir, **compte tenu de l'élargissement constant du périmètre des enquêtes administratives s'appuyant sur la consultation de fichiers soumis au droit d'accès indirect,** tels que le TAJ.

Ainsi, les dispositions réglementaires portant sur le dispositif dit **« grands évènements »** (compétitions sportives, conférences internationales...) prévues par l'article L. L211-11-1 du code de la sécurité intérieure, ont été adoptées le 20 avril 2017, après avis de la CNIL.

4 039

demandes de droit d'accès indirect

7 170

vérifications à mener

8 297

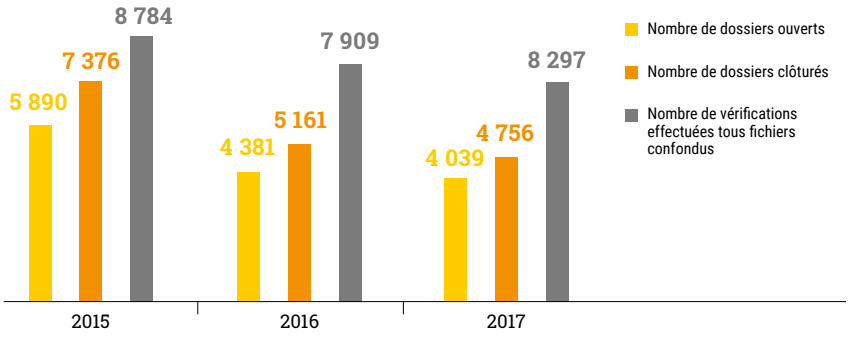
vérifications effectuées (soit + 4,90 %)

INFOSPLUS

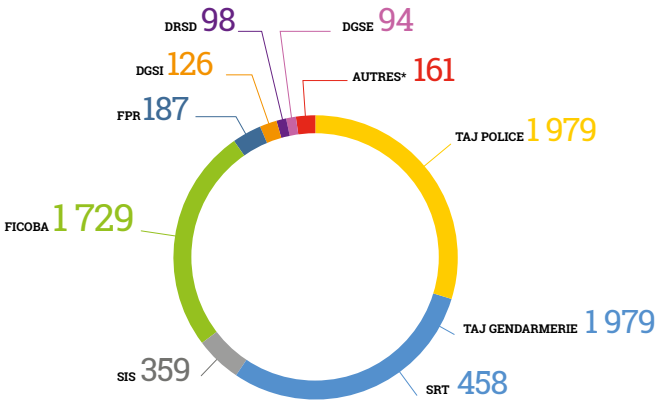
Le droit d'accès indirect comment ça marche ?

À réception de la demande accompagnée d'une copie d'un titre d'identité, un magistrat de la CNIL appartenant ou ayant appartenu au Conseil d'État, à la Cour de Cassation ou à la Cour des Comptes est désigné pour mener les investigations utiles et faire procéder, le cas échéant, aux modifications nécessaires. Les données peuvent ensuite être portées à la connaissance de la personne concernée si, en accord avec l'administration gestionnaire, cette communication n'est pas de nature à nuire à la finalité du fichier, la sûreté de l'État, la défense ou la sécurité publique.

Évolution des demandes de droit d'accès indirect 2015/2017



Demandes de droit d'accès indirect 2017 : 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...

Toute personne autre qu'un spectateur ou un participant (technicien, fournisseur, prestataire de services, journaliste, sponsor, etc.) souhaitant accéder à un établissement ou une installation accueillant un tel évènement, désigné par décret, est soumis à une enquête administrative tendant à assurer que son comportement ou ses agissements ne sont pas de nature à porter atteinte à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'État.

Récemment mis en place à l'occasion du sommet international sur le climat du 12 décembre 2017, ce dispositif a notamment vocation à pleinement s'appliquer lors des jeux olympiques de 2024. Les enquêtes sont menées par le nouveau service national d'enquêtes administratives de sécurité (SNEAS) institué en 2017, qui est également compétent pour les enquêtes relatives à certains personnels ou candidats à l'embauche de transport public ou de transport de marchandises dangereuses.

L'année 2017 a également vu la création, auprès du directeur général de la gendarmerie nationale, d'un service à compétence nationale, dénommé **COSSEN** (commandement spécialisé pour la sécurité nucléaire). Ce service est chargé des enquêtes administratives pour la sphère du nucléaire, qui étaient précédemment réparties entre, d'une part, les préfets de département et, d'autre part, la direction de la sécurité du Commissariat à l'Énergie Atomique (CEA).

Les **4 039 demandes reçues** au cours de l'année 2017 représentent un total de **7 170 vérifications** à mener dans un ou plusieurs fichiers soumis à ce régime particulier d'accès pour répondre aux attentes exprimées par les personnes.

La diminution du nombre de demandes en 2017 a été sans effet sur le nombre de vérifications menées par les magistrats de la CNIL en charge du droit d'accès indirect : 8 297 vérifications de fichiers ont ainsi été menées au cours de l'année 2017, portant principalement sur le Traitement d'Antécédents Judiciaires (59 %).

Le rythme des vérifications auprès des services de police et de gendarmerie s'est particulièrement intensifié afin de respecter les délais fixés par l'article 87-1 du décret n°2005-1309 du 20 octobre 2005, c'est-à-dire d'assurer le traitement de toute nouvelle demande dans un délai moyen de 6 mois et de procéder, dans les meilleurs délais possibles, à l'apurement des demandes plus anciennes.

40 ans !

30
demandes en 1980

70
demandes en 1988

401
demandes en 1998

4 039
demandes en 2017

Les demandes d'accès au fichier TAJ

L'ensemble des vérifications menées en 2017 pour les procédures établies par la police nationale s'est traduit par :

- la suppression de 17 % des fiches examinées concernant des personnes mises en cause ;
- la mise à jour par mention des suites judiciaires favorables intervenues dans 18 % 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).

1 979

demandes d'accès au TAJ

La proportion d'effacements ou de mises à jour demeure toujours plus importante pour les personnes enregistrées dans le fichier par la gendarmerie nationale car les personnes sont enregistrées pour un nombre moins important d'affaires et l'obtention de réponses de la part des procureurs de la République sur les suites judiciaires intervenues en est facilitée.

Le pourcentage de fiches supprimées progresse en 2017 tant pour la police (2 %) que la gendarmerie nationales (9 %). Cela trouve notamment son origine dans la faculté désormais ouverte aux procureurs de la République de prescrire l'effacement de faits ayant bénéficié d'une décision de classement sans suite, quel qu'en soit le motif (article 230-8 du code de procédure pénale modifié par la loi n° 2016-731 du 3 juin 2016 pour tenir compte des incidences de la condamnation de la France par la Cour européenne des droits de l'homme).

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	2 831	2 087
Nombre de personnes inconnues	601	1 295
Nombre de personnes enregistrées uniquement en tant que victimes	485	271
Nombre de fiches de personnes « mises en cause » vérifiées	1 745	521
- dont pourcentage de fiches supprimées	17	25
- 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)*	18	34
- 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)*	64,5	40,5

À SUIVRE

Perspectives d'extension des possibilités d'effacement anticipé du Traitement d'Antécédents Judiciaires (TAJ)

Les conditions d'effacement du Traitement d'Antécédents Judiciaires (TAJ), avant le terme du délai de conservation, sont strictement définies par l'article 230-8 du code de procédure pénale. Seule l'obtention d'une décision judiciaire favorable (jugement d'acquittement ou de relaxe, ordonnance de non-lieu, décisions de classement sans suite), peut actuellement permettre aux personnes d'obtenir un effacement des faits concernés sous réserve de l'accord du procureur de la République territorialement compétent ou, si les infractions ont été commises dans plusieurs ressorts territoriaux, du magistrat référent en charge de ce fichier.

À la suite de la condamnation de la France par la Cour européenne des droits de l'homme en septembre 2014, cet article a connu une modification d'importance en juin 2016 afin de permettre l'effacement des faits pour toutes les décisions de classement sans suite (rappel à la loi, injonction thérapeutique, dédommagement de la victime...) sur décision du procureur de la République qui peut l'accepter ou le refuser en fonction de la finalité de ce fichier, de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé.
Une nouvelle modification législative s'annonce pour 2018 afin de tirer les conséquences de la décision n° 2017-670 QPC du Conseil constitutionnel du 27 octobre 2017. Par cette décision, le Conseil constitutionnel a jugé que les dispositions de l'article 230-8 portent une atteinte disproportionnée au droit au respect de la vie privée dans la mesure où elles privent les personnes mises en cause dans une procédure pénale, autres que celles ayant obtenu une décision judiciaire favorable, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le TAJ.

La possibilité d'effacement anticipé des données de TAJ a ainsi vocation à être étendue dans les prochains mois aux personnes ayant été condamnées avec dispense de peine ou dispense de mention au bulletin n°2 de leur casier judiciaire.

FOCUS

Le contentieux du droit d'accès indirect

L'exercice du droit d'accès indirect aux fichiers n'emporte pas, pour la personne, un droit à communication des données enregistrées dans les fichiers vérifiés par l'un des magistrats de la CNIL.

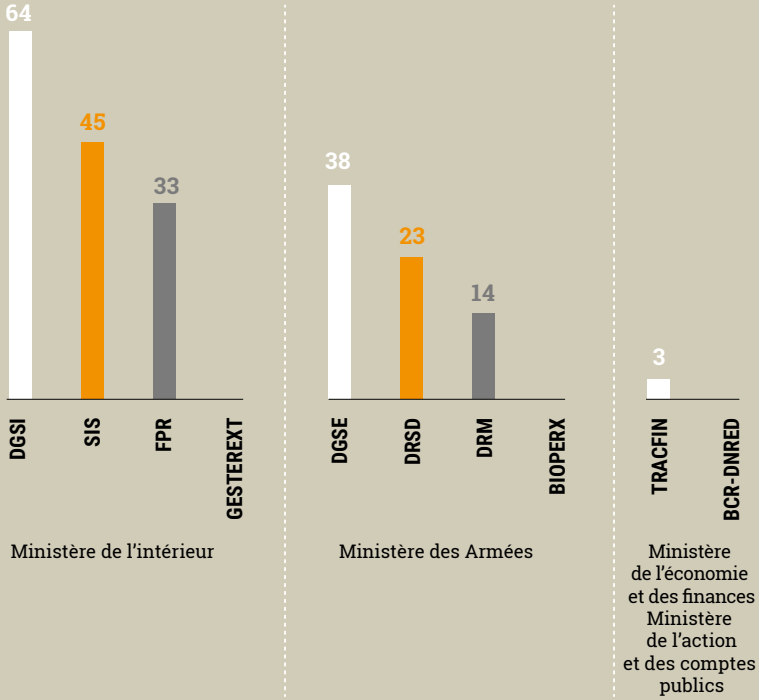
Les données ne peuvent être ainsi communiquées à la personne que si le responsable du fichier concerné estime que cette communication n'est pas de nature à nuire à la finalité du fichier, la sûreté de l'État, la défense et la sécurité publique. Toute opposition du responsable du traitement fait donc obstacle à la moindre communication de la CNIL, y compris si la personne s'avère inconnue du fichier. La CNIL peut uniquement assurer la personne de la réalisation des vérifications sollicitées et lui indiquer les voies de recours qui lui sont ouvertes pour contester le refus de communication.

Ces recours, qui doivent être dirigés contre le ministère, responsable du traitement, relèvent de la compétence :

- du tribunal administratif de Paris en premier ressort ;
- de la formation spécialisée du Conseil d'État, instituée par la loi n° 2015-912 du 24 juillet 2015 sur le renseignement, pour tout ou partie des fichiers intéressant la sûreté de l'État désignés par l'article R 841-2 du code de la sécurité intérieure. 11 fichiers relèvent actuellement de la compétence de cette formation spécialisée (cf. infra).

Depuis la mise en place effective de la formation spécialisée, au 1er trimestre 2016, la CNIL a produit, en qualité d'observateur, des mémoires dans le cadre de 189 requêtes. La formation spécialisée a, depuis lors, rendu 79 décisions concluant majoritairement au rejet des requêtes en l'absence d'irrégularité, sauf pour deux d'entre-elles. Elle a ainsi enjoint en 2017 le ministère des armées à procéder à l'effacement des données relatives à deux requérants figurant respectivement dans les fichiers de la DRSD et de la DRM.

Fichiers concernés par les requêtes auprès de la formation spécialisée 2016/2017*



*certaines requêtes introduites devant la formation spécialisée porte sur plusieurs de ces fichiers.

La formation spécialisée s'est également prononcée sur deux questions prioritaires de constitutionnalité portant sur l'article L.773-8 du code de justice administrative au motif que cet article, en ne prévoyant qu'une simple faculté pour le juge de sanctionner une irrégularité commise dans la tenue des fichiers couverts par le secret de la défense nationale, méconnaît le droit au recours effectif tel que garanti par l'article 16 de la Déclaration des droits de l'homme et du citoyen.

Le Conseil d'État a estimé que, dans la mesure où l'article contesté prévoit qu'en cas d'irrégularité, le responsable du traitement a l'obligation d'effacer ou de rectifier les données, le législateur n'avait pas méconnu ce droit et que, faute de question nouvelle ou sérieuse, ces deux questions n'avaient pas lieu d'être renvoyées au Conseil constitutionnel.

Histoires vécues...

MONSIEUR K., 51 ANS, confronté à un refus de renouvellement de son badge aéroportuaire, indispensable au maintien de son emploi, a souhaité exercer son droit d'accès indirect au TAJ. Les vérifications ont permis d'assurer la suppression de l'infraction qui y faisait obstacle (« violences avec incapacité inférieure à 8 jours et menace de délit contre les personnes sous condition ») car il avait bénéficié d'un jugement de relaxe.

MADAME O., 44 ANS, agent de police municipale depuis 2004 a été confrontée, à la suite d'une mutation dans un autre département, à des difficultés liées à son enregistrement dans le TAJ pour deux infractions alors même que le procureur de la République en avait respectivement prescrit l'effacement en 2013 et 2014 (classements sans suite pour « infraction insuffisamment caractérisée »). Les vérifications menées ont permis d'assurer l'effectivité de ces prescriptions.

MONSIEUR A., 42 ANS, a engagé une procédure de droit d'accès indirect car deux infractions enregistrées dans le fichier TAJ, dans le contexte d'un divorce difficile (« dégradation ou détérioration d'un bien appartenant à autrui » et « violences volontaires sur conjoint » auxquelles s'applique un délai de conservation de 20 ans), faisaient obstacle à l'obtention d'un emploi dans la sécurité privée. Compte tenu des classements sans suite intervenus dans ces deux affaires, le procureur de la République en a prescrit l'effacement en application de l'article 230-8 du code de procédure pénale, tel que modifié après la condamnation de la France par la Cour européenne des droits de l'homme (affaire Brunet contre France du 18 septembre 2014).

MONSIEUR E., 62 ANS, s'est vu opposer un refus d'accès dans une enceinte portuaire au motif de son enregistrement dans TAJ à la suite d'une plainte déposée à son encontre en 2004 par un copropriétaire de son immeuble avec lequel il avait eu une altercation alors qu'il occupait la fonction de syndic bénévole (« destruction, dégradation importante du bien d'autrui », soumise à un délai de conservation de 20 ans). Cette affaire a été requalifiée en « dégradations légères du bien d'autrui » (délai de conservation de 5 ans), ce qui a permis sa suppression immédiate.

MONSIEUR S., 60 ANS, a saisi la CNIL d'une demande de droit d'accès indirect au TAJ en raison de difficultés rencontrées du fait d'agissements commis par une personne usurpant son identité depuis plus de trente ans. Au terme des vérifications menées, Monsieur S. a pu être assuré par la CNIL qu'il ne faisait plus l'objet d'enregistrements en qualité de mis en cause dans le fichier TAJ.

MONSIEUR H., 32 ANS, a déposé une candidature pour travailler dans la sécurité privée sur le territoire suisse. Pour répondre aux exigences alors imposées par les autorités de cet État, il a exercé son droit d'accès indirect au TAJ par l'intermédiaire de la CNIL. L'affaire pour laquelle il était enregistré dans ce fichier (« recel »), qui aurait pu faire obstacle à l'obtention de cet emploi, a été supprimée sur prescription du procureur de la République compte tenu du classement sans suite intervenu.

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 2017, la CNIL a été fortement sollicitée pour répondre aux demandes d'avis des pouvoirs publics ; elle a également initié des travaux en vue de faciliter la transition vers le règlement européen.

Ophélia
Assistante
et Anne
Juriste au service de la santé, pôle recherche

L'activité de notre pôle consiste à accompagner les professionnels qui déposent des demandes d'autorisation de recherche. Deux jours par semaine, comme toutes les autres juristes du service santé, nous assurons une permanence téléphonique.
Pour certaines questions complexes, le demandeur est invité à nous faire une demande écrite. Beaucoup de chercheurs qui réalisent des thèses nous sollicitent, par exemple afin de savoir quelle formalité réaliser. D'une manière générale, une part importante de notre travail consiste à rendre accessible et compréhensible une matière qui, il faut bien le dire, est relativement complexe pour des non-juristes.

Nous contactons souvent les demandeurs afin d'obtenir des compléments d'informations à leur dossier : par exemple, la justification des demandes de dérogation à l'obligation d'informer les personnes, la motivation du traitement des données sensibles ou encore afin de suggérer de modifier la note d'information des personnes dont les données vont être traitées. Nous examinons également le protocole de recherche afin d'apprécier la proportionnalité du traitement envisagé.

Nous élaborerons aussi, en concertation avec les acteurs concernés, des procédures de simplification. En plus des échanges avec les chercheurs et les industriels, nous avons également de très nombreux contacts avec nos homologues des ministères concernés (santé et recherche) ou des organismes publics impliqués (INDS, INSERM, etc.).
Cela permet que les décisions de la CNIL s'inscrivent dans une logique globale favorisant, en France, la recherche dans le domaine de la santé tout en assurant un haut niveau de protection des données à caractère personnel.

Enfin, comme de nombreux autres métiers de la CNIL, notre activité nous permet d'être en première ligne des évolutions technologiques notamment en recherche médicale.

FOCUS

Traitement des données de santé : une logique de simplification et de responsabilisation accrue des acteurs

La CNIL poursuit, dans le secteur de la santé, son action de simplification des formalités préalables. C'est ainsi qu'après avoir adopté de nouvelles méthodologie de référence dans le domaine de la recherche, qui ont d'ores et déjà permis un allègement des formalités pour plus d'un millier demandes depuis juillet 2016, elle a décidé de soumettre au régime de la déclaration les traitements de données de santé qui relèvent des exceptions prévues à l'article 8 II de la loi Informatique et Libertés.

Ainsi, à titre d'illustration, les traitements tels que les dossiers médicaux partagés, les dispositifs de télémédecine ou d'éducation thérapeutique ne font dorénavant plus l'objet de demandes d'autorisation.
Cette évolution s'inscrit dans la philosophie générale portée par le règlement européen sur la protection des données qui confère au consentement des personnes concernées une place particulière dans la maîtrise de leurs données, favorise une responsabilisation accrue des acteurs et renforce le contrôle en aval par la CNIL.

Cette évolution est également justifiée par la maturité plus grande des responsables de traitement de données de santé quant à leurs obligations au regard de la loi. Enfin, elle permettra de favoriser l'innovation, privée ou publique, dans un secteur devenu stratégique en matière de données.

Le régime de la demande d'autorisation continuera à s'appliquer à tout traitement qui, ne relevant pas de ces exceptions, serait cependant justifié par un intérêt public. De même, cette évolution n'impacte pas les demandes d'autorisations en matière de recherche et d'évaluation soumises au chapitre IX de la loi Informatique et Libertés.

SIMPLIFIER LES FORMALITÉS ADMINISTRATIVES ET ANTICIPER L'APPLICATION DU RGPD

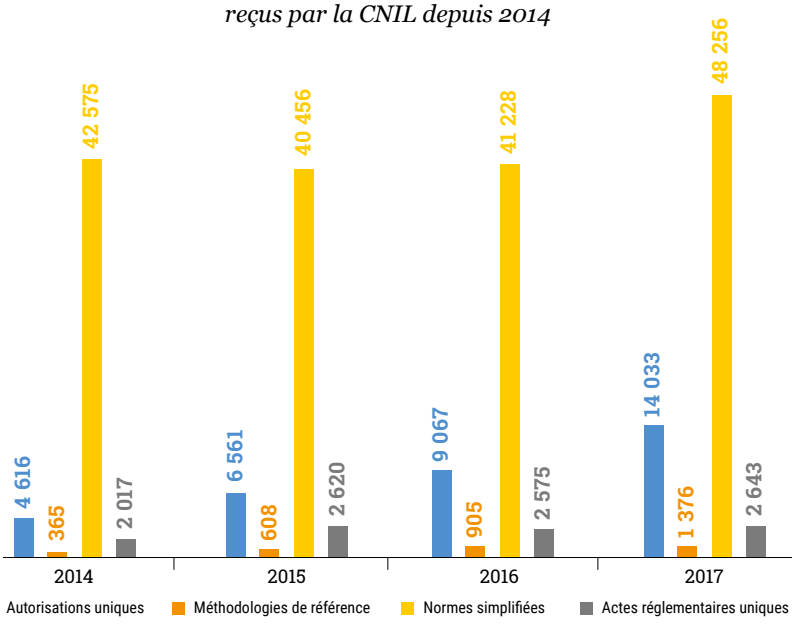
La CNIL est engagée depuis plusieurs années dans un processus de simplification administrative auprès des organismes publics et privés. Elle peut adopter des dispenses de déclaration, des normes simplifiées pour les traitements soumis à régime déclaratif, des autorisations uniques pour les traitements 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. Cette démarche de simplification s'inscrit également dans la logique du RGPD, qui verra la plupart des formalités préalables disparaître (hors santé).

En 2017, les effets de la simplification des formalités ont été particulièrement sensibles, notamment dans le champ des autorisations avec plus de 14 000 engagements de conformité reçus. Elaborés 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 67.000 dossiers pour 2017).

Nombre d'engagements de conformité à une norme de simplification reçus par la CNIL depuis 2014



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 2017, la CNIL a rendu 177 avis. On peut citer par exemple les avis portant sur :

- les modalités de mise en œuvre de la réforme du prélèvement à la source de l'impôt sur le revenu, au travers de plusieurs délibérations concernant des projets de texte visant à adapter à cette réforme les fichiers et outils utilisés par la Direction générale des finances publiques, administration chargée de la gestion de l'impôt.

- un décret encadrant l'évolution de la procédure d'agrément des hébergeurs de données de santé au profit d'un dispositif de certification, en estimant que le périmètre d'application du dispositif de certification des hébergeurs de données de santé devait-être précisé. Le décret publié (n°2018-137 du 26 février 2018) a ainsi déterminé des critères d'exclusion de l'activité d'hébergeur de données de santé.

- le décret relatif à la confidentialité des correspondances électroniques privées (délibération 2017-001) dans lequel la CNIL y rappelle que le consentement requière la manifestation d'une volonté libre, spécifique et éclairée et que le retrait de ce consentement ne doit pas conduire à l'arrêt du service pour les utilisateurs. Le décret prévoyant que le consentement des utilisateurs des services de communication au public en ligne doit être recueilli à une périodicité d'un an, la CNIL recommande aux responsables de traitement qui traiteront les correspondances des utilisateurs, de mettre en place un système de notification pour informer périodiquement ces derniers et s'acquitter de leur obligation.

Parmi les 101 autorisations adoptées en 2017, figurent des « autorisations uniques » qui ont vocation à encadrer un type de traitement et pas seulement autoriser le traitement d'un seul organisme. Ainsi l'autorisation unique n° 004, adoptée en 2005 pour encadrer les dispositifs d'alertes professionnelles, a été actualisée en juillet 2017 afin d'intégrer les mécanismes d'alertes professionnelles issus de la loi Sapin 2. Les points de vigilance à souligner vis-à-vis de ce type de traitement sont relatifs à l'absence de sanction liée au recours au dispositif d'alerte, sauf si les personnes ont émis une alerte de manière frauduleuse ou de mauvaise foi, la prudence à apporter au traitement des alertes anonymes et aux obligations de confidentialité et de sécurité pour éviter tout risque d'altération ou de communication frauduleuse des données.

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.

4 124
décisions

DONT

2 964
autorisations de transfert de données hors UE

810
autorisations recherche médicale ou évaluation des pratiques de soins

350
délibérations
dont 177 avis sur des projets de texte
dont 110 autorisations

40 ans!

de décisions et délibérations

en 1980	en 1988	en 1998	en 2008	en 2017
41	129	67	453	4 124

LA RECOMMANDATION SUR LES MOTS DE PASSE

La CNIL a adopté en janvier 2017 une recommandation relative aux mots de passe, qui permet aux professionnels comme aux particuliers de connaître les conditions minimales pour respecter l'obligation de sécurité posée par la loi. Elle met également des outils pratiques à disposition des professionnels et des particuliers.

Bien que ce moyen d'authentification soit de plus en plus critiqué et mis à l'épreuve, le mot de passe reste LE sésame pour accéder à la plupart des services numériques. De nombreux utilisateurs ne sont pas informés des pratiques élémentaires de sécurité et de gestion de ces secrets, alors que le nombre de comptes et la sensibilité des informations qu'ils protègent ne cessent de croître.

Un accroissement spectaculaire des attaques qui ont compromis des mots de passe

La multiplication des attaques informatiques, parfois spectaculaires, a notamment entraîné la compromission de bases de données entières de comptes et des mots de passe associés. Ont ainsi été rendus publics de nombreux mots de passe.

« Très répandu, le mot de passe offre pourtant un faible niveau de sécurité s'il n'est pas associé à d'autres mesures de sécurité. »

Les principales plateformes ont renforcé la sécurité de leurs dispositifs d'authentification, en complétant l'authentification par mot de passe par des dispositifs de sécurité complémentaires (double authentification via un code mobile, blocage du compte au bout de X tentatives).

Toutefois, il suffit qu'une seule plateforme soit défaillante en termes de sécurité (par exemple, en cas de vol massif de données d'authentification) pour qu'elle fasse courir un risque de sécurité à l'ensemble de l'écosystème numérique : les comptes, notamment les « webmails » (gestionnaires de courrier en ligne), dont le mot de passe a été découvert, compromettent en cascade l'ensemble des services auxquels les personnes sont inscrites.

Une doctrine pragmatique, tenant compte des mesures de sécurité complémentaires

Partant des constats faits lors de ses missions de contrôle et des échanges avec les responsables de traitement dans le cadre de leurs demandes d'avis, d'autorisation ou de conseils, la CNIL recommande des mesures minimales et pragmatiques, après avoir consulté différents acteurs de la sécurité, ainsi que l'ensemble des autorités de protection des données européennes. Cette recommandation n'exclut pas que d'autres mesures soient mises en œuvre en fonction des risques spécifiques qui pourraient être identifiés.

Ainsi, la longueur et la complexité du mot de passe varient en fonction des autres mesures de sécurité mises en œuvre pour l'authentification (temporisation d'accès au compte, double authentification, matériel détenu en propre par la personne).

La CNIL propose sur son site internet un kit de ressources et d'outils pour adopter les bons gestes pour protéger vos accès ; générer des mots de passe forts et faciles à retenir ; promouvoir et partager ces conseils.

LES OBSERVATIONS DE LA CNIL SUR LE PROJET DE LOI RENFORÇANT LA SÉCURITÉ INTÉRIEURE ET LA LUTTE CONTRE LE TERRORISME

La CNIL n'a pas été saisie pour avis du projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme. Cependant elle a examiné ce texte en formation plénière le 6 juillet 2017 en insistant sur la vigilance tant de méthode que de fond qu'exige la préparation des lois affectant les données personnelles des citoyens.

Sur le plan de la méthode, la CNIL aurait dû être consultée sur ce projet de loi. Les citoyens attendent que la lutte contre le terrorisme soit efficace, mais aussi qu'elle se fasse dans le respect dû à la protection de leur vie privée et de leurs données. C'est une condition de respect de l'État de droit, d'acceptabilité sociale et de légitimité des politiques de sécurité. La CNIL a précisément reçu du législateur la mission de veiller à cet équilibre. Cette mission ne peut toutefois s'exercer pleinement que si la CNIL est consultée, au préalable, sur les projets ayant une forte incidence sur le traitement et la protection de données personnelles.

Les points de vigilance de la CNIL sur le projet de loi

Sur le fond, la CNIL a pu rappeler la doctrine qu'elle suit dans l'examen des textes en matière de sécurité, en recherchant une juste conciliation entre la prévention des atteintes à l'ordre public et le droit au respect de la protection des données personnelles.

La Commission a notamment relevé, sur le projet en cause, que des garanties étaient prévues pour encadrer les mesures les plus intrusives, en ce qui concerne en particulier les conditions de placement sous surveillance électronique, les modalités de saisie et d'exploitation de données informatiques dans le cadre des visites ou la surveillance des communications hertziennes. La CNIL a toutefois estimé que ces garanties devraient être renforcées sur trois points : l'obligation de déclarer les numéros d'abonnement et les identifiants des moyens de communication électronique prévue dans certaines hypothèses ; les données PNR (*Passenger Name Record*) ; la saisie de données informatiques dans le cadre de visites.

Le nécessaire contrôle des fichiers de renseignement

La Commission a également rappelé, à l'occasion de ce projet de loi, la nécessité d'étendre sa compétence de contrôle des fichiers de renseignement, déjà soulignée par le passé.

Le code de la sécurité intérieure prévoit certes un encadrement strict de la collecte de données par des techniques intrusives mises en œuvre par les services de renseignement, seulement après intervention de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et autorisation du Premier ministre. Le législateur a par ailleurs prévu un « droit d'accès indirect », par lequel une personne peut obtenir qu'un membre de la CNIL s'assure de la régularité des données enregistrées, le cas échéant, dans l'un de ces fichiers. De même, la formation spécialisée du Conseil d'État est compétente pour connaître de requêtes individuelles concernant le recours aux techniques de recueil de renseignement ou le droit d'accès indirect aux fichiers mis en œuvre par les services spécialisés.

Cependant, au-delà de ces contrôles ponctuels, à la demande d'une personne, il n'existe pas aujourd'hui de dispositif de contrôle global des fichiers de renseignement eux-mêmes. Les textes qui les ont créés les ont en effet soustraits, dans la plupart des cas, au contrôle *a posteriori* de la CNIL. Il en résulte une situation paradoxale : les fichiers constitués à partir des données ainsi collectées sont pleinement soumis aux principes de la loi Informatique et Libertés (principe de finalité, proportionnalité des données collectées, exigence d'exactitude et de mise à jour, etc.), mais aucun contrôleur externe n'est désigné pour en assurer, de manière générale, le respect.

Le chiffrement, élément clé de la sécurité des données

Bien que ce sujet ne soit pas traité par le projet de loi, la CNIL a voulu réaffirmé, comme l'avait fait l'ANSSI (Agence Nationale de la sécurité des systèmes d'information), que la mise en place de portes dérobées (« *backdoors* ») dans les systèmes de chiffrement et de « clés maitres », ou encore l'interdiction pour le grand public d'utiliser des techniques de chiffrement des données à la main des utilisateurs, mettraient 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. Elles créeraient un risque collectif d'affaissement du niveau de sécurité des personnes et des institutions, et renforceraient leur exposition à de graves préjudices économiques, politiques ou de sécurité publique.

LES RELATIONS AVEC LE PARLEMENT

La CNIL a participé, en 2017, à une vingtaine d'auditions parlementaires organisées par les commissions permanentes et organes de contrôle du Parlement. Les auditions relatives aux projets de loi et propositions de loi ont été moins nombreuses au cours du premier semestre en raison de l'interruption des travaux au Parlement pour la période électorale.

La CNIL a été plus particulièrement sollicitée, au cours de cette période, par les missions de réflexion, de prospective et de contrôle du Parlement. À l'Assemblée nationale, les questions européennes ont donné lieu à plusieurs auditions afin de faire le point sur la stratégie numérique de la Commission européenne, tant en fin de législature qu'à l'automne 2017, dans le cadre de la mission d'information de la Commission des affaires européennes relative à la politique européenne du numérique. La Présidente de la CNIL a également participé, au mois de décembre, à la conférence organisée par la Présidente de la Commission des affaires européennes intitulée : « quelle modèle européen pour la révolution numérique ? ».

Au Sénat, la CNIL a participé aux travaux de la commission d'enquête sur les frontières européennes, le contrôle des flux des personnes et des marchandises en Europe et l'avenir de l'espace Schengen ; du groupe de travail de la Commission des affaires européennes sur les véhicules autonomes, collaboratifs ou connectés ainsi que ceux de la mission d'information de la Commission de la Culture sur la formation au numérique.

La CNIL a, comme l'année précédente, été régulièrement sollicitée par l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) et a ainsi été entendue au cours de l'année 2017 sur l'intelligence artificielle, les algorithmes et la décision publique (cas du portail Admission Post-Bac) et les enjeux des compteurs communicants.

Au second semestre 2017, la CNIL a été auditionnée sur plusieurs projets de loi en préparation dont le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme (juillet), le projet de loi pour un État au service d'une société de confiance (octobre) et au mois de décembre par la rapporteure du projet de loi relatif à la protection des données personnelles. Ce texte, qui procède à une vaste refonte de la loi Informatique et Libertés, avait fait l'objet, en amont, d'une mission préparatoire d'information de la Commission des lois de l'Assemblée nationale devant laquelle la CNIL avait été entendue en janvier 2017.

L'examen de ce texte est prévu au Parlement au cours du premier trimestre 2018.

Enfin, la CNIL a eu l'occasion d'accueillir dans ses murs des élus de l'Assemblée nationale :

EN OCTOBRE :

M. Cédric Villani, Député de l'Essonne, dans le cadre de la mission qui lui a été confiée par le Premier ministre sur le développement de l'intelligence artificielle ;

EN NOVEMBRE :

une visite de la CNIL organisée pour les membres de la Commission des lois, en présence de sa Présidente, **M^me^ Yaël Braun-Pivet.**

ACCOMPAGNER
la conformité

L'accompagnement par la CNIL de la mise en conformité de l'ensemble des professionnels de la sphère publique et privée prend une signification particulière cette année avec la transition vers le RGPD. Celui-ci entérine en effet l'importance d'une culture de la conformité qui dépasse la sphère juridique en constituant un indicateur de bonne gouvernance, répondant aussi à l'enjeu de réputation, de confiance, vital dans le monde numérique et également à celui de compétitivité pour les entreprises.
Cette mise en conformité constitue l'objectif prioritaire de la régulation et s'appuie sur des acteurs privilégiés que sont les CIL qui vont se transformer en Délégués à la Protection des données (DPO). La CNIL a développé une pratique des labels et codes de conduite internes que sont les BCR, qui sont promus par le règlement. Enfin, les « packs de conformité », futurs référentiels de bonnes pratiques, qu'ils soient sectoriels ou rattachés à une thématique démontre le succès d'une co-régulation avec les acteurs. Ils déclinent, de la manière la plus opérationnelle en tenant compte des besoins des acteurs, les principes de la loi au contexte spécifique d'un secteur donné.

Valérie
Responsable du pôle Labels

Le pôle Labels est composé de 2 personnes, dont 1 assistante. Notre rôle est de traiter les dossiers de labellisation, de la réception du formulaire de candidature à la délivrance des labels. Au-delà de l'analyse de la recevabilité de leurs demandes et de l'instruction des pièces qu'ils nous ont transmises, nous effectuons un réel accompagnement des candidats pour mener leur procédure ou produit à un taux de conformité de 100% au référentiel de labellisation qu'ils ont choisi.

Le pôle travaille en transversalité avec le service de l'expertise technologique, et les services sectoriels de la Direction de la Conformité, dont les analyses sont nécessaires pour les items techniques ou spécifiques auxquels les demandeurs à la labellisation doivent répondre. Nos observations se veulent des guides, des moyens de satisfaire les exigences, et non des « sentences » définitives.

Avec la future entrée en application du RGPD, le pôle Labels s'est impliqué dans la rédaction de lignes directrices européennes en matière de certification et d'accréditation. Au plan national, il a fallu envisager l'avenir des labels, c'est-à-dire leur évolution vers des mécanismes de certification, en s'entourant des différents acteurs concernés, dont le COFRAC (Comité français d'accréditation).

ACCOMPAGNER ET PRÉPARER LES FUTURS DÉLÉGUÉS À LA PROTECTION DES DONNÉES (DPO)

Acteur de la conformité, le délégué à la protection des données, successeur du Correspondant Informatique et Libertés, est incontournable dans le règlement européen qui lui consacre un rôle essentiel que ce soit vis-à-vis des personnes concernées ou au sein de l'organisme qui l'aura désigné. En tant qu'autorité de régulation, la CNIL accompagne le développement de ce métier.

Le délégué veille et contrôle la conformité au règlement européen sur la protection des données des traitements l'organisme qui l'a désigné. Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.

Pour garantir l'effectivité de ses missions, le règlement prévoit que le délégué :

- doit disposer de qualités professionnelles et de connaissances spécifiques en protection,
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

Des lignes directrices pour accompagner les désignations de délégués

Après une phase de consultation publique, les lignes directrices du G29 sur le délégué adoptées en avril 2017 ont pour objectif d'accompagner les professionnels dans la mise en place de la fonction de délégué ainsi que d'assister ces délégués dans l'exercice de leurs missions.

Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.

En particulier, elles clarifient la compréhension des critères posés par le règlement sur les aspects suivants :

- les notions d'« organisme public », de « grande échelle » et de « suivi régulier et systématique », qui commandent l'obligation de désignation d'un délégué dans le secteur privé ;
- 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 ;
- les modalités d'externalisation de la fonction ;
- la notion de conflit d'intérêts.

Enrichies d'une foire aux questions, les lignes directrices sont devenues indispensables pour organiser la fonction au sein des organismes publics ou privés.

Des actions de sensibilisation en nette augmentation

La CNIL a été particulièrement attentive à la diffusion d'informations à destination du plus grand nombre de CIL ainsi qu'à leurs représentants sectoriels. Pour sensibiliser les entreprises, les administrations centrales, les collectivités et les associations, la CNIL a enrichi ses contenus sur son site internet, dont une rubrique dédiée à la désignation du DPO. Également, elle a procédé durant l'été 2017 à des campagnes d'informations directes à destination des organisations professionnelles représentant un large nombre de secteurs d'activités, des grandes entreprises françaises du CAC40 et des CIL.

Très actifs, les CIL des collectivités territoriales ont aussi manifesté leur besoin d'accompagnement auprès de la CNIL, qui a créé des contenus spécifiques à leur attention. C'est aussi pour cette raison qu'un éclairage particulier a été apporté sur les modalités de mutualisation et d'externalisation de la fonction au sein des petites collectivités qui devront désigner un DPO.

FOCUS

Convention de partenariat entre la CNIL et l'ADF

(Assemblée des départements de France)

Les Départements sont amenés à traiter de très nombreuses données personnelles et certains de leurs traitements, tels ceux mis en œuvre pour la gestion de leurs activités en matière sociale et médico-sociale ou en matière de conservation et de valorisation d'archives publiques, impliquent le traitement de données d'une sensibilité particulière. Dans ce contexte, la CNIL et l'ADF ont décidé de mener des actions communes pour préparer aux mieux les Départements.
L'ADF apportera aux Départements un accompagnement dans leurs démarches de mise en conformité, en particulier via son Groupe technique sur la protection des données personnelles dont les travaux, depuis septembre 2017, portent principalement sur les conditions de mise en place d'une gouvernance Informatique et Libertés (mutualisation des réflexions, outils et bonnes pratiques).

Ce groupe de travail composé de CIL et futurs DPO sera le point de contact de référence pour ses échanges avec la CNIL sur les principales questions que les Départements pourront porter à sa connaissance.

Ce modèle d'organisation au sein de ce réseau est emblématique des bonnes pratiques à développer au sein de tous les secteurs d'activités privés, publics ou associations.

L'évolution des ateliers CIL : vers des Mooc et webinars

Pour répondre aux besoins exprimés par les professionnels, les ateliers CIL ont intégré dès 2016 les principaux changements apportés par le RGPD. En 2017, tous les ateliers CIL ont été transformés progressivement pour se concentrer sur le règlement. Fort de ces nouveaux programmes, les ateliers ont été ouverts à un public toujours plus nombreux (+ 40 % par rapport à 2016) et exigeant.
Afin de proposer au plus grand nombre des contenus pédagogiques sur les règles de la protection des données personnelles, la CNIL travaille actuellement à la transformation des ateliers les plus demandés en MOOC (formation en ligne ouverte à tous), notamment sur les fondamentaux du RGPD et sur la sécurité. Le parcours pédagogique envisagé prévoit un parcours permettant d'avancer à son rythme et selon ses contraintes.
En outre, des webinars viendront compléter l'offre d'accompagnement de la CNIL envers les DPO et les professionnels en général.

Un guide à destination des sous-traitants

Par ailleurs, au vu des nombreux échanges engagés sur ce sujet avec les CIL, un guide à destination des prestataires et sous-traitants a pu voir le jour afin de clarifier les nouvelles obligations qui reposent sur ces professionnels. En effet, le règlement impose des obligations spécifiques aux sous-traitants dont la responsabilité est susceptible d'être engagée en cas de manquement.

« En interne, le DPO doit aussi bien dialoguer avec le top management qu'avec les métiers. »

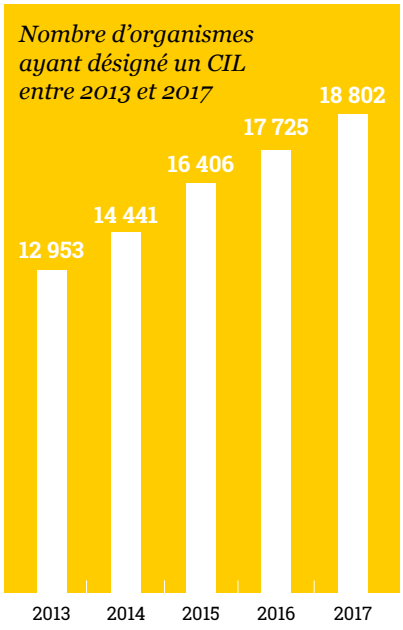
+ de 80 000

organismes devront désigner un DPO

Ce guide propose notamment des exemples de clauses contractuelles pour aider les professionnels de façon très opérationnelle.

- La formation initiale et continue apparait indispensable pour exercer le métier de DPO que ce soit à temps plein ou à temps partiel.
- Le top management doit être porteur de la gouvernance de la conformité et soutenir le DPO dans ses actions de conseil, de sensibilisation et de contrôle du respect de la protection des données personnelles.

Nombre d'organismes ayant désigné un CIL entre 2013 et 2017



Chiffres 2017

5 107

CIL sont désignés dans 18 802 organismes

1 700

personnes accueillies lors de 37 ateliers dans les locaux de la CNIL (+ 40%)

2 249

demandes de conseil de CIL reçues

4 079

appels traités lors de la permanence téléphonique quotidienne

LES PACKS DE CONFORMITÉ, FUTURS RÉFÉRENTIELS SECTORIELS OU THÉMATIQUES

Le pack « véhicules connectés »

Le pack de conformité a été élaboré en concertation avec les acteurs de la filière automobile, les entreprises de plusieurs secteurs d'activité dont les assurances et les télécoms et les autorités publiques.

Il constitue pour ces professionnels une véritable boîte à outils leur permettant d'intégrer la dimension « protection des données personnelles » dès la phase de conception des produits et d'assurer la maîtrise par les personnes de leurs données.

Une telle démarche conditionne la confiance des utilisateurs, donc le développement pérenne de ces technologies. Elle est enfin la traduction d'une régulation innovante, à la fois évolutive et concertée.
Ces lignes directrices permettent, pour chaque type de traitement identifié, de préciser leurs finalités, les catégories de données collectées, leurs durées de conservation, les droits des personnes, les mesures de sécurité à mettre en place et les destinataires des informations.

Le pack met en particulier l'accent sur les points suivants :

- **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 d'autodétermination informationnelle, de transparence et de loyauté de la collecte**, qui impliquent, *a minima* une information des personnes concernées, voire le recueil de leur consentement.

- **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.

- **La CNIL encourage les acteurs à privilégier le scénario IN => IN, qui implique le traitement des données en local, dans le véhicule, sans transmission vers le fournisseur de services.** Il offre de bonnes garanties en matière de la vie privée pour les usagers et entraîne pour les responsables de traitement des obligations allégées sur le plan Informatique et Libertés.

Le pack a également vocation à être porté au niveau européen pour permettre aux acteurs de se positionner sur un marché européen, voire mondial.

Le pack de conformité « Silver économie »

Dans le cadre de **l'accompagnement des professionnels du secteur social et médico-social dans leur démarche de mise en conformité**, la CNIL a élaboré, en 2016, des autorisations uniques destinées à simplifier les formalités des organismes tout en leur offrant un cadre de référence leur permettant de traiter les données nécessaires des personnes qu'ils accompagnent dans le respect de leurs droits et libertés.
À ce jour, près de 5 000 engagements de conformité ont été effectués dont la grande majorité concerne les traitements destinés à l'accompagnement, au suivi social et médico-social des personnes handicapées et des personnes âgées.

Dans le prolongement de ces travaux, la CNIL a élaboré un nouveau pack de conformité visant à encadrer le traitement des données issues de l'utilisation de produits et service de la « silver économie » destinés à améliorer la qualité de vie des seniors ou à leur apporter plus de sécurité, qu'ils soient actifs, en situation de fragilité ou dépendants en raison de leur âge ou d'un handicap.

En effet, compte tenu de l'émergence de ces produits et services, la CNIL, en concertation avec la Fédération des Industries Électriques, Électroniques et de Communication (FIEEC), a souhaité dégager des bonnes pratiques pour permettre aux professionnels d'intégrer dès la conception de leurs produits la protection des données personnelles et garantir ainsi la maîtrise par les personnes concernées de leurs données.

Il ressort de ces travaux trois scénarios qui décrivent les conditions dans lesquelles les données peuvent être traitées au regard de la loi Informatique et Libertés ainsi que les points de vigilance auxquels les professionnels seront confrontés avec l'application du Règlement européen sur la protection des données personnelles applicable au 25 mai 2018 :

Scénario 1

« IN => IN » : les données sont traitées dans l'espace privé, via des dispositifs restant sous la maîtrise unique de la personne concernée et pour son usage personnel.

Scénario 2

« IN => OUT » : les données sont traitées dans l'espace privé et transmises à l'extérieur.

Scénario 3

« IN => OUT => IN » : les données sont traitées dans l'espace privé et transmises à l'extérieur pour permettre en retour une action automatique sur les équipements situés dans l'espace privé.

Le suivi des packs de conformité existants

5 000

engagements de conformité aux autorisations uniques élaborées par la CNIL pour les professionnels du secteur social et médico-social

Ces outils doivent leur succès au suivi qui en est fait afin de maintenir leur adéquation aux besoins des professionnels. Les packs sont des documents évolutifs qui ont vocation à être complétés et mis à jour du fait de l'entrée en application du règlement européen sur la protection des données le 25 mai 2018.

À RETENIR

RGPD et prévention de la fraude

Le RGPD reconnait la prévention de la fraude comme poursuivant un intérêt légitime. Le considérant 47 rappelle que *« le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné. »*

L'intérêt légitime réside dans la vigilance que doit mettre en œuvre un organisme d'assurance à l'égard du fondement des prestations dont le versement lui est demandé dans le cadre de la réglementation propre à son activité.

Le pack de conformité du secteur de l'assurance

Une question nouvelle abordée : la mutualisation de la fraude pour les contrats d'assurance automobile

Le « club conformité » qui réunit la CNIL et les professionnels pour faire vivre le pack a travaillé sur les modalités de mise en place d'un dispositif expérimental de lutte contre la fraude strictement limité aux sinistres. Le bilan a permis d'identifier 1 548 suspicions de fraudes organisées sur 3 367 alertes générées par l'outil de détection. Le dispositif a ensuite été autorisé par la CNIL en septembre 2017.

À RETENIR

Un référentiel RGPD pour le secteur de l'assurance

Avec le règlement européen, le référentiel mettra l'accent sur l'information des personnes en distinguant les informations « essentielles » de celles dites « complémentaires » sans oublier de rappeler que pour certains traitements, comme en matière de lutte contre la fraude, l'information est renforcée. S'agissant des droits des personnes, le référentiel insistera plus particulièrement sur les nouveaux droits issus du RGPD tels que le droit à l'effacement ou encore la portabilité des données.

3 000

suspicions de fraudes organisées seraient détectées sur une année d'après les prévisions de l'ALFA

La CNIL a autorisé une expérimentation puis la généralisation d' un traitement visant la lutte contre la fraude en assurance automobile. Le dispositif nécessitait une mutualisation des données des sinistres automobiles détenues par les assureurs.

La mise à jour du pack assurance avec le RGPD

Bientôt un référentiel pour le secteur de l'assurance

Dès le printemps 2017, le club conformité assurance a commencé ses travaux pour mettre à jour le pack de conformité avec le règlement européen.

Les professionnels de l'assurance poursuivent leurs échanges avec la CNIL avec pour objectif d'établir un référentiel pour le secteur. À l'image des fiches pratiques du pack assurance, les travaux offriront aux professionnels une documentation claire et opérationnelle pour les accompagner dans leur démarche de conformité avec le RGPD. En 2017, le club assurance s'est d'ailleurs élargi pour accueillir de nouveaux membres et compléter la connaissance par le régulateur des pratiques professionnelles : les comparateurs en assurance.

Le pack de conformité du secteur banque

La CNIL a complété sur plusieurs points importants le pack, suite aux travaux menés en étroite collaboration avec les professionnels du secteur bancaire (FBF, ASF, OCBF) afin de constituer une « boîte à outils » de la conformité spécifique au secteur bancaire.

Ainsi, lors de la séance du 20 juillet 2017, elle a adopté une **autorisation unique pour les traitements ayant pour finalité la lutte contre la fraude externe** dans le secteur bancaire et financier. L'autorisation unique encadre les traitements dont la finalité est la détection d'anomalies, l'analyse et la gestion des alertes, ainsi que la constitution de listes d'auteurs de fraudes avérées, dans le cadre d'activités portant notamment sur les services et produits bancaires et financiers, ainsi que d'activités relatives aux produits et services dits « connexes». Seules les entités visées au livre V du code monétaire et financier (CMF) ainsi que les filiales contrôlées par ces entités exerçant une activité qualifiée de « connexe » peuvent procéder à un engagement de conformité à cette autorisation unique.

La CNIL a également mis à jour la **dispense n°9 sur les listes d'initiés** au regard du règlement MAR qui a instauré de nouvelles règles en la matière. La dispense tient compte, notamment, de l'ajout de nouvelles données dans le cadre de l'uniformisation européenne destinée à faciliter l'identification des personnes pouvant être inscrites sur les listes d'initiés. Les durées de conservations sont étendues à 5 ans. Enfin, les listes doivent désormais être établies dans le format prévu par le règlement d'exécution (UE) 2016/347 du 10 mars 2016 et sont transmises à l'AMF à sa demande.

Par ailleurs, elle a adopté une **délibération portant modification de la recommandation** concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance. Cette modification vise en particulier à tenir compte de l'utilisation de la carte bancaire pour les paiements multiples ou récurrents d'abonnements souscrits en ligne qui implique que les données bancaires soient conservées au-delà de la première transaction pour la réémission du paiement, à chaque mensualité par exemple, pendant la durée de l'abonnement. Or, cette conservation pour paiements successifs n'était pas explicitement prévue par la « recommandation CB » du 14 novembre 2013. **Une fiche pratique** sur le paiement à distance par carte bancaire a été publiée à cette occasion sur le site internet de la CNIL.

De plus, la CNIL a **autorisé neuf établissements bancaires** à mettre en œuvre, à titre expérimental, un dispositif d'authentification de clients par reconnaissance vocale sur serveur d'appels. Elle a également accordé le 14 septembre 2017 une **autorisation à la Société générale** pour la mise en œuvre d'un système d'identification par reconnaissance faciale des prospects dans le cadre d'un processus d'entrée en relation à distance.

Une refonte de **l'autorisation unique 003** relative aux traitements mis en œuvre par les organismes financiers dans le cadre de la lutte contre le blanchiment et le financement du terrorisme est également à l'étude. Cette refonte prendra la forme d'un référentiel dans la perspective de l'entrée en application du RGPD à partir du 25 mai 2018. Enfin, ce travail d'élaboration de référentiels se poursuit afin d'encadrer les traitements dédiés à la lutte contre la fraude interne et à la consultation de listes de sanctions édictant des mesures restrictives.

LES LABELS : UN GAGE DE CONFIANCE

Une nette recrudescence des demandes de labellisation

2017 marque l'année du plus grand nombre de réception de dossiers de candidature, parmi les six années de labellisation. 98 demandes ont en effet été adressées, soit plus de 2 fois le nombre de dossiers reçus en 2016. 28 labels ont été délivrés, dont 14 pour les formations Informatique et Libertés, 6 pour les procédures de Gouvernance Informatique et Libertés et 6 pour les procédures d'Audit.

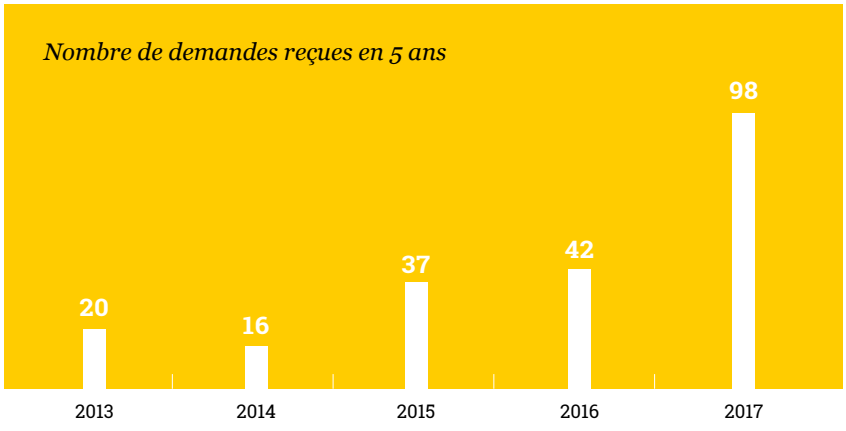
Afin d'anticiper l'entrée en application du règlement européen en mai 2018, la Commission a procédé, dès juillet 2017, à l'actualisation de deux de ses quatre référentiels de labellisation. Ces nouveaux labels « Gouvernance RGPD » et « Formation RGPD » constituent ainsi, depuis leur publication au Journal Officiel, un outil d'aide à la mise en conformité au RGPD pour les organismes, qui peuvent d'ailleurs se prévaloir de la conformité de leur gouvernance Informatique et Libertés ou formation avant même l'entrée en application du texte européen.

Adaptation des labels à l'entrée en application du RGPD : de la labellisation vers la certification

Le Règlement européen invite les autorités de protection des données à encourager la mise en place de mécanismes de certification, de labels et de marques en matière de protection des données.
Aussi, compte tenu de cette nouvelle mission et des nombreuses demandes de labellisation dont elle est saisie, la CNIL a décidé de s'engager dans une démarche de promotion de la certification, et de mettre fin à son activité de labellisation.

Ces certifications seront délivrées par des organismes certificateurs, sur la base de référentiels élaborés par la CNIL.

Des travaux ont été engagés avec l'organisme national d'accréditation, le COFRAC, afin d'étudier selon quelles modalités pourraient être instaurés ces mécanismes de certification, avec un agrément des tiers certificateurs par la Cnil ou une accréditation des certificateurs par le COFRAC.



Les labels en chiffres

4
référentiels

199
demandes de labels reçues depuis 2013 dont 29 demandes de labels RGPD (labels Gouvernance ou Formation actualisés au regard du RGPD)

98
demandes de labels reçues en 2017

4,5
mois de délai moyen

123
labels délivrés

LES BCR : UN OUTIL DE GOUVERNANCE DE LA DONNÉE AU-DELÀ DES GARANTIES APPORTÉES POUR ENCADRER LES TRANSFERTS

La globalisation de l'économie digitale facilite inévitablement les flux transfrontaliers de données ; la protection des données transférées vers des pays tiers n'est dès lors efficace que si cette protection a été pensée en amont via un processus de gouvernance globale de la donnée. Loin de se cantonner aux transferts, les *Binding Corporate Rules* (BCR) proposent déjà les bases d'un programme global de conformité au RGPD (cf. tableau de mise en relation RGPD et BCR). En effet, les BCR sont les premiers instruments précurseurs de l'*accountability*, principe désormais au cœur du nouveau règlement européen.

Les BCR sont avant tout un outil à destination des grands groupes qui ont atteint une masse critique dans la gestion de leurs données et par conséquent des transferts internationaux associés. De par leur implantation géographique, les groupes doivent composer avec de nombreuses législations nationales.
Le choix des BCR permet de fournir une structure de gouvernance de la donnée unique, complète et harmonisée au sein d'un groupe, ainsi qu'un socle commun de protection. L'objectif est clairement d'assurer un niveau cohérent de protection afin d'éviter des divergences qui pourraient entraver leurs activités mais aussi de garantir la sécurité juridique de leurs opérations. En outre, les BCR permettent aux entreprises de remporter la bataille de la confiance des clients car il est un facteur de différenciation reconnu.

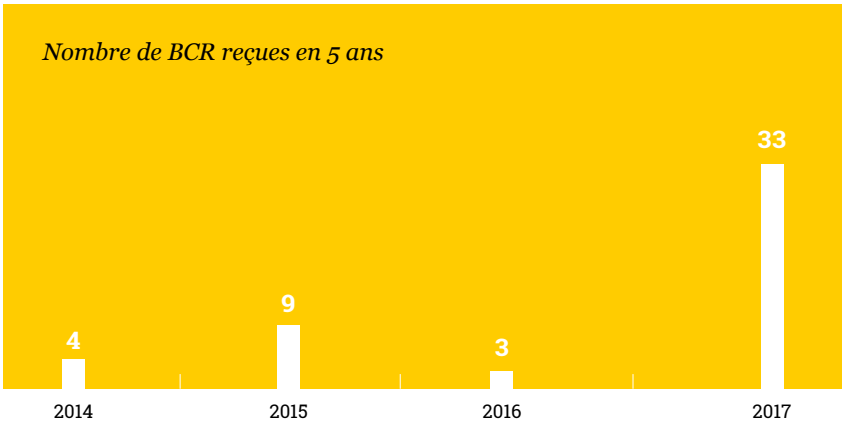
Une montée en puissance des BCR

117

détenteurs de BCR

Réservées pour le moment à une centaine de groupes, les BCR bénéficient d'une attractivité nouvelle comme en témoignent les chiffres, près d'une quarantaine de BCR en cours d'instruction auprès de la CNIL en qualité d'autorité chef de file. Mais outre cet engouement lié à la date butoir du 25 mai 2018, l'intérêt grandissant pour les BCR traduit un mouvement plus profond. C'est un instrument à la fois politique, juridique, organisationnel, international, avec une caractéristique majeure : il est « accountable » par essence. Il est la traduction de la politique interne d'un groupe, de la façon dont un groupe interprète et applique de manière opérationnelle les grands principes de la protection des données.
L'élaboration de ses règles contraignantes prend en compte les spécificités du groupe auquel elles se rattachent ; elles s'appuient sur son organisation et ses procédures internes ce qui donne au groupe d'entreprises une plus grande marge de manœuvre mais également assure une meilleure effectivité ; le suivi du respect des BCR peut être assuré par des auditeurs internes et/ou externes et enfin, le fait que l'approbation est délivrée directement par les autorités de contrôle donne un crédit particulier aux BCR.

Nombre de BCR reçues en 5 ans



Les BCR et les autres outils de conformité

La CNIL considère que la promotion de la certification et des codes de conduite dans la sphère de la protection des données est complémentaire des autres outils, tels que les BCR, et vise à offrir une boîte à outils renouvelée et diversifiée afin de prendre en considération les besoins de tous les secteurs d'activités.

Au-delà de la qualification de « garantie appropriées » pour les transferts, les BCR sont le point de départ de l'élaboration d'une politique globale de gouvernance des données personnelles.

Les BCR RT & ST sont des instruments de conformité dynamiques et continueront à évoluer dans les années à venir car elles ont un fort potentiel et sont désormais portées par des acteurs cruciaux.

À ce titre, le Comité européen de la protection des données aura un rôle important à jouer dans les années à venir et sera amené à publier des lignes directrices, des recommandations et des bonnes pratiques aux fins de préciser davantage les critères et exigences applicables aux transferts comme le prévoit explicitement l'article 70-1 i) du RGPD.

Répartition par secteur d'activité des 117 groupes ayant adopté des BCR

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

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

PARTICIPER
à la régulation internationale

Outre la préparation au règlement européen, qui a été au cœur de l'activité du G29 dont la CNIL en assurait la présidence jusqu'à février 2018, l'année 2017 a encore été marquée par les travaux sur l'accord privacy Shield. En octobre 2017, la Présidente de la CNIL a été élue à la présidence de la conférence internationale et l'association des autorités francophones l'AFAPDP a fêté ses 10 ans.

Étienne
Juriste au service des affaires européennes et internationales

Le service des affaires européennes et internationales a poursuivi en 2017 son rôle de conseil auprès des services sur les sujets présentant une dimension européenne et internationale, tout en participant également à la communication et promotion des positions de la CNIL auprès de nos partenaires dans l'Union et au-delà.

Jusqu'en février 2018, Isabelle Falque-Pierrotin a assuré la présidence du G29 (CNIL européennes). Notre service a donc continué de coordonner les activités du G29, d'organiser ses séances plénières et groupes de travail, mais aussi d'impulser les orientations stratégiques. Un travail de fond a été mené afin de mettre en « ordre de marche » le futur modèle de gouvernance européen prévu par le Règlement, mais aussi de définir notre interprétation commune au travers de lignes directrices en vue d'assurer la mise en œuvre effective des dispositions clés du RGPD à partir du 25 mai 2018. Pour ma part, j'ai ainsi participé à l'organisation de FabLab ouvert à la société civile destinés à alimenter les réflexions du groupe, et à la préparation des positions du G29 sur divers sujets.
Autre temps fort de l'année 2017 : la première revue annuelle du Privacy Shield s'est tenue à Washington. Elle a permis d'évaluer ce dispositif de la Commission européenne et d'adresser une série de recommandations sur les garanties à apporter au transfert de données personnelles entre l'Union européenne et les États-Unis.

En 2017, Isabelle Falque-Pierrotin a été élue à la Présidence de la Conférence internationale des autorités de protection de données (ICDPPC) qui rassemble près de 120 autorités. Je m'occupe en particulier de la consultation stratégique lancée auprès des membres du réseau, afin de définir le rôle et les orientations stratégiques de l'organisation pour les années à venir.

BILAN DES ACTIVITÉS 2017 DU G29 EN LIEN AVEC LE RÈGLEMENT EUROPÉEN

Au niveau européen, l'année 2017 a été marquée par la poursuite et l'aboutissement des travaux engagés par la CNIL et ses homologues européens au sein du G29 afin d'accompagner la transition des différents acteurs concernés vers le nouveau cadre introduit par le Règlement. Aussi, à quelques mois de l'entrée en application du Règlement, 2017 a constitué une étape clé au cours de laquelle le G29 a œuvré pour traduire le Règlement en une réalité opérationnelle et permettre aux organismes d'être prêt pour le 25 mai 2018.

Ces activités qui s'inscrivent dans le cadre du programme de travail 2016-2018 et du plan d'action pour 2017 du G29 visent d'une part, à rendre le Règlement le plus opérationnel possible pour les responsables de traitement et les sous-traitant et d'autre part, à mettre en place le nouveau modèle de gouvernance pour les autorités de protection des données.

Le G29 a ainsi adopté en 2017 des lignes directrices afin de fournir aux organismes concernés une interprétation commune et un éclairage pratique sur une série de concepts clés ou de nouvelles obligations prévues par le Règlement. Les lignes directrices ayant fait l'objet d'une adoption finale concernant le délégué à la protection des données, le droit à la portabilité, l'autorité chef de file et les études d'impact sur la vie privée. Les G29 a par ailleurs pré-adopté des lignes directrices concernant les violations de données personnelles, la prise de décision automatisée et le profilage, la transparence, le consentement, et des référentiels en matière de transferts internationaux de données mis à jour au regard du Règlement (adéquation et BCR responsable de traitement et sous-traitant).

L'ensemble de ces documents ont été élaborés selon une approche de co-construction, le G29 s'étant appuyé sur deux ateliers collaboratifs, *Fablab*, ainsi que des consultations publiques organisées au niveau européen et au niveau national en partenariat avec des représentants de la société civile, des fédérations professionnelles et du milieu universitaire en vue de recueillir leurs questions concrètes, les éventuelles difficultés d'interprétation, et les exemples de bonne pratique. L'objectif d'une telle démarche vise à produire des recommandations en phase avec la réalité concrète du terrain.

L'action du G29 a en outre porté sur la construction du nouveau modèle de gouvernance pour les autorités, marqué par la création d'un nouvel organe communautaire, le Comité européen de protection des données (CEPD) qui succédera au G29. À cet égard, le G29 s'est attaché à définir la boîte à outils en vue d'organiser l'action des autorités demain, à travers les différents mécanismes de coopération prévus par le Règlement, leurs pouvoirs de sanctions et les règles de procédure permettant le fonctionnement effectif du CEPD au 25 mai 2018.

Ce travail s'est accompagné d'actions au niveau national afin de sensibiliser les personnes dont le Règlement renforce les droits et le contrôle qu'elles peuvent exercer sur l'usage qui est fait de leurs données personnelles.

Le point sur les guidelines au 20/02/2018

PIA	Adoption Définitive
Autorité chef de file	Adoption Définitive
Délegué à la protection des données	Adoption Définitive
Transparence	Adoption pour consultation
Profilage	Adoption définitive
Notification de violations	Adoption définitive
Référentiel d'adéquation	Adoption définitive
BCR	Adoption définitive
BCR sous-traitant	Adoption définitive
Consentement	Adoption pour consultation
Certification	Adoption pour consultation
Portabilité	Adoption définitive
Dérogations transferts	Adoption pour consultation
Champ d'application	En cours
Codes de conduite	En cours

DERNIÈRE MINUTE

La CNIL a assuré pendant 4 ans la présidence du G29.

Le 7 février 2018, Andrea Jelinek, la Présidente de l'autorité autrichienne a été élue présidente du G29.

LA PARTICIPATION DU G29 À LA 1ère ÉVALUATION CONJOINTE DE L'ACCORD PRIVACY SHIELD

Au niveau international, le G29 a participé à la première évaluation conjointe UE/US de la décision d'adéquation « Bouclier de protection de la vie privée » (*Privacy Shield*). Dans le cadre cette mission, le G29 a participé à la préparation des questionnaires adressés aux parties prenantes et aux autorités américaines en amont de la revue, et 8 représentants du G29 ont participé aux deux jours de réunions organisés à Washington par la Commission européenne en septembre 2017. Deux membres de la CNIL faisaient partie de cette délégation, qui a ensuite préparé le projet de rapport discuté au sein du G29.

À l'issue de ces travaux, le G29 a adopté son propre rapport, distinct de celui de la Commission européenne et formulé plusieurs recommandations, dont les plus prioritaires (en particulier la nomination d'une « *ombudsperson* » indépendante, la désignation de l'ensemble des membres du *Privacy and Civil Liberties Oversight Board,* et la fourniture d'explications complémentaires sur les règles de procédure encadrant le suivi du *Shield*) devront être mises en œuvre d'ici le 25 mai prochain.

Dans l'hypothèse où ces recommandations ne seraient pas mises en œuvre, les membres du G29 ont également indiqué dans leur rapport qu'elles envisageraient de saisir les juges nationaux afin qu'ils puissent en référer à la CJUE, conformément à la jurisprudence de la Cour dans l'affaire « *Schrems* » et aux dispositions du Règlement général sur la protection des données.

LA CNIL ÉLUE À LA PRÉSIDENCE DE LA CONFÉRENCE INTERNATIONALE

La CNIL élue à la tête de la Conférence internationale des commissaires à la protection des données et de la vie privée pour un an.

Membre du comité exécutif de la Conférence depuis 2014, la CNIL tient un rôle actif dans ce forum regroupant les autorités du monde entier. La Conférence est un lieu d'échanges où les 120 membres partagent bilans, bonnes pratiques respectives et adoptent des positions communes.

En 2017, la Conférence s'est penchée particulièrement sur le sujet *"Safe Government Information Sharing"* et a également adopté des positions communes sur :

- La protection des données dans les véhicules automatisés et connectés ;
- La coopération internationale ;
- La collaboration avec les autorités de protection des consommateurs.

ICDPPC
International Conference of Data Protection & Privacy Commissioners

Pour 2018, la CNIL a proposé un programme de travail ambitieux :

La Conférence internationale a décidé de mener une série de consultations sur son avenir et sur la manière dont elle peut devenir un organisme plus structuré, offrant un cadre de coopération plus performant. La CNIL et l'Autorité Fédérale Canadienne organiseront cette consultation en partenariat avec les réseaux régionaux : Europe, Asie-Pacifique, réseaux francophone et ibéro-américain, etc. Des propositions concrètes seront portées lors de la prochaine réunion annuelle.

Le thème de la prochaine réunion entre membres portera sur l'Intelligence Artificielle. Les autorités ont souhaité travailler ensemble sur cet enjeu majeur de la vie privée.

La prochaine Conférence se tiendra en octobre 2018 à Bruxelles, symbole important l'année de l'entrée en application du RGPD.

FRANCOPHONIE : LES 10 ANS DE L'AFAPDP

Depuis sa création en 2007, le secrétariat de l'Association francophone des autorités de protection des données personnelles (AFAPDP) est assuré par la CNIL. En 2017, l'AFAPDP a célébré son dixième anniversaire et mené de nombreuses activités, avec l'appui des agents de la CNIL.

La Francophonie : un espace dynamique

En 2017, 60 des 84 États et Gouvernements membres de la Francophonie disposent d'une loi et 50 d'entre eux d'une autorité. Cette attention à la protection des données personnelles se mesure également à la proportion de pays francophones candidatant à une adhésion à la Convention 108 du Conseil de l'Europe et obtenant des avis favorables concernant leur demande.

Comme chaque année, les représentants de ces autorités francophones se sont réunis à l'invitation de l'AFAPDP : la 10e Conférence francophone s'est déroulée à Gammarth, en Tunisie le 5 septembre 2017. Identification biométrique ; rôle du délégué à la protection des données ; nouveau règlement européen sur la protection des données et protection des données personnelles dans l'action humanitaire internationale ont rythmé les discussions. L'AFAPDP a tenu le lendemain sa 11e Assemblée générale extraordinaire, à l'occasion de laquelle une résolution sur l'accompagnement du développement de l'intelligence artificielle, initiée par la CNIL, a été adoptée.

Porter la voix des francophones à l'international

Afin d'encourager une plus grande diversité culturelle, et notamment une meilleure représentation des francophones au sein de la conférence mondiale, l'AFAPDP consacre chaque année une partie de son budget au financement de la traduction simultanée de la dite Conférence. Elle favorise également la participation à celle-ci de représentants d'autorités francophones, récemment installées ou ne disposant des ressources suffisantes, en prenant en charge intégralement leur déplacement. Cette année, six représentants d'autorités francophones ont pu bénéficier de cette prise en charge. Par ailleurs, le Comité exécutif de la Conférence mondiale a accueilli un nouveau membre francophone, en la personne de Marguerite Ouédraogo, Présidente de la Commission de l'informatique et des libertés du Burkina Faso et Vice-présidente de l'AFAPDP. Cette élection est une avancée pour l'AFAPDP dans son combat pour le multiculturalisme.

Un espace francophone performant

L'échange de bonnes pratiques et le renforcement des capacités sont au cœur des missions de l'AFAPDP. Si l'espace francophone est dynamique, l'association entend contribuer à le rendre toujours plus performant. À cet égard, la CNIL et d'autres institutions membres expérimentées, jouent un rôle moteur. Plusieurs sessions de formation sur les techniques de contrôle se sont tenues, en ligne et en présentiel, au cours de l'année 2017, réunissant plus de trente agents issus de 16 pays différents.

10 ans de l'AFAPDP

À l'occasion du dixième anniversaire de l'AFAPDP, la CNIL a souhaité recevoir tous les membres de l'AFAPDP à Paris. Une consultation sur le futur de la Conférence internationale a aussi été organisée. Les autorités francophones se sont fortement mobilisées : 17 pays sur 19 étaient représentés et les discussions ont été fructueuses.

Les membres ont par la suite été conviés à se rendre au siège de l'Organisation internationale de la Francophonie pour une célébration plus festive. L'AFAPDP avait pour l'occasion organisé une discussion avec des écrivains francophones d'horizons variés, autour de la notion d'intimité. Faire un pas de côté sur les sujets qui intéressent les membres, confronter des points de vue et stimuler la réflexion étaient les objectifs poursuivis par cet exercice singulier.

Enfin, l'AFAPDP a souhaité dresser le bilan d'une décennie de coopération francophone et analyser les nouveaux défis qui se présentent à elle. Ces réflexions ont fait l'objet d'une publication disponible sur le site internet de l'association : « 2007-2017 : 10 ans d'AFAPDP ».

En 2018, les membres de l'AFAPDP se réuniront une nouvelle fois à Paris pour la 11ème Conférence francophone et la 12ème assemblée générale du réseau, accueillies pour la première fois par la CNIL.

POUR EN SAVOIR PLUS > www.afapdp.org / twitter : @afapdp

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

Lionel
Juriste
et Bernard
Auditeur des systèmes d'information au service des contrôles

Concrètement, notre métier consiste, par le biais de contrôles sur place, sur pièces, en ligne ou par des auditions, à consulter et copier des échantillons représentatifs des données personnelles collectées et à interroger les responsables, afin de comprendre pour quelles finalités et dans quelles conditions les données sont traitées.

Notre activité nécessite une bonne synergie entre compétences juridiques et informatiques : c'est pourquoi une équipe de contrôle est le plus souvent composée d'un juriste et d'un auditeur des systèmes d'information.

Le juriste présente le cadre juridique du contrôle. Il veille au respect des droits des personnes auxquelles se rapportent les données. Il analyse les contrats conclus avec les consommateurs, employés, prestataires et partenaires.

L'auditeur des systèmes d'information assure la sécurité des pièces informatiques copiées et procède à leur analyse. Il évalue le niveau de sécurité des systèmes d'information et effectue les requêtes informatiques nécessaires pour vérifier le respect de la législation relative à la protection des données personnelles.

Nous effectuons un à trois contrôles par semaine, par exemple auprès de fournisseurs d'accès à internet, de start-ups, de centres d'appels, de compagnies aériennes, d'entreprises équipées d'un système de vidéosurveillance ou de sociétés d'assurance.

Nous animons également des sessions d'information auprès des Correspondants Informatique et Libertés sur le déroulement d'un contrôle et sur la sécurité informatique.

CONTRÔLER

La CNIL a réalisé 341 contrôles en 2017, conformément à ce qu'elle s'était fixée dans le cadre de son programme annuel qui en prévoyait 300.

Les missions effectuées cette année ont permis d'amorcer la nouvelle stratégie de contrôle de la CNIL qui consiste, notamment dans le cadre de l'application prochaine du règlement européen sur la protection des données, à effectuer des contrôles approfondis auprès des organismes, en utilisant l'ensemble des modalités de contrôle à disposition, à savoir les contrôles sur place, en ligne, sur pièces et les auditions.

La CNIL a ainsi procédé à **65 contrôles en ligne** et à près **d'une vingtaine de contrôles sur pièces** qui permettent de recueillir des éléments d'information parfois en amont d'un contrôle sur place. La CNIL continue par ailleurs d'effectuer des contrôles sur les - trop - nombreuses violations de données issues de failles de sécurité des systèmes d'information.

47 contrôles ont permis à la CNIL de s'assurer de la conformité des dispositifs de vidéoprotection et de vidéosurveillance, qu'il s'agisse de vérifications diligentées sur le fondement de plaintes ou à l'initiative de la Commission. Ces contrôles ont permis de rappeler aux organismes concernés le régime juridique applicable, qui ressort tant du code de la sécurité intérieure que de la loi Informatique et Libertés, en fonction du positionnement des caméras.

La CNIL a en outre réalisé une cinquantaine d'audits à l'occasion du *Sweep Day*.

En 2017, 73 % des missions de contrôle réalisées ont concerné le secteur privé, 27 % le secteur public.

Bilans du programme annuel 2016

Ces bilans font suite aux premiers éléments présentés dans le rapport d'activité 2016.

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

Le dispositif « SNIIRAM » (Système national d'information inter-régimes de l'assurance maladie) mis en œuvre par la CNAMTS (Caisse nationale de l'assurance maladie des travailleurs salariés) contient plusieurs dizaines de millions de données sensibles relatives à la santé des assurés sociaux (acte médical, feuille de soins, séjour hospitalier, etc.). Ce système vise notamment à contribuer à une meilleure gestion des politiques de santé.

À la suite d'un rapport de la Cour des comptes paru en 2016 faisant état d'une sécurité insuffisante des données du SNIIRAM, la CNIL a conduit une série de contrôles au sein de la CNAMTS, du centre d'hébergement des données, du prestataire en charge du développement, d'une caisse primaire d'assurance maladie ainsi qu'auprès d'un destinataire des données. Les vérifications ont porté sur les conditions de sécurité des données traitées et ont permis de mettre en évidence des insuffisances au regard des exigences de la loi Informatique et Libertés. Les manquements relevés par la CNIL portent notamment sur la pseudonymisation des données, les procédures de sauvegarde, l'accès aux données par les utilisateurs et par des prestataires, la sécurité des postes de travail des utilisateurs, les extractions de données individuelles ainsi que la mise à disposition d'extractions de données agrégées aux partenaires.

Compte-tenu de ces insuffisances sur des données particulièrement sensibles, la Présidente de la CNIL a décidé de mettre en demeure la CNAMTS de prendre toute mesure utile pour garantir la sécurité et la confidentialité des données des assurés sociaux conformément aux dispositions de l'article 34 de la loi Informatique et Libertés. Cette mise en demeure a été rendue publique en février 2018.

341
CONTRÔLES

DONT

65
CONTRÔLES EN LIGNE

47
CONTRÔLES VIDÉO

INFOSPLUS

L'origine des contrôles

62 %
sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;

15 %
résultent du programme annuel décidé par les membres de la Commission ;

17 %
s'inscrivent dans le cadre de l'instruction de plaintes ;

6 %
sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction.

Les courtiers en données (Data brokers)

Le marché de la valorisation de la donnée à des fins publicitaires n'a cessé d'évoluer ces dernières années. Si le cœur de métier du marketing direct consistait, il y a une décennie, essentiellement en la revente de coordonnées aux fins d'envoi de prospection électronique par des annonceurs, leur activité s'est considérablement complexifiée pour se concentrer sur la segmentation et la valorisation de profils de consommateurs.

En 2016, la CNIL a procédé à 53 contrôles auprès des différents types d'acteurs liés à l'activité des courtiers de données « data brokers » qui agrègent, enrichissent, transforment et commercialisent les données.

Ces contrôles ont principalement eu pour objectif d'identifier les acteurs concernés et leur rôle dans le traitement de données collectées par certains et réutilisées par d'autres.

Ces contrôles révèlent, d'une manière générale, que les personnes concernées ne sont pas suffisamment informées sur le sort ultérieur de leurs données à l'issue de leur première collecte et que plus il y a d'intermédiaires impliqués, moins la démonstration du consentement initial de la personne n'est assurée.

Au vu des constats effectués et dans la perspective du Règlement européen, la Commission reviendra en 2018 vers chacun des organismes contrôlés et, par ailleurs, émettra des recommandations pour assurer une plus grande maîtrise des personnes sur le cycle de vie de leurs données tout en assurant une réponse pragmatique et claire aux professionnels du secteur.

Cette transparence sera notamment garantie par la nécessité pour ces acteurs de recueillir un consentement préalable, spécifique et éclairé, avant tout traitement ou toute transmission de données. Cela permettra de faciliter l'exercice des droits des personnes et, notamment, des droits d'accès, de rectification, de suppression et d'opposition ainsi que leur droit au retrait du consentement.

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, d'abord à titre expérimental, en 2013, puis créé de manière pérenne par décret du 26 septembre 2014. Mis en œuvre par les ministres de l'intérieur, de la défense, des douanes et en charge du transport, API-PNR vise notamment à prévenir des délits et crimes graves, les actes de terrorisme, ainsi que les atteintes aux intérêts fondamentaux de la Nation. Il traite les données de réservation (PNR) et d'enregistrement (API) des passagers et des équipages transmises par les transporteurs aériens pour les vols à destination ou en provenance du territoire national, à l'exception des vols intérieurs.

Compte-tenu de la mise en place progressive du dispositif, les vérifications ont débuté dès lors qu'il est devenu opérationnel. Une série de contrôles a ainsi été menée auprès de l'Unité Information Passagers en charge de la collecte des données, de services ministériels utilisateurs du dispositif ainsi qu'auprès de compagnies aériennes contribuant à son renseignement. Les constatations effectuées ont permis de relever des insuffisances liées notamment à des dysfonctionnements dans l'application de gestion des données, lors de leur transmission aux services utilisateurs, et dans le respect des droits des passagers (information et accès aux données). Les ministres concernés ont été destinataires des points nécessitant une mise en conformité au regard des dispositions encadrant le traitement.

Premiers éléments sur le programme annuel 2017

Ces premiers éléments portent sur les contrôles réalisés dans le cadre du programme annuel des contrôles pour 2017, actuellement en cours d'instruction et qui feront l'objet d'un bilan définitif dans le rapport d'activité 2018.

La confidentialité des données de santé traitées par les sociétés d'assurance

Les sociétés d'assurance sont appelées à traiter de nombreuses données à caractère personnel, et en particulier de données relatives à l'état de santé de prospects souhaitant souscrire un contrat d'assurance ou encore de clients lors de la déclaration d'un sinistre ou d'une demande de prestations.

Dans la perspective d'une régulation du secteur, la CNIL a adopté un pack de conformité « Assurance » en novembre 2014 afin notamment d'encadrer le traitement de données de santé au regard de l'obligation de secret médical. Ce pack de conformité fait expressément référence à la convention dite « AERAS », signée par les différents acteurs du secteur et intégrant un code de bonne conduite concernant la collecte et l'utilisation des données relatives à l'état de santé des assurés en vue de la souscription ou de l'exécution d'un contrat d'assurance.

Deux ans après l'adoption de ce pack, la CNIL a souhaité s'assurer de la conformité des sociétés d'assurance aux règles de confidentialité des données de santé et au respect du secret médical.

Des missions d'investigation ont majoritairement été conduites auprès de grands acteurs du secteur, y compris leurs agences commerciales, ainsi qu'auprès d'un courtier en assurances et d'un prestataire, délégataire de gestion des données de santé pour le compte d'assureurs. Ces contrôles ont porté principalement sur l'information délivrée aux prospects/clients au moment de la collecte de leurs données de santé ainsi que sur les conditions garantissant leur confidentialité et leur sécurité. Il ressort des premiers éléments constatés que les organismes d'assurance, conscients de la sensibilité des données qu'ils traitent, ont mis en place certaines mesures de nature à préserver la confidentialité et la sécurité de telles données. Toutefois, la CNIL poursuit son analyse afin de déterminer si les garanties apportées sont suffisantes au regard des exigences légales.

Les fichiers de renseignement

Le contrôle des fichiers de renseignement a concerné d'une part les fichiers dits de renseignement territorial, mis en œuvre par les services centraux et locaux de police et de gendarmerie, et d'autre part le fichier STARTRAC mis en œuvre par le service TRACFIN du ministère de l'action et des comptes publics. Le service des contrôles de la CNIL a

ainsi procédé à des investigations sur quatre fichiers de renseignement à ce stade.

Deux d'entre eux sont des traitements relatifs au recueil et à l'analyse d'informations relatives au comportement et à l'activité d'individus suivis par les services compétents (PASP et GIPASP, respectivement mis en œuvre par la police nationale et la gendarmerie nationale). Exploités dans le cadre des missions de police administrative, ces fichiers ont pour objet de faciliter la prévention des atteintes à la sécurité publique en adaptant le suivi ou, le cas échéant, en intervenant afin d'empêcher l'atteinte.

Le troisième fichier contrôlé, dénommé EASP, a pour objet de centraliser et conserver le résultat des enquêtes administratives réalisées par les services de police à la demande du préfet compétent. Ces enquêtes sont réalisées dans le cadre de l'accès à certains types d'emploi (magistrats, policiers, agents de sécurité notamment) pour lesquels l'État vérifie si la personne répond aux « conditions de moralité » requises pour ces fonctions. La conservation des données obtenues par les services de police lors de ces enquêtes a pour finalité de faciliter la réalisation de vérifications ultérieures et d'améliorer leur suivi.

Enfin, le fichier STARTRAC a été contrôlé en tant que fichier de renseignement mis en œuvre par le service à compétence nationale TRACFIN chargé, notamment, de la lutte contre le blanchiment d'argent et le financement du terrorisme.

Pour l'ensemble de ces fichiers, les investigations menées ont principalement eu pour objet d'analyser les modalités de gestion des fichiers par les services centraux, et d'exploitation par leurs utilisateurs. Les constats ont plus particulièrement porté sur la doctrine d'utilisation de tels fichiers, la pertinence des données enregistrées, le respect des durées de conservation ainsi que les modalités de partage entre services de renseignement.

Les constats opérés font actuellement l'objet d'une instruction par les services de la CNIL.

La télévision connectée (« SMART TV »)

L'expression « télévision connectée » désigne le fait, via son accès internet, de consulter des programmes de télévision et d'utiliser des services connexes (ex : vidéo à la demande ou « Replay ») au moyen d'un téléviseur, d'un smartphone, d'une tablette, d'un ordinateur. Ce service implique le partage d'un grand nombre de données personnelles, ce qui a incité la CNIL à inscrire cette thématique à son programme annuel des contrôles.

Avant de procéder à des missions de vérification, la Commission a jugé utile de rencontrer le Conseil supérieur de l'audiovisuel (CSA) et l'Autorité de régulation des communications électroniques et des postes (ARCEP), qui contrôlent également ce secteur en tant que régulateurs.

Puis, afin d'avoir une vue d'ensemble des acteurs et de leurs rôles respectifs, la CNIL a procédé à une série de contrôles, en ligne et sur place, auprès de neuf organismes : des éditeurs de chaînes de télévision, des fournisseurs d'accès à internet et des fabricants de téléviseurs connectés.

Les contrôles ont notamment permis de révéler la grande variété des données collectées par ces différents acteurs telles que les coordonnées du téléspectateur couplées à l'historique détaillé des programmes visualisés. La CNIL poursuit ses travaux afin de déterminer si les données ainsi collectées sont proportionnées aux finalités poursuivies, si les durées de conservation appliquées sont justifiées, et si l'information des téléspectateurs ainsi que les mesures de sécurité mises en œuvre sont suffisantes.

GROS PLAN

JOUETS CONNECTÉS

Les jouets connectés, qui prennent souvent la forme d'objets d'apparence anodine (poupées, robots, babyphones), sont de plus en plus prisés des enfants. Ils doivent néanmoins conduire à une attention particulière des consommateurs notamment en ce qui concerne la sécurité de leurs données personnelles.

En 2017, la CNIL a effectué des missions de vérification sur deux jouets connectés, le robot « I-QUE » et la poupée « My Friend Cayla ». Ces jouets, équipés d'un microphone et d'un haut-parleur, répondent aux questions des enfants sur des sujets divers tels que les fées et les dinosaures. La réponse est extraite d'internet et donnée à l'enfant par l'intermédiaire de ces objets.

Les contrôles réalisés ont permis de relever que la société hongkongaise, qui commercialise ces jouets, collecte par leur intermédiaire une multitude d'informations personnelles sur les enfants et leur entourage, notamment leur voix et le contenu des conversations échangées. Plus encore, il a été constaté que le défaut de sécurisation des jouets permet à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des adultes les entourant, et d'avoir ainsi accès aux discussions échangées dans un cercle familial ou amical.

Au vu de ces éléments, la Présidente de la Commission a considéré que les traitements mis en œuvre n'étaient pas conformes à la loi Informatique et Libertés, en raison du non-respect de la vie privée des personnes et de l'absence d'information des personnes concernées, et a décidé en conséquence de mettre en demeure le responsable de traitement (la société Genesis Industries Limited) d'adopter des mesures correctrices sous un délai de deux mois. Cette mise en demeure a été rendue publique en décembre 2017.

Bilan des actions coordonnées au niveau européen et international

En 2017, la CNIL a, pour la cinquième année consécutive, contribué aux actions menées par les autorités européennes et internationales de protection des données en participant au « *Sweep Day* ». Elle a par ailleurs mené des contrôles auprès de WhatsApp dans le cadre d'une coopération avec d'autres autorités européennes de protection des données.

Sweep day : de quel contrôle les utilisateurs disposent-ils sur leurs données à caractère personnel ?

En 2017, la CNIL a contribué à une opération d'audit coordonnée dans le cadre du « *Sweep Day* », menée par 24 autorités de protection des données membres du *Global Privacy Enforcement Network* (GPEN - réseau d'organismes agissant au sein de l'OCDE pour la protection de la vie privée). Cette opération a porté sur 455 sites internet et applications mobiles de la vie quotidienne dans les secteurs bancaire, du commerce en ligne, du voyage, des réseaux sociaux, des jeux, de la santé et de l'éducation.

Cet audit international a révélé que les politiques de confidentialité des acteurs contrôlés étaient floues, imprécises et comportaient des clauses génériques, que l'information était globalement insatisfaisante concernant le devenir des données et la nature des organismes avec lesquels elles sont partagées. Il a été relevé également l'absence d'information sur les garanties prises pour assurer la sécurité des données des utilisateurs et un manque de clarté sur le pays hébergeant les données et les mesures de protection mises en œuvre. Enfin, il a été constaté que seule la moitié des sites et applications informait les utilisateurs sur leur droit d'accès à leurs données et les modalités pour l'exercer.

Au niveau national, la CNIL a concentré son audit sur 49 sites web et applications mobiles dans les domaines du « voyage » et de la « vente en ligne ». Les vérifications menées ont fait apparaitre que plus de 80 % des sites et applications informaient correctement les utilisateurs sur les finalités pour lesquelles les données étaient traitées et les modalités selon lesquelles elles étaient collectées. En revanche, la nature des données transmises à des tiers et l'identité de ces derniers n'étaient pas suffisamment indiquées par la même proportion de sites et applications. En outre, ils ne donnaient pas (ou peu) d'information sur les modalités de stockage des données et les mesures prises pour en garantir la sécurité et la confidentialité. Enfin, un tiers d'entre eux ne facilitaient pas l'accès des utilisateurs aux données les concernant, et ne fournissent pas de moyens simples et conviviaux pour en permettre l'effacement.

Les sites ayant révélé les dysfonctionnements les plus importants lors de l'audit ont fait l'objet de vérifications plus approfondies dans le cadre de procédures de contrôle formelles.

De telles actions d'audit coordonnées sont une manière, pour la CNIL et ses homologues européens, de se préparer aux futures opérations conjointes qui pourront être réalisées à partir du 25 mai 2018, le règlement européen sur la protection des données étant alors applicable.

WhatsApp

À la suite de la mise à jour des conditions générales d'utilisation de l'application Whatsapp indiquant que les données des utilisateurs seraient désormais transmises à la société FACEBOOK Inc., la CNIL a décidé de contrôler la conformité à la loi Informatique et Libertés des traitements relatifs à cette application. D'octobre 2016 à novembre 2017, elle a ainsi diligenté des contrôles en ligne et sur pièces et a procédé à une audition de la société.

Ces contrôles s'inscrivaient dans le cadre d'une coopération européenne, le G29 (groupe des CNIL européennes) ayant chargé son sous-groupe en charge de la coopération en matière d'enquêtes et de sanctions de coordonner les investigations.

CE QUI CHANGE AVEC LE RÈGLEMENT

La coopération prévue par le règlement européen

L'entrée en vigueur du règlement européen sur la protection des données, qui unifie le droit applicable au sein de l'Union européenne, va entraîner une plus grande coopération entre les différentes autorités de protection des données, notamment dans le cadre de leur pouvoir de contrôle.

En effet, en présence de traitements transfrontaliers, c'est-à-dire lorsque le responsable de traitement est établi dans plusieurs États membres ou lorsque le traitement est susceptible d'affecter sensiblement des personnes dans plusieurs États membres, les autorités pourront mener leurs investigations ensemble, sous la conduite d'une autorité chef de file. Différents mécanismes destinés à faciliter la coopération et à assurer une application cohérente du règlement ont ainsi été institués. Des enquêtes conjointes pourront être menées par les autorités et ces dernières devront se communiquer, sous un délai contraint, toutes les informations utiles, notamment celles relatives aux organismes contrôlés.

Plus concrètement, les agents de la CNIL pourront désormais se déplacer dans toute l'Union européenne pour exercer leurs missions et accéder aux locaux de responsables de traitements. Ils pourront également accueillir sur le territoire français des agents d'autres autorités pour mener ensemble ces opérations, dans le respect du droit procédural français.

Les autorités de contrôle européennes ont déjà été amenées à collaborer sur des dossiers et à coordonner leurs actions. Toutefois, les procédures restaient purement nationales et les réponses apportées étaient propres à chaque État. Désormais, les opérations menées conduiront à l'adoption d'une décision unique.

40 ans !

de contrôles

34
en 1990

33
en 1998

218
en 2008

341
en 2017

Si la CNIL a été informée que les données des 10 millions d'utilisateurs français n'avaient jamais été traitées à des fins de ciblage publicitaire, plusieurs manquements à loi Informatique et Libertés ont été constatés.

D'une part, la société WHATSAPP transmettait à la société FACEBOOK Inc. les numéros de téléphone de ses utilisateurs et leurs habitudes d'utilisation de l'application, à des fins de « business intelligence », sans base légale, en particulier sans que leur consentement, libre et spécifique, ait été valablement recueilli.
D'autre part, cette société a méconnu son obligation de coopérer avec la Commission, en refusant de lui communiquer un échantillon des données des utilisateurs français transmises à FACEBOOK Inc.
Compte tenu de ces manquements à la loi Informatique et Libertés, la Présidente de la CNIL a décidé le 27 novembre 2017 de mettre en demeure la société WHATSAPP.

SANCTIONNER

La présidente de la CNIL a prononcé 79 mises en demeure dont 3 publiques. Les responsables de traitement mis en demeure de se conformer à la loi Informatique et Libertés peuvent demander à 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.

La Présidente de la CNIL a prononcé

79
MISES EN DEMEURE
dont 6 publiques

La formation restreinte a prononcé

14
SANCTIONS

DONT

9
sanctions pécuniaires
dont 6 publiques

5
avertissements dont 2 publics

Une amende de 150 000 € à l'encontre de FACEBOOK

En 2015, à la suite de l'annonce par FACEBOOK de la modification de sa politique d'utilisation des données, la CNIL a procédé à divers contrôles afin de vérifier la conformité du réseau social à la loi Informatique et Libertés.

De nombreux manquements à la loi ont été relevés lors de ces investigations, notamment que FACEBOOK procédait à la combinaison massive des données personnelles des internautes à des fins de ciblage publicitaire et que la société traçait à leur insu les internautes, avec ou sans compte, sur des sites tiers via le cookie « datr ».

Au regard des manquements constatés, la Présidente de la CNIL a décidé, le 26 janvier 2016, de mettre en demeure les sociétés FACEBOOK INC. et FACEBOOK IRELAND de se conformer à la loi Informatique et Libertés. Les deux sociétés ayant adressé à la CNIL des réponses insatisfaisantes à un certain nombre de manquements, une procédure de sanction a été engagée à leur encontre.

La formation restreinte, chargée de prononcer les sanctions, s'est donc réunie le 23 mars 2017. Elle a considéré que :

- Concernant la combinaison de données dont font l'objet les utilisateurs de FACEBOOK, les sociétés FACEBOOK INC. et FACEBOOK IRELAND effectuent ce traitement en l'absence de base légale. En effet, si les utilisateurs disposent de moyens pour maitriser l'affichage de la publicité ciblée, ils ne consentent pas à la combinaison massive de leurs données et ne peuvent s'y opposer, que ce soit lors de la création de leur compte ou *a posteriori*.

- Concernant la collecte des données de navigation des internautes, via le cookie « datr », l'information dispensée via le bandeau d'information relatif aux cookies est imprécise et ne permet pas aux internautes de clairement comprendre que leurs données sont systématiquement collectées dès lors qu'ils naviguent sur un site tiers comportant un module social. Cette collecte est ainsi déloyale.

Sur les autres manquements, la formation restreinte a considéré que :

- Les sociétés ne délivrent aucune information immédiate aux internautes sur leurs droits et sur l'utilisation qui sera faite de leurs données notamment sur le formulaire d'inscription au service.

- Les sociétés ne recueillent pas le consentement exprès des internautes lorsqu'ils renseignent des données sensibles dans leurs profils (ex : leurs opinions politiques, religieuses ou leur orientation sexuelle).

INFOSPLUS

Les droits du plaignant précisés par le Conseil d'État

Dans une décision du 19 juin 2017, le Conseil d'État précise les droits du plaignant attaquant une décision de sanction prise par la CNIL à l'encontre d'un responsable de traitement.

Le Conseil d'État considère que le plaignant n'est pas recevable à demander l'annulation de la sanction prononcée à l'encontre de l'organisme mis en cause et qui ne serait pas assez sévère selon le plaignant. Celui-ci ne dispose d'aucun intérêt à agir dans ce cas.

En revanche, le Conseil d'État estime que lorsque la plainte conduit la CNIL à sanctionner l'organisme mis en cause, le plaignant a le droit d'obtenir communication de la nature des manquements retenus et de la teneur de la sanction prononcée, que la sanction soit publique ou non.

- En renvoyant au paramétrage du navigateur, les sociétés ne permettent pas aux utilisateurs de s'opposer valablement aux cookies déposés sur leur équipement terminal.

- Les sociétés ne démontrent pas en quoi la conservation de l'intégralité des adresses IP des internautes pendant toute la durée de vie de leur compte est nécessaire.

En conséquence, la formation restreinte de la CNIL a décidé de prononcer une sanction publique de 150 000 € à l'encontre des sociétés FACEBOOK INC et FACEBOOK IRELAND, compte tenu du nombre important de manquements, de leur gravité et du volume d'utilisateurs en France (33 millions).

La décision de la formation restreinte s'inscrit dans le prolongement des travaux conduits de manière concertée avec les autorités de protection des données de Belgique, d'Allemagne (Land d'Hambourg), d'Espagne, et des Pays-Bas. Ces autorités partagent de nombreux constats même si leurs procédures portent sur des périmètres parfois différents et s'inscrivent dans des calendriers distincts.

La décision de la CNIL a fait l'objet d'un recours devant le Conseil d'État de la part des deux sociétés.

Les recours devant le Conseil d'État

La question de la portée territoriale du déréférencement est renvoyée devant la Cour de justice de l'Union européenne

Le 10 mars 2016, la formation restreinte de la CNIL a prononcé une sanction publique de 100 000 € à l'encontre de la société Google Inc. pour ne s'être pas conformée à la mise en demeure de la Présidente de la Commission, lui enjoignant de faire droit aux demandes de déréférencement sur toutes les extensions de son moteur de recherche.

La société Google Inc. a formé un recours à l'encontre de cette sanction devant le Conseil d'État afin d'en obtenir l'annulation.

Pour rappel, le droit au déréférencement a été consacré par la Cour de justice de l'Union européenne (CJUE), dans son arrêt Google Spain du 13 mai 2014. Il permet aux internautes résidant en Europe d'obtenir des moteurs de recherche, sous certaines conditions, la suppression de la liste des résultats obtenus à la suite d'une recherche effectuée par le nom d'une personne, des liens vers des pages web publiées et contenant des informations la concernant.

Le Conseil d'État a, tout d'abord, estimé que le traitement de données à caractère personnel que constitue le moteur de recherche exploité par la société requérante est un traitement unique, effectué dans le cadre d'une de ses installations, Google France, établie sur le territoire français. Il en a déduit - contrairement à ce que soutenait la société Google Inc. - que la loi Informatique et Libertés était bien applicable et que la formation restreinte de la CNIL était compétente pour prononcer une sanction pécuniaire à son encontre.

Ensuite, le Conseil d'État a considéré que la question de savoir si le droit au déréférencement implique, lorsqu'il est fait droit à une demande, que le déréférencement soit opéré de telle sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel cette recherche est lancée, y compris hors de l'Union européenne, posait une difficulté sérieuse d'interprétation du droit de l'Union européenne. C'est pourquoi, il a décidé de saisir la CJUE.

Dans l'attente de réponse de la CJUE quant à l'interprétation à donner à la directive du 24 octobre 1995, le Conseil d'État a décidé de sursoir à statuer sur la requête de la société Google Inc.

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

FOCUS

Clôture de la mise en demeure contre Microsoft pour conformité

À la suite du lancement de Windows 10 en juillet 2015, l'attention de la CNIL a été appelée par voie de presse et de signalements de partis politiques sur de potentiels manquements à la loi Informatique et Libertés.

À l'occasion de multiples contrôles réalisés, plusieurs manquements ont été constatés et notamment : une collecte excessive de données à des fins de télémétrie, un suivi de la navigation des utilisateurs sans leur consentement et un défaut de sécurité des données des utilisateurs.

Ces constats ont conduit la Présidente de la CNIL à mettre en demeure, le 20 juillet 2016, la société MICROSOFT CORPORATION de se conformer à la loi. La réponse de la société a permis de considérer que les manquements avaient cessé. La société a, en effet, pris des mesures afin de se mettre en conformité avec les injonctions de la mise en demeure.

- La société a réduit de moitié le volume des données collectées dans le niveau de « base » de son service de télémétrie. Elle a limité cette collecte aux données strictement nécessaires pour maintenir le système et les applications en bon état de fonctionnement et assurer leur sécurité.
- Les utilisateurs sont désormais informés, par une mention claire et précise, qu'un identifiant publicitaire assure un suivi de leur navigation pour leur proposer de la publicité ciblée. En outre, la procédure d'installation de Windows 10 a été modifiée : les utilisateurs ne peuvent finaliser l'installation tant qu'ils n'ont pas activé ou désactivé l'identifiant publicitaire. Ils peuvent revenir à tout moment sur ce choix.
- La société a renforcé la robustesse du code PIN de 4 chiffres permettant aux utilisateurs de s'authentifier pour accéder à l'ensemble des services en ligne de la société et notamment à leur compte Microsoft : les combinaisons trop communes sont désormais refusées et en cas de saisie incorrecte, il existe un mécanisme de temporisation d'authentification (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives).

En outre, la société a :
- inséré des mentions d'information conformes à l'article 32 de la loi Informatique et Libertés ;
- effectué des demandes d'autorisation auprès de la CNIL pour ses traitements de lutte contre la fraude ;
- adhéré au Privacy Shield pour régir les transferts internationaux de données personnelles ;
- mis fin au dépôt de cookies sans recueil préalable du consentement des internautes lors de la consultation de la plupart de ses sites web Windows 10 et s'est engagée à le faire pour l'ensemble avant le 30 septembre 2017.

La Présidente de la CNIL a considéré que la société s'était mise en conformité avec la loi Informatique et Libertés et a ainsi décidé clôturer la procédure de mise en demeure.

Ce modèle d'organisation au sein de ce réseau est emblématique des bonnes pratiques à développer au sein de tous les secteurs d'activités privés, publics ou associations.

ANTICIPER
et innover

En 2017, la CNIL a poursuivi le développement de son laboratoire d'innovation numérique. À la fois dispositif de veille, média de prospective et incubateur de projets d'innovation et d'expérimentation, LINC se veut un miroir de l'activité du régulateur au prisme des tendances émergentes du numérique. De la *smart city* aux assistants vocaux intelligents en passant par une interpellation sur le rôle des algorithmes dans notre vie, tour d'horizon d'une année de faits et idées porteurs d'avenir.

Amandine
Ingénieure Experte, Service de l'Expertise Technologique

Nous sommes 12 experts au sein du service (ingénieurs, chercheurs, consultants ou designer), chacun avec ses spécialités (cybersécurité, biométrie, objets connectés, big data, cryptographie, blockchain, anonymisation et pseudonymisation, 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 et les évolutions 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, notamment dans le cadre du G29. Je participe ainsi au sous-groupe eGov du G29 qui traite des problématiques régaliennes ainsi que de gestion de l'identité numérique.

Nous sommes également actifs dans le domaine de la normalisation au sein de l'ISO : la CNIL participe ainsi à l'élaboration des normes techniques qui serviront demain de référentiel à l'élaboration de nouveaux produits ou services. En intervenant ainsi très en amont nous nous assurons qu'un maximum d'entreprises pourra traiter et respecter la réglementation.

LES DONNÉES PERSONNELLES AU CŒUR DE LA FABRIQUE DE LA *SMART CITY*

Le 10 octobre 2017, la CNIL publiait son cinquième cahier Innovation et prospective, qui présente une exploration des enjeux politiques et sociaux émergeants autour de la place des données dans la ville.

La plateforme d'une ville contribue aux débats et questionnements en cours sur la smart city, à travers un éclairage propre à la CNIL. Ce cahier souligne les conséquences de la massification des données sur les politiques publiques urbaines et en particulier sur les rapports public-privé. Il propose également de remettre en perspective la ville au prisme de l'économie des plateformes, et des équilibres entre acteurs publics, acteurs privés et citoyens. Il s'adresse à tous les acteurs et notamment aux collectivités locales qui font face à de nouvelles problématiques.

Quelle place pour l'individu dans la *smart city*

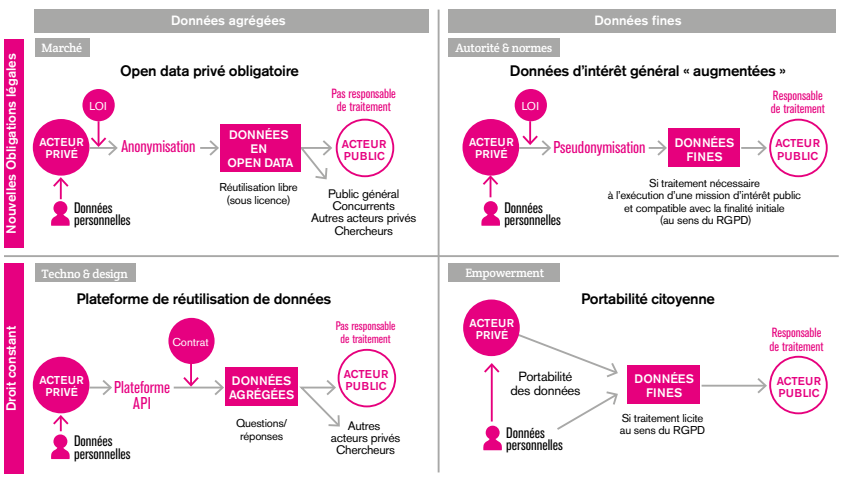
Après une première partie décrivant les limites de l'expression « *smart city* », la mise en données de la ville numérique est abordée selon trois angles :

- L'arrivée des grandes plateformes du numérique dans les services urbains (Sidewalk CityLab, Waze Connected Citizen de Alphabet/Google, Uber ou Facebook), qui permet d'analyser les contreparties demandées aux individus et aux acteurs publics pour des services présentés comme gratuits ;
- La promesse de la ville fluide et sans frictions, qui pose la question des droits des individus, parfois réduits à une somme d'éléments à optimiser par la technologie ;
- Les impératifs de sécurité et la généralisation des dispositifs de captation, qui mettent à mal l'anonymat pourtant constitutif de la ville.

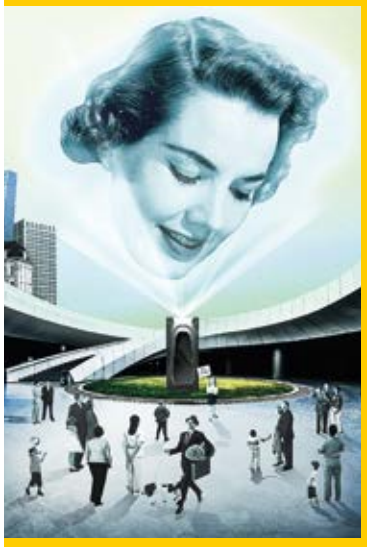
Des recommandations et quatre scénarios prospectifs

Le cahier formule de nombreuses recommandations et il explore notamment quatre scénarios prospectifs de régulation pour engager un rééquilibrage privé/public par les données, en tentant d'apporter des réponses aux questions suivantes : comment organiser un retour vers l'acteur public de données produites dans les services portés par des acteurs privés ? Comment permettre aux acteurs publics de réutiliser des données à forte valeur ajoutée pour des finalités d'intérêt général, dans le respect des droits des et libertés des personnes concernées ?

Ces quatre scénarios, présentés dans une matrice à quatre entrées comme autant de leviers actionnables, envisagent notamment des configurations privilégiant le recours à un open data privé obligatoire, des données d'intérêt général augmentées, le recours à des plateformes d'accès aux données, ou encore la portabilité citoyenne. Sans privilégier l'un ou l'autre de ces scénarios il s'agit de présenter l'économie générale de chacun, de souligner leurs potentialités et de mettre en lumière les enjeux qu'ils soulèvent pour la protection des données personnelles des citoyens.



Le cahier IP 5 est distribué avec son tiré à part, « Voyage au centre de la ville de demain », qui expose trois scénarios à horizon 2026 conçus dans le cadre d'ateliers de design fiction, organisés et animés par la CNIL en partenariat avec Five by Five (agence d'innovation) et Usbek & Rica (magazine d'exploration du futur).



Parmi ces scénarios-fictions, Marianne Reloaded : une intelligence artificielle disponible sur smartphone ou sous la forme d'un hologramme, avec laquelle des citadins peuvent communiquer, porter réclamation ou proposer des suggestions. En croisant ces retours avec les données locales et les informations collectées par les capteurs de la ville, la municipalité optimise son processus décisionnel en temps réel, anticipant les besoins des citadins.

Les invités de LINC

LINC s'incarne également dans les locaux de la CNIL, par un espace de démonstration, d'ateliers et de rencontres entre des acteurs des questions de données numériques et la CNIL.

En 2017, LINC a accueilli près de 500 personnes (agents de la CNIL, agents publics ou experts) dont Tristan Nitot, Serge Abiteboul, Bilel Benbouzid, la startup Drust, ou encore Geoffrey Dorne.

DE L'EXERCICE FACILITÉ DU DROIT AU DÉRÉFÉRENCEMENT À LA RENCONTRE AVEC « HALLY L'ORACLE DU NET » : LES OUTILS EN BÊTA TEST

LINC est également un dispositif de conduite de projets d'expérimentation et de prototypage d'outils, de services ou de concepts visuels autour des données. Cette activité d'innovation publique prend donc différentes formes concrètes, au-delà des travaux de veille et de prospective : il s'agit pour la CNIL de tester et proposer ses propres outils ou d'apporter son expertise à des projets lancés par d'autres, avec comme objectif d'apprendre à partir des retours et des réactions, tout en proposant des outils fonctionnels.

Cette approche de bêta test peut s'appliquer au développement d'outils à destination des professionnels comme pour l'outil PIA ou la datavisualisation des articles du RGPD.

Mais il s'agit aussi de proposer des outils au grand public. En 2017, ce choix s'est incarné en particulier dans deux outils, aujourd'hui utilisables par tout un chacun.

Un outil pour aider à exercer son droit au déréférencement et à vérifier l'effectivité de ce droit

Le premier est un projet interne qui a été transformé et mis en forme pour être utilisable par les citoyens, afin de répondre à un besoin : comment suivre l'état d'avancement et l'effectivité d'une demande de déréférencement ?

Depuis 2014 le droit au déréférencement permet aux citoyens européens de demander à un moteur de recherche de supprimer certains résultats de recherche associés à leurs noms et prénoms. La demande de déréférencement implique dans un premier temps de vérifier si le résultat à déréférencer apparaît dans les résultats de recherche. Mais comme il peut y avoir un grand nombre de résultats pour une requête, la vérification peut s'avérer fastidieuse si le résultat n'apparaît qu'après un grand nombre de pages. Par ailleurs, l'ordre des résultats peut varier suivant de nombreux critères, comme votre adresse IP, votre historique de recherches, ou la date de la requête. Ainsi, ce n'est pas parce qu'un résultat n'apparaît plus sur une page donnée qu'il a forcément été déréférencé.
Pour vérifier l'effectivité de l'exercice de vos droits, LINC a développé une extension pour trois navigateurs (Firefox, Chrome et Opéra) qui permet de déterminer si un lien apparaît ou non parmi l'ensemble des résultats d'un moteur de recherche, à la saisie du nom. Cette extension peut ainsi simplifier les démarches en déterminant rapidement si un résultat apparait et s'il a bien été déréférencé suite à une demande.

Comme toujours pour les projets de la CNIL, cette extension est, en code source ouvert et sous licence libre (GNU GPL v3.0). Toute personne intéressée peut y contribuer sur le github de LINC.

Hally, l'oracle du net vous révèle comment les plateformes choisissent des contenus pour vous

Hally est un tout autre type de rencontre. Dans un contexte où les algorithmes sont mis en débat dans le cadre de la nouvelle mission de la CNIL sur l'éthique du numérique, LINC a souhaité accompagner un projet de design dont l'objectif est d'inviter les internautes à s'interroger sur la manière dont les algorithmes les calculent lorsqu'ils naviguent sur le web.

L'oracle du net s'incarne dans un personnage, Hally, qui va accompagner les internautes dans leur navigation sur les réseaux sociaux et moteurs de recherche, afin de révéler le fonctionnement des algorithmes et enjeux qui y sont associés. En mobilisant une interface d'utilisation originale et ludique permettant de « gratter » et de découvrir d'autres couches du web, l'oracle du net fait prendre conscience des mécanismes sous-jacents qui conditionnent la manière dont les internautes accèdent, interagissent et réagissent à l'information

In fine l'oracle encourage l'utilisateur à réfléchir au fonctionnement de ces services afin qu'il ne se laisse pas enfermer dans des calculs algorithmiques et qu'il conserve son libre arbitre.

Concrètement, le parcours se déroule en 3 étapes :

1 Tout d'abord sur le site de l'oracle du net, Hally dresse un premier portrait du visiteur. Cette première étape a vocation à interpeller l'internaute et à l'inviter à en savoir plus en téléchargeant Hally sous forme d'extension navigateur.

2 L'extension offre ensuite la possibilité de pouvoir gratter certaines pages web et d'accéder ainsi à de nouvelles informations permettant de mieux comprendre, par exemple, comment sont hiérarchisées les informations ou construites certaines recommandations ou suggestions de contacts, d'amis, ou de sujets d'intérêts.

3 Enfin, les plus curieux qui auront gratté suffisamment de zones d'une page, pourront accéder à une troisième couche mettant en évidence de manière plus conceptuelle certaines grandes tendances du web et offrant des conseils pour « hacker leur auto-prophétie ».

Là aussi, l'ensemble du code est accessible sur Github sous licence creative commons BY-NC-SA et il est ouvert à la communauté pour son enrichissement et sa réutilisation éventuelle sur d'autres pages web.

POUR EN SAVOIR PLUS ET INSTALLER CES EXTENSIONS, RENDEZ-VOUS SUR
> linc.cnil.fr, onglet « Expérimentations »

FOCUS

Linc.fr

En 2017, l'espace éditorial LINC (https://linc.cnil.fr) passe la barre des 150 publications, en français et en anglais.

À l'avant-garde des activités de prospective de la CNIL, les sujets explorés auront été nombreux, depuis la blockchain jusqu'à l'intelligence artificielle et les chatbots, en passant la régulation des plateformes de l'économie du partage et les « Learning Analytics ». LINC apporte un angle vie privée sur des sujets au cœur des débats en cours et à venir.

Dans sa partie expérimentation, le site LINC explore sous forme de datavisualisation les données anonymisées des taxis new-yorkais pour déterminer des scénarios d'usages pour lesquels l'anonymisation n'altère pas la qualité des résultats (voir infra.).

Dans un onglet Publications, téléchargez au format pdf l'ensemble des Cahiers IP et des Lettres innovation et prospective. (https://linc.cnil.fr/publications).

2017 : LA CNIL S'EMPARE DE SA NOUVELLE MISSION ÉTHIQUE

et éthique numérique
les algorithmes en débat

Algorithmes et intelligence artificielle : une indispensable réflexion éthique

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 de traiter dès janvier 2017 le thème des algorithmes et de l'intelligence artificielle.
Dans notre monde de plus en plus numérique, les algorithmes et l'intelligence artificielle sont partout : pour simuler l'évolution de la propagation de la grippe en hiver, pour recommander des livres à des clients, pour suggérer aux forces de police des zones où patrouiller en priorité, pour piloter de façon autonome des automobiles, pour élaborer automatiquement un diagnostic médical personnalisé, pour individualiser un fil d'activité sur les réseaux sociaux, etc. Des tâches complexes, parfois critiques, sont ainsi déléguées à des systèmes de plus en plus autonomes à mesure que les techniques d'apprentissage propres à l'intelligence artificielle se développent.
L'irruption dans nos vies quotidiennes des algorithmes et de l'intelligence artificielle fait l'objet d'une attention publique soutenue, depuis que quelques cas emblématiques (APB, rôle des réseaux sociaux dans les présidentielles américaines, etc.) ont marqué les citoyens, ici en France ou à l'étranger.

Un débat public ouvert et décentralisé pour une réflexion pluraliste

Pour conduire cette réflexion, la CNIL a animé un débat public ouvert et décentralisé de janvier à octobre 2017 : 3 000 personnes ont participé à 45 manifestations qui se sont tenues à l'initiative de 60 partenaires (administrations, entreprises, universités, syndicats, fédérations professionnelles) dans toute la France et ont porté sur divers secteurs (éducation, santé, culture, sécurité, justice, etc.). Une concertation citoyenne a également été organisée à Montpellier le 14 octobre. Le 15 décembre, la CNIL a présenté le rapport de synthèse du débat public en présence de Mounir MAHJOUBI, Secrétaire d'État chargé du Numérique et de Cédric VILLANI, Député, chargé par le gouvernement d'une mission sur l'intelligence artificielle.

Les problématiques soulevées par les algorithmes et l'IA

Les débats ont permis d'identifier 6 problématiques éthiques essentielles à relever :

- L'autonomie humaine au défi de l'autonomie des machines : jusqu'où déléguer tâches et décisions critiques aux machines ? Comment assurer que l'homme reste en responsabilité ?
- Biais, discrimination et exclusion : comment appréhender des effets néfastes qui, à l'heure du machine learning, peuvent se développer à l'insu même de ceux qui déploient les algorithmes ?
- Fragmentation algorithmique : comment faire en sorte que la logique de personnalisation au cœur de maints usages des algorithmes n'affecte pas des logiques collectives essentielles à la vie de nos sociétés (pluralisme démocratique et culturel, mutualisation du risque) ?
- Comment concilier le fort besoin de l'IA en données et la protection des libertés pour tirer de ces nouvelles technologies dans un cadre de confiance ?
- Qualité, quantité, pertinence des données : comment entretenir une attitude critique nécessaire à la bonne exploitation des algorithmes et de l'IA ?
- L'identité humaine au défi de l'intelligence artificielle : comment appréhender les formes de brouillage de la frontière entre humains et machines (autonomisation croissante des machines, hybridation homme/machine, développement de robots humanoïdes affectifs).

Vigilance, loyauté et recommandations pratiques : un rapport en forme de contribution à la réflexion publique

Les débats ont permis de dégager deux principes fondateurs pour une intelligence artificielle au service de l'homme. Ces principes pourraient s'inscrire dans une nouvelle génération de garanties et de droits fondamentaux à l'ère numérique, des « droits-système » organisant la gouvernance mondiale de notre univers numérique :

- Un principe de loyauté appliqué à tous les algorithmes et intégrant les impacts collectifs, et pas seulement personnels, de ces derniers. Tout algorithme, qu'il traite ou non des données personnelles, doit être loyal envers ses utilisateurs, non pas seulement en tant que consommateurs, mais également en tant que citoyens, voire envers des communautés ou de grands intérêts collectifs dont l'existence pourrait être directement affectée. L'intérêt des utilisateurs doit primer. Par exemple, un tel principe pourrait avoir vocation à s'appliquer à l'impact potentiel des réseaux sociaux sur la structure du débat public

« L'objectif de ce débat est de garantir que l'intelligence artificielle augmente l'homme plutôt qu'elle ne le supplante et participe à l'élaboration d'un modèle français de gouvernance éthique de l'intelligence artificielle. »

dans nos démocraties (segmentation du corps politique par le ciblage de l'information) ou à celui d'algorithmes de police prédictive sur des communautés ou quartiers entiers.

- Un principe de vigilance/réflexivité : il s'agit d'organiser une forme de questionnement régulier, méthodique et délibératif à l'égard de ces objets mouvants. Ce principe constitue une réponse directe aux exigences qu'imposent ces objets technologiques du fait de leur nature imprévisible, inhérente au machine learning, du caractère très compartimenté des chaînes algorithmiques au sein desquels ils s'insèrent et, enfin, de la confiance excessive à laquelle ils donnent souvent lieu. C'est l'ensemble des maillons de la chaîne algorithmique (concepteurs, entreprises, citoyens) qui doit être mobilisé pour donner corps à ce principe, au moyen de procédures concrètes (par exemple, des comités d'éthique assurant un dialogue systématique et continu entre les différentes parties-prenantes).

Ces principes fondateurs sont complétés par des principes organisationnels ayant trait à l'intelligibilité et à la responsabilité des systèmes algorithmiques ainsi qu'à la nature de l'intervention humaine dans la prise de décision algorithmique.

Les 6 recommandations opérationnelles

Ces principes font l'objet d'une déclinaison sous la forme de 6 recommandations opérationnelles à destination tant des pouvoirs publics que des diverses composantes de la société civile (entreprises, grand public, etc.) :

- Former à l'éthique tous les acteurs-maillons de la « chaîne algorithmique » (concepteurs, professionnels, citoyens) : l'alphabétisation au numérique doit permettre à chaque humain de comprendre les ressorts de la machine ;
- Rendre les systèmes algorithmiques compréhensibles en renforçant les droits existants et en organisant la médiation avec les utilisateurs ;
- Travailler le design des systèmes algorithmiques au service de la liberté humaine, pour contrer l'effet « boîtes noires » ;
- Constituer une plateforme nationale d'audit des algorithmes ;
- Encourager la recherche sur l'IA éthique et lancer une grande cause nationale participative autour d'un projet de recherche d'intérêt général ;
- Renforcer la fonction éthique au sein des entreprises (par exemple, l'élaboration de comités d'éthique, la diffusion de bonnes pratiques sectorielles ou la révision de chartes de déontologie peuvent être envisagées).

2e ÉDITION DU PRIX CNIL-INRIA : LE *PRIVACY BY DESIGN* RÉCOMPENSÉ

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.

La 2e édition, organisée en 2017, a récompensé l'article intitulé « *Engineering privacy by design reloaded* » initialement publié dans les actes de l'Amsterdam Privacy Conference 2015.

Les auteures, **Seda Gürse**, **Carmela Troncoso**, et **Claudia Diaz**, ont reçu leur trophée lors de la 11e Conférence internationale Computers, Privacy and Data Protection (CPDP) le 26 janvier 2018 en présence d'**Isabelle Falque-Pierrotin**, Présidente de la CNIL, et de **Daniel Le Métayer**, Directeur de Recherche à Inria.

L'article détaille la méthode employée par les ingénieurs en protection des données pour appliquer les stratégies de *Privacy by Design*. Les auteures distinguent et analysent différentes stratégies de minimisation (telles que la minimisation de la collecte, la capacité de liaison, la durée de conservation, la centralisation, etc.) et les relient à la minimisation des risques et au besoin de confiance. Elles fournissent des lignes directrices pour minimiser la quantité de données confiées aux responsables de traitement ou aux sous-traitants en dehors du domaine d'utilisation.

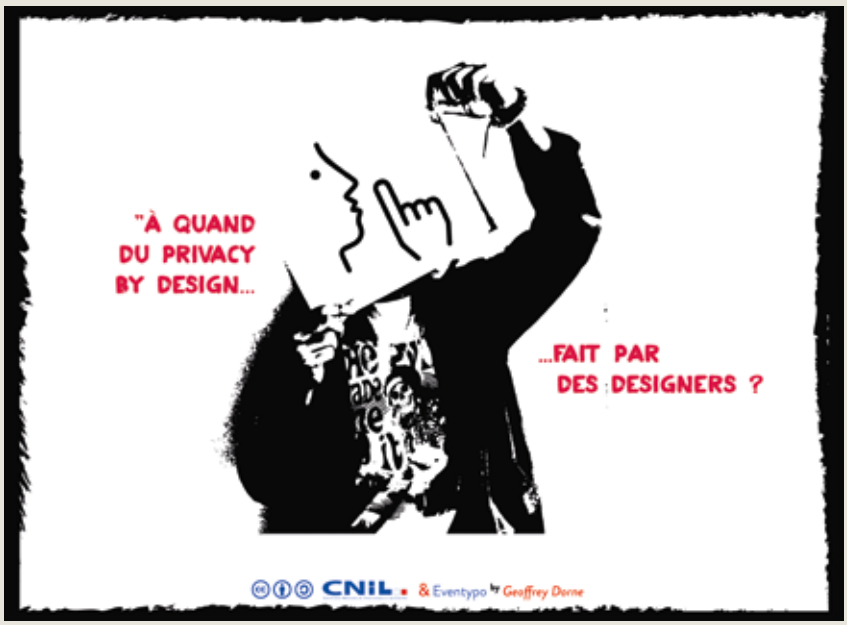
Cette approche pratique a retenu toute l'attention du jury car elle pourrait inspirer les fabricants et développeurs, un travail particulièrement utile à l'heure de la mise en œuvre du nouveau règlement européen.

Le Jury souhaite en effet encourager les travaux de recherche qui ont pour objectif de promouvoir la mise en pratique opérationnelle des principes juridiques de la protection des données souvent considérés comme abstraits.

Les sujets de réflexion en 2018

Du privacy by design au design de la privacy

Le Design sera au cœur des prochaines réflexions de la CNIL, avec l'idée d'explorer les enjeux Informatique et Libertés en mobilisant des champs disciplinaires peu utilisés jusqu'à présent. L'arrivée de services numériques reposant sur des modalités d'interaction « naturelles » (voix, geste) attire l'attention sur leur conception tout comme sur l'influence que les designers peuvent avoir sur les choix des personnes.



Les autorités de protection des données s'intéressent depuis longtemps à l'encadrement juridico-technique de l'utilisation des informations relatives à des personnes. À l'heure où les plateformes numériques investissent massivement dans les nouvelles interfaces hommes machines et l'interprétation des émotions[1], il devient tout aussi important de comprendre comment ces interfaces sont conçues et avec quelles intentions s'agissant de la manière dont elles influencent les utilisateurs.

En d'autres termes, il s'agit de s'intéresser au rôle du design des technologies numériques dans la captation de l'attention et en conséquence à la place du designer dans la production de ces mécanismes.

La CNIL a entamé depuis plusieurs mois des travaux en lien avec des communautés actives sur les enjeux éthiques du design.

Le rôle du design des technologies numériques dans la captation de l'attention

Le design est un formidable outil pour façonner l'expérience utilisateur, pour qu'elle soit « sans friction » et faire disparaitre la complexité en exploitant les biais cognitifs des utilisateurs.

En effet, la manière dont l'ergonomie d'un service est conçue, par exemple l'emplacement de la molette permettant de régler les paramètres de confidentialité, ou encore la hiérarchisation et le nombre de cases à cocher, ont naturellement une influence sur le comportement des utilisateurs.

Les travaux de l'économiste Alessandro Acquisti[2] et ceux de Ryan Calo[3] ont déjà mis en évidence la manière dont les marchés numériques orientent les choix des personnes en offrant en apparence davantage de possibilités, qui vont en réalité contribuer à abaisser leur vigilance, et leur conférer une forme d'illusion de contrôle.

1 Camille Alloing, Julien Pierre, « *Le web affectif, une économie numérique des émotions* », INA, Collection Études et Controverses, 2017.
2 Alessandro Acquisti, Laura Brandimarte, George Loewenstein, *Privacy and Human Behavior In the Age of Information*, Science, Vol. 347 no. 6221 pp. 509-514, 2015.

« L'objet de cette exploration est de comprendre comment il est possible d'innover par le design. »

Ces enjeux sont de plus en plus essentiels à mesure que l'attention des utilisateurs devient une ressource rare à capter et pour laquelle les plateformes rivalisent d'ingéniosité. Les vidéos qui démarrent toutes seules sur les réseaux sociaux, les *timelines* que l'on peut scroller indéfiniment, ou les notifications intempestives sont autant de techniques qui détournent l'utilisateur de son objectif initial, et sont la démonstration que le design a vocation à garder l'utilisateur connecté le plus longtemps possible au service, car c'est ce qui est valorisé économiquement[4].

Plus récemment, une enquête du New York Times[5] mettait en évidence les stratégies de certaines entreprises de VTC pour augmenter la durée de disponibilité des travailleurs indépendants au sein des plateformes à travers des mécanismes incitatifs *(nudges)* insistant sur leurs opportunités de gains.

Éthique et le rôle du designer

Le designer est celui qui façonne la dernière étape entre une technologie et son utilisateur. On voit naitre de plus en plus de questionnements sur son rôle et les conséquences éthiques de ses choix. Le design doit-il seulement être au service du masquage de la complexité ? Peut-on injecter de l'éthique dans le design des services numériques ?

Plus les utilisateurs dépendent des interfaces pour communiquer, plus il est nécessaire qu'ils soient en mesure de comprendre ces outils et les choix qui leur sont proposés, de manière à conserver la liberté du consentement.

Pour la CNIL, l'objet de cette exploration est de comprendre comment il est possible d'innover par le design. Il s'agira de s'interroger sur le rôle du design pour aider les utilisateurs à garder le contrôle et sur le rôle du designer pour accompagner l'utilisateur dans cette démarche.

Pour ces raisons, les intersections des différents champs disciplinaires design, sciences cognitives et comportementales sont des espaces que la CNIL va investiguer dans le cadre de ses activités d'innovation et de prospective pour mieux comprendre comment se forment les décisions au plus proche des individus.

INFOSPLUS

Quelle grammaire inventer pour les nouvelles interfaces vocales ?

Si les interactions numériques restent relativement codifiées lorsque nous sommes face à un écran, la question de la capacité de contrôle des individus se pose différemment dès lors que les interfaces disparaissent. S'agissant par exemple des assistants vocaux, de nouveaux enjeux se posent en particulier en termes de design :

- Dans un contexte où l'assistant ne renvoie qu'une seule réponse, et non une liste de résultats comme sur un moteur de recherche, comment est sélectionné le résultat qui est considéré le plus pertinent ? Doit-il être personnalisé selon le profil de l'utilisateur.
- Les requêtes en langage naturel exposent-elles davantage les utilisateurs à travers une baisse de leur vigilance ou parce qu'il serait possible d'inférer des informations par l'exploitation de leur tonalité vocale ?
- Où doit-on cliquer pour « en savoir plus » lorsqu'il n'y a plus d'écran ?

3 Ryan Calo, *Digital Market Manipulation*, The George Washington law review, vol. 82:995, 2014.
4 LINC, Comment les technologies nous influencent – et pourquoi les neurosciences sont utiles ?, linc.cnil.fr septembre 2017, https://linc.cnil.fr/fr/comment-les-technologies-nous-influencent-et-pourquoi-les-neurosciences-sont-utiles
5 LINC, Nudger n'est pas jouer : comment Uber et Lyft influencent leurs chauffeurs à leur avantage, linc.cnil.fr, avril 2017, https://linc.cnil.fr/fr/nudger-nest-pas-jouer-comment-uber-et-lyft-influencent-leurs-chauffeurs-leur-avantage

Un prochain ouvrage dans la collection « Point CNIL » consacré à la protection de données des enfants

Le premier volume de la collection thématique « POINT CNIL », consacré aux données génétiques, est paru en septembre 2017 à la Documentation française. Plusieurs des sujets qui y sont abordés relèvent des thèmes débattus dans le cadre des États généraux de la bioéthique, dont l'organisation a été confiée au Comité national d'éthique pour les sciences de la vie et de la santé (CCNE) pour préparer les travaux de révision des lois de bioéthique.

C'est pourquoi la CNIL a choisi de participer, en 2018, à ces débats ainsi qu'à plusieurs manifestations consacrées à la génétique humaine et médicale.

Le deuxième titre de la collection, qui sortira fin 2018, sera consacré à la protection des données des enfants. Le sujet s'imposait dès lors que, selon l'UNICEF, un internaute sur trois a moins de 18 ans et qu'il y a consensus sur la nécessité de protéger, de façon spécifique, les données concernant ces jeunes.

En Europe, le règlement général sur la protection des données instaure, pour la première fois, un régime de protection particulier pour les données des moins de 18 ans.

L'ouvrage a pour ambition de faire le point sur les règles de protection des données applicables aux mineurs, que ce soit en milieu scolaire, dans le monde de la santé, dans les fichiers de police, en matière de prospection commerciale ou tout simplement sur Internet. Quelles sont les garanties mises en place pour préserver leur devenir et éviter tout risque de profilage prédictif ? Quels sont les droits des enfants sur leurs données ? Dans ce monde numérique de l'enfance comprenant l'école digitale ou les jouets connectés, il s'agit aussi de dresser un état des lieux des nouveaux enjeux et d'exposer le point de vue de la CNIL, tout en faisant le tour des débats en cours.

Les Ressources

LES RESSOURCES HUMAINES

Une nouvelle fois, en 2017, la CNIL s'inscrit dans un tendanciel d'augmentation soutenue de ses missions traditionnelles et d'accroissement de son périmètre d'intervention, avec une évolution prévisible d'un approfondissement de ses missions avec l'entrée en application du Règlement européen sur la protection des données personnelles (RGPD).

Elle a dû également assurer **des missions nouvelles** confiées par le législateur français (la loi du 13 novembre 2014 charge la CNIL de contrôler le bien-fondé des décisions de « blocage administratif » de sites internet en lien avec le terrorisme et la pédopornographie prises par le ministère de l'intérieur. Ses compétences ont aussi été étendues par la loi pour une République numérique de 2016 qui prévoit l'extension des cas de consultation de la CNIL, l'animation d'une réflexion sur les enjeux éthiques du numérique et la certification des processus d'anonymisation. D'autres missions découlent de la réglementation européenne applicable à partir de mai 2018, comme la gestion des notifications de violations de données, étendues par le RGPD à l'ensemble des opérateurs.

En 2017, le plafond d'emploi de la CNIL est passé de 195 emplois en 2016 à **198 emplois, soit une progression de 1,54 %.** Les nouveaux emplois ont permis de consolider les équipes dédiées à l'accompagnement des responsables de traitement et des usagers afin d'améliorer constamment la qualité du service rendu, mais aussi de renforcer les équipes en raison des nouvelles missions confiées par le législateur (expertise technique).
Compte tenu du bouleversement numérique lié à l'explosion du recours aux données personnelles et à la mise en œuvre du règlement européen sur la protection des données personnelles, la CNIL a poursuivi, en 2017, l'adaptation de son organisation et l'accompagnement interne des agents en matière de développement des compétences au travers d'un plan de formation renforcé et orienté vers les évolutions introduites par le RGPD.

L'année 2017 a également été marquée par l'adhésion de la CNIL à des mutualisations de certaines fonctions supports qui s'est traduite par le transfert de 5 agents à la Direction des services administratifs et financiers des services du Premier ministre.

DONNÉES SOCIALES

198 emplois fin 2017

63% de femmes

37% d'hommes

40 ans Âge moyen

8 ans l'ancienneté moyenne à la CNIL

76% des agents occupent un poste de catégorie A

36% des postes occupés par des juristes

26% des postes occupés par des assistants

14% des postes occupés par des ingénieurs / auditeurs

51% des agents travaillant à la CNIL sont arrivés entre 2012 et 2017

LES RESSOURCES FINANCIÈRES

En 2017, le budget alloué à la CNIL s'élève à **17 161 536 €** en autorisation d'engagement et à 17 008 456 € en crédits de paiement, répartis comme suit : 14 088 832 € pour le budget de personnel (titre 2) et 3 072 704 € en autorisation d'engagement et 2 919 624 € en crédits de paiement pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6).

La diminution du budget de fonctionnement en crédits de paiement de 61,1 % correspond à la mutualisation de certaines activités support et à un transfert de crédits devenu effectif le 1er janvier 2017. Il est à préciser que les mesures d'économies en matière de coûts de fonctionnement se poursuivent en 2018.

Dans l'enveloppe allouée à la CNIL, l'effort budgétaire demandé aux institutions publiques, particulièrement contraignant en 2017 pour la CNIL, avec un gel et un sur-gel des crédits en cours de gestion, l'a contrainte à revoir à la baisse la finalisation de certains projets déjà engagés, à l'image de la refonte du Schéma Directeur des Systèmes d'Information (SDSI) revue à la baisse alors même que le règlement européen de la protection de la donnée entre en vigueur le 25 mai 2018.

Ainsi au cours de cet exercice, la CNIL a poursuivi 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, lorsque ceux-ci répondaient aux besoins de l'institution.

CRÉDITS 2017	Autorisations d'engagement	Crédits de paiement
Budget LFI	**17 529 246**	**17 362 855**
Titre 2	14 159 630	14 159 630
Hors Titre 2	3 369 616	3 203 225
Budget disponible	**17 161 536**	**17 008 456**
Titre 2	14 088 832	14 088 832
Hors Titre 2	3 072 704	2 919 624
Budget consommé	**16 474 777**	**16 059 122**
Titre 2	13 517 617	13 517 617
Hors Titre 2	2 957 160	2 541 505

Organigramme des Directions et Services

Isabelle FALQUE-PIERROTIN
Présidente

Jean LESSI
Secrétaire général

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

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, Frédérique Plas, Philarty Photography
Illustration de couverture : Geoffrey Dorne

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

Diffusion
Direction de l'information légale et administrative

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

ISBN : 978-2-11-145682-2
DF : 5HC47240
Prix : 15 €

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles