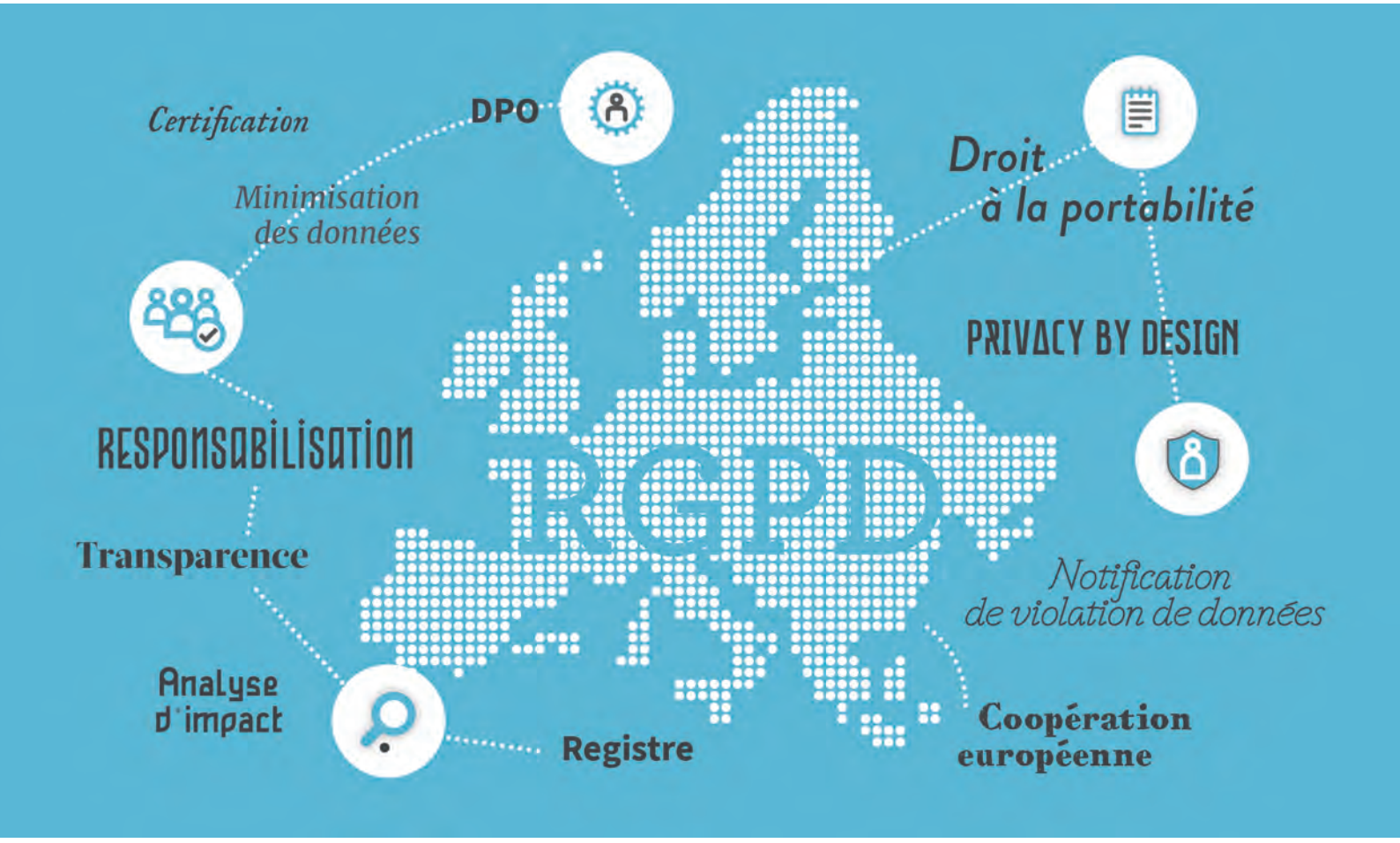
2018

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

2018

Rapport d'activité

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

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

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

LES CHIFFRES CLÉS 2018

CONSEILLER & RÉGLEMENTER

322 AUTORISATIONS DE TRANSFERTS DE DONNÉES HORS UE

360 AUTORISATIONS RECHERCHE MÉDICALE OU ÉVALUATION DES PRATIQUES DE SOINS

342 DÉLIBÉRATIONS DONT :

- **120** AVIS SUR DES PROJETS DE TEXTE
- **110** AUTORISATIONS

ACCOMPAGNER LA CONFORMITÉ

39 500 ORGANISMES ONT DÉSIGNÉ UN DÉLÉGUÉ

16 000 DÉLÉGUÉS

1 170 NOTIFICATIONS DE VIOLATIONS DE DONNÉES

PROTÉGER

11 077 PLAINTES

+ 32,5 %

4 264 DEMANDES DE DROIT D'ACCÈS INDIRECT

6 609 VÉRIFICATIONS EFFECTUÉES

INFORMER

189 877 APPELS

16 877 REQUÊTES SUR LA PLATEFORME « BESOIN D'AIDE » +15 %

8 MILLIONS DE VISITES SUR CNIL.FR +80 %

108 000 FOLLOWERS SUR TWITTER

31 000 FANS SUR FACEBOOK

64 000 NOMBRE D'ABONNÉS SUR LINKEDIN

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

CONTRÔLER & SANCTIONNER

310 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT :

204 CONTRÔLES SUR PLACE :

20 CONCERNANT LA VIDÉOPROTECTION

51 CONTRÔLES EN LIGNE

51 CONTRÔLES SUR PIÈCES

4 AUDITIONS

48 MISES EN DEMEURE DONT :

13 MISES EN DEMEURE PUBLIQUES

11 SANCTIONS DONT :

9 SANCTIONS PÉCUNIAIRES PUBLIQUES

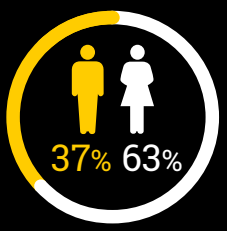
1 AVERTISSEMENT NON PUBLIC

1 NON-LIEU

RESSOURCES HUMAINES

BUDGET : **17,6 MILLIONS D'€**

199 emplois



40 ans Âge moyen

44% DES POSTES OCCUPÉS PAR DES JURISTES

25% PAR DES ASSISTANTS

18% PAR DES INGÉNIEURS / AUDITEURS DES SYSTÈMES D'INFORMATION

77% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A

53% DES AGENTS TRAVAILLANT À LA CNIL SONT ARRIVÉS ENTRE 2013 ET 2018

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 2018

Janvier

06/01 > 40 ans et toujours dans l'air du temps

09/01 > Darty : sanction pécuniaire pour une atteinte à la sécurité des données clients

10/01 > Innovation dans le secteur social-logement : un pack de conformité pour les produits et services de la silver économie

22/01 > Admission post-bac (APB) : clôture de la mise en demeure

23,24/01 > La CNIL au 10e forum international de la cybersécurité (FIC)

31/01 > La CNIL et INRIA décernent le prix protection de la vie privée 2017 à une équipe de recherche européenne

Février

27/02 > SNIIRAM : la CNAMTS mise en demeure pour des manquements à la sécurité des données

Mars

21/03 > Cambridge Analytica : les autorités de protection européennes se saisissent du sujet

27/03 > Direct Energie : mise en demeure pour une absence de consentement concernant les données issues du compteur communicant Linky

Avril

10/04 > Publication du guide de sensibilisation sur le RGPD pour les TPE/PME avec Bpifrance

Mai

25/05 > Entrée en application du RGPD

Juin

07/06 > Optical Center : sanction de 250.000 € pour une atteinte à la sécurité des données des clients du site internet www.optical-center.fr

28/06 > Sanction de 75 000 euros pour une atteinte à la sécurité des données de demandeurs de logements

Juillet

19/07 > Applications mobiles : mises en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire

20/07 > Jouets connectés : clôture de la procédure de mise en demeure à l'encontre de la société Genesis Industries Limited

24/07 > Vidéosurveillance excessive : mise en demeure de l'institut des techniques informatiques et commerciales (ITIC)

31/07 > OPH de Rennes : sanction pécuniaire pour une utilisation du fichier des locataires incompatible avec la finalité initiale

Août

02/08 > Dailymotion : sanction de 50.000€ pour une atteinte à la sécurité des données des utilisateurs

07/08 > Entrée en vigueur de la nouvelle loi Informatique et Libertés et de son décret d'application

09/08 > Étude réalisée à partir de messages postés sur twitter par EU DisinfoLab : la CNIL est saisie du dossier

Septembre

03/09 > Biométrie sur le lieu de travail : la CNIL lance une consultation publique sur le futur règlement type

19/09 > La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo

20/09 > Biométrie au travail illégale : sanction de 10.000 €

26/09 > Montres connectées pour enfants : quels enjeux pour leur vie privée ?

27/09 > Alliance française Paris Île-de-France : sanction de 30.000 € pour une atteinte à la sécurité des données des utilisateurs

Octobre

04/10 > Applications mobiles : clôture de la mise en demeure à l'encontre de la société Teemo

17/10 > Dispositifs de mesure d'audience et de fréquentation dans des espaces accessibles au public : la CNIL rappelle les règles

18/10 > Mise en demeure de cinq sociétés d'assurance pour détournement de finalité des données des assurés

25/10 > Direct Energie : clôture de la mise en demeure

30/10 > Vidéosurveillance excessive : mise en demeure de l'école 42

Novembre

07/11 > Pratiques abusives « mise en conformité RGPD » : comment s'en prémunir avec la CNIL et la DGCCRF ?

6/11 > Publication d'une liste des traitements pour lesquels une analyse d'impact est requise

16/11 > Données génétiques : les réserves de la CNIL sur l'amendement portant sur l'élargissement du FNAEG

25/11 > Premier bilan 6 mois après l'entrée en application du RGPD

29/11 > Gestion commerciale et gestion des impayés : la CNIL lance une consultation publique sur les futurs référentiels

29/11 > Applications mobiles : clôture des mises en demeure

Décembre

03/12 > Jouets connectés : quels conseils pour les sécuriser ?

05/12 > Signature d'une convention triennale sur la protection des données personnelles dans les usages numériques de l'éducation

19/12 > Publication de l'ordonnance de réécriture de la loi Informatique et Libertés

20/12 > Enceintes intelligentes : des assistants vocaux connectés à votre vie privée

20/12 > Uber : sanction de 400.000 € pour une atteinte à la sécurité des données des utilisateurs

26/12 > Parcoursup et les établissements d'enseignement supérieur : questions-réponses

27/12 > Bouygues Telecom : sanction pécuniaire pour manquement à la sécurité des données clients

28/12 > Transmission des données à des partenaires à des fins de prospection électronique : quels sont les principes à respecter ?

LES MEMBRES DE LA CNIL

© PhilArty Photography

LE BUREAU

01

PRÉSIDENTE

Marie-Laure DENIS,

Conseiller d'État.
Marie-Laure DENIS a été nommée Présidente de la CNIL par décret du Président de la République pour un mandat de cinq ans à compter du 2 février 2019.

02

VICE-PRÉSIDENTE DÉLÉGUÉE

Sophie LAMBREMON

Conseiller honoraire à la Cour de cassation.
Secteur : Intérieur.
Sophie LAMBREMON est membre et Vice-présidente déléguée de la CNIL depuis février 2019.

03

VICE-PRÉSIDENT

Éric PERES

Membre du Conseil économique, social et environnemental.
Secteur : Environnement, transports et énergie.
Éric PERES est membre de la CNIL depuis décembre 2010, puis Vice-président depuis février 2014.

LES MEMBRES ÉLUS DE LA FORMATION RESTREINTE

- Alexandre LINDEN (Président)
- Philippe-Pierre CABOURDIN (Vice-président)
- Anne DEBET
- Philippe GOSSELIN
- Sylvie LEMMET
- Christine MAUGÜE

COMMISSAIRE DU GOUVERNEMENT

- Nacima BELKACEM
- Adjointe, Eve JULIEN

04

Sylvie LEMMET

Conseillère maître à la Cour des comptes.
Secteur : Défense / Administration numérique.
Sylvie LEMMET est membre de la CNIL depuis février 2019.

05

Christine MAUGÜE

Conseiller d'État.
Secteur : Justice.
Christine MAUGÜE est membre de la CNIL depuis février 2019.

06

Christian KERT

Secteur : Sport, médias et culture.
Christian KERT est membre de la CNIL depuis février 2019.

07

Valérie PEUGEOT

Chercheuse au sein d'Orange Labs et Présidente de l'association Vecam.
Secteur : Santé et assurance maladie.
Valérie PEUGEOT est membre de la CNIL depuis avril 2016.

08

Alexandre LINDEN

Président de la formation restreinte.
Conseiller honoraire à la Cour de cassation.
Secteur : Travail et ressources humaines (formation professionnelle, recrutement, cybersurveillance, etc.).
Alexandre LINDEN est membre de la CNIL depuis février 2014.

09

Loïc HERVÉ

Sénateur de la Haute-Savoie.
Secteur : Travail et ressources humaines (formation professionnelle, recrutement, cybersurveillance, etc.).
Loic HERVÉ est membre de la CNIL depuis septembre 2014.

10

Dominique CASTERA

Membre du Conseil économique, social et environnemental.
Secteur : Vie politique et citoyenne.
Dominique CASTERA est membre de la CNIL depuis octobre 2010.

11

François PELLEGRINI

Professeur des universités à l'université de Bordeaux.
Secteur : Commerce et publicité / Cybersécurité / Europe et international.
François PELLEGRINI est membre de la CNIL depuis février 2014.

12

Bertrand du MARAIS

Conseiller d'État.
Secteur : Communications électroniques et Technologies innovantes / Plateformes en ligne / Europe et international.
Bertrand DU MARAIS est membre de la CNIL depuis février 2019.

LES MEMBRES (COMMISSAIRES)

13

Philippe-Pierre CABOURDIN

Conseiller maître à la Cour des comptes, Vice-président de la formation restreinte de la CNIL.
Secteur : Banque, assurance et fiscalité.
Philippe-Pierre CABOURDIN est membre de la CNIL depuis février 2019.

14

Anne DEBET

Professeur des universités
Secteur : Données publiques et recherche / Délégués à la protection des données et nouveaux outils de conformité.
Anne DEBET est membre de la CNIL depuis février 2019.

15

Jean LESSI

Secrétaire général.

Albane GAILLOT

Députée du Val-de-Marne et membre de la commission des Affaires sociales de l'Assemblée nationale.
Secteur : Collectivités territoriales.

Philippe GOSSELIN

Député de la Manche
Secteur : Social, logement et immobilier.
Philippe GOSSELIN est membre de la CNIL depuis février 2015.

Sylvie ROBERT

Sénatrice d'Ille-et-Vilaine.
Secteur : Éducation et enseignement supérieur.
Sylvie ROBERT est membre de la CNIL depuis décembre 2016.

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.

16

Marie-Françoise GUILHEMSANS

Membre de la CADA, suppléante de Monsieur Marc DANDELOT.

AVANT-PROPOS DE LA PRÉSIDENTE

Marie-Laure DENIS
Présidente de la CNIL

LE RGPD : UN IMPACT SANS PRÉCÉDENT POUR LA CNIL QUI DOIT DEVENIR UN SUCCÈS OPÉRATIONNEL EN 2019

Une année exceptionnelle pour la CNIL marquée par la préparation et l'entrée en application du RGPD, le Règlement général sur la protection des données.

2018, UNE ANNÉE PONCTUÉE PAR PLUSIEURS DATES EMBLÉMATIQUES POUR LA CNIL

L'année a commencé avec la célébration des 40 ans de la CNIL, le **6 Janvier**. Cet anniversaire a été l'occasion de revenir sur son histoire riche et singulière de différentes façons : témoignages et regards croisés de personnalités d'horizons divers sur le rôle de la CNIL, vidéo sur 40 ans de protection des données en France, sélection d'archives vidéos proposée par l'INA retraçant l'action de la CNIL et les grands sujets qui ont marqué son histoire.

Quatre mois plus tard, une autre date clé allait faire couler beaucoup d'encre : le « fameux » **25 Mai**, évènement majeur dans le monde de la protection des données personnelles, préparé depuis plusieurs années par la CNIL et ses homologues, signe d'une volonté de souveraineté européenne forte.

De nombreuses interrogations se sont alors exprimées : la CNIL allait-elle dès le 26 mai au matin contrôler la conformité de tous les organismes ? Les premières sanctions pouvant atteindre 4 % du chiffre d'affaires mondial d'une entreprise allaient-elles intervenir ?

Le nouveau cadre juridique a été très médiatisé. Résultat, 6 mois après son entrée en application, 65 % des Français avaient entendu parler du RGPD, selon un sondage IFOP réalisé pour la CNIL.

La préparation de cette échéance, engagée deux ans auparavant, a nécessité des efforts considérables pour les équipes de la CNIL. Ceux-ci se poursuivent aujourd'hui pour la mise en œuvre du RGPD.

Il y a un avant et un après 25 mai, en Europe bien sûr mais aussi dans le monde puisque ce nouveau modèle européen inspire d'autres pays.

Enfin, les dates du **20 juin et du 12 décembre** ont quasiment parachevé le nouveau cadre juridique. La loi du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés afin de mettre en conformité le droit national avec le cadre juridique européen. Elle a permis la mise en œuvre concrète du RGPD et de la Directive « police-justice », applicable aux fichiers de la sphère pénale.

L'ordonnance du 12 décembre 2018, publiée le 13 décembre 2018, a quant à elle achevé, au niveau législatif, cette mise en conformité du droit national et amélioré la lisibilité du cadre juridique. La CNIL a rendu trois avis relatifs au projet de loi, au décret d'application de la loi et à l'ordonnance et nombre de ses observations ont été retenues.

40 ans après la loi du janvier 1978, cette dernière est réécrite et la protection des données s'est adaptée aux nouvelles réalités du numérique.

LES ACTIONS DE LA CNIL EN 2018 SE SONT CONCENTRÉES SUR LA MISE EN ŒUVRE DU RGPD

Le travail fourni par les équipes s'est étendu au niveau national mais aussi au niveau européen et international. Si le mandat de la présidence du G29 (Groupe des CNIL européennes jusqu'au 25 mai 2018) a pris fin en février 2018, la CNIL a été très investie pendant les quatre années de cette présidence avec une feuille de route ambitieuse fixant un cap pour que les autorités de protection soient en ordre de marche le 25 mai.

La CNIL, qui présidait la conférence internationale a aussi beaucoup œuvré en 2018 pour dessiner le futur de cette conférence, en posant les bases d'une organisation internationale permanente de la protection des données et en proposant une position commune sur l'intelligence artificielle.

Concernant l'entrée en application du RGPD, la CNIL a été sur tous les fronts mais de façon séquencée et articulée avec le calendrier européen fixé par le G29.

Elle a d'abord contribué activement à l'élaboration des lignes directrices du G29, dont elle a été rapporteur pour plusieurs d'entre elles.

Elle a intégré la coopération européenne dans le travail quotidien de la CNIL, notamment dans le cadre de l'instruction de plaintes transfrontalières.

« La préparation du RGPD, engagée deux ans auparavant, a nécessité des efforts considérables pour les équipes de la CNIL.»

« La politique répressive doit s'opérer en conciliant le respect des règles issues du RGPD et la préservation des équilibres économiques. »

Elle s'est préparée à recevoir des flux importants relatifs aux notifications de violation de données ou aux désignations de délégués à la protection des données.

Elle s'est emparée, dès le mois de mai, des nouveaux outils de régulation prévus par le RGPD : référentiels, certification, règlements type, la liste des analyses d'impact obligatoires.

Enfin, elle a expliqué sans relâche ce nouveau cadre et ses principes, proposé des plans d'action de mise en conformité adaptés aux différents niveaux de maturité des professionnels et vulgarisé les bonnes pratiques notamment à destination des TPE/PME.

2018, UNE ANNÉE DE TOUS LES RECORDS EN CHIFFRES QUI TÉMOIGNENT D'UN SPECTACULAIRE « EFFET RGPD », DÉJÀ RESSENTI DÈS 2017.

Le bilan d'activité présenté en partie II de ce rapport annuel atteste de cet impact sur tous les indicateurs quantitatifs de la CNIL qui ont atteint des niveaux inédits.

La CNIL a ainsi reçu plus de 11 000 plaintes et cette tendance à la hausse (+32 %) est confirmée sur les premiers mois de l'année 2019. Cette augmentation s'explique par une médiatisation importante du RGPD et une plus grande sensibilité aux questions de protection des données. En effet, selon un sondage IFOP réalisé en octobre pour la CNIL, **66 % des Français se disent plus sensibles que ces dernières années à la protection de leurs données personnelles.** La CNIL doit faire face à ces flux toujours plus nombreux de plaintes. 20 % d'entre elles environ font désormais l'objet d'une coopération européenne.

Du côté des professionnels, la CNIL a reçu plus de 1 000 notifications de violations de données et la désignation de 16 000 délégués (DPO) représentant 39 500 organismes. Le nombre des visites du site de la CNIL, d'appels téléphoniques ou de consultations des questions/réponses disponibles en ligne (+ 59 %) enregistre une hausse très importante qui s'explique par le besoin d'information sur le RGPD et par l'identification de la CNIL comme la source de référence en la matière.

Le collège de la CNIL a rendu 120 avis sur des projets de texte d'origine gouvernemetale concernant la protection des données personnelles ou créant de nouveaux fichiers et 110 autorisations. Au cours de l'année, la CNIL a participé à une trentaine d'auditions, sous toutes ses formes

QUELLES PERSPECTIVES 2019 ? PÉDAGOGIE ET DISSUASION

Le RGPD constitue indéniablement un nouvel environnement de travail pour la CNIL. Il lui impose d'accentuer son agilité et sa capacité à travailler avec d'autres pour proposer une doctrine européenne cohérente et lisible.

L'année 2019 sera décisive pour crédibiliser ce nouveau cadre juridique. La pression sur les autorités de protection des données n'a jamais été si forte. Elle émane autant de la société civile que des acteurs économiques. Il faut désormais s'atteler à transformer cet ambitieux pari européen en succès opérationnel.

Depuis le mois de février, un nouveau collège de la CNIL est en place. La grande diversité de ses 18 membres est un atout précieux. Je suis fière de présider une institution qui a su avec des équipes aussi professionnelles qu'engagées se mettre en ordre de marche.

En 2019, l'action de la CNIL s'articulera autour de trois priorités :
- **réussir la mise en œuvre effective du RGPD pour les particuliers et les professionnels ;**
- **développer la capacité d'expertise technique et prospective de la CNIL ;**
- **conserver un rôle moteur au niveau européen et international.**

La CNIL va poursuivre ses actions de pédagogie sur les principes et les droits issus du RGPD à destination des particuliers et ses initiatives en faveur de l'éducation au numérique.

La réussite de la mise en œuvre du RGPD par les professionnels passe par une **amplification des actions d'accompagnement** qui leur sont dédiées.

Pour les organismes les moins « matures » ou les plus petits, cela se traduit par plus de **pédagogie** de la part de la CNIL pour

promouvoir l'esprit du RGPD et en favoriser son appropriation. Ce sera notamment le cas avec la publication, avant l'été, d'un guide de sensibilisation au RGPD pour les collectivités locales, sur le même modèle que celui élaboré pour les TPE/PME l'année dernière.

La CNIL doit aussi proposer des **outils de conformité** qui servent de cadres de référence aux professionnels en poursuivant et développant ce qu'elle a initié depuis mai en matière de lignes directrices, référentiels, règlements type, listes d'analyse d'impact, etc.

Parce que le RGPD a ouvert la voie à un **nouvel écosystème de la régulation** que la CNIL avait d'ailleurs anticipé avec une approche sectorielle au travers de packs de conformité, elle doit développer cette ouverture en s'appuyant sur des relais. Une stratégie de sensibilisation des « têtes de réseau » permettra de favoriser la montée en compétence de tous les secteurs et de démultiplier l'action de la CNIL. Les délégués à la protection des données et les organismes certificateurs agréés par la CNIL sont aussi des acteurs clés de cette co-régulation. L'inter-régulation mérite aussi d'être renforcée, la question des données personnelles dépassant le strict cadre de leur protection.

Cette amplification des actions d'accompagnement s'opérera en parallèle d'un contrôle exigeant et, dans les cas qui le nécessitent, des sanctions seront prononcées car la crédibilité du RGPD repose aussi sur une **politique de contrôles et de sanctions efficace**. C'est la contrepartie naturelle de la responsabilisation accrue des acteurs et de leur capacité à apporter la preuve de leur conformité par une approche dynamique et continue. Si la CNIL ne doit pas hésiter à utiliser son pouvoir renforcé de sanction, elle doit en user avec discernement et veiller à la sécurité juridique de ses décisions. Cette politique répressive doit s'opérer en conciliant le respect des règles issues du RGPD et la préservation des équilibres économiques, en recherchant un point d'équilibre entre la mission du régulateur et les intérêts des acteurs. Au travers de ses décisions, l'objectif de la CNIL est de faire évoluer le modèle d'affaires ou le comportement de certains acteurs vers des pratiques plus responsables et vertueuses, desquelles pourront découler, à moyen terme, des avantages économiques ou concurrentiels. Sanctionner, c'est dissuader dans une optique de pédagogie préventive.

Enfin, les autorités de protection doivent s'attacher à **faire fonctionner la coopération européenne**. Le mécanisme de « guichet unique » qui consiste à prendre des décisions communes pour des traitements transfrontaliers suppose une coopération fluide et quotidienne que la CNIL a engagée dès le 25 mai. C'est une innovation majeure.

La CNIL doit aussi **renforcer sa capacité d'expertise technique et prospective** déjà reconnue au niveau national et international. Dans un contexte d'innovation permanente, cette capacité lui permet à la fois d'anticiper les nouveaux usages ou technologies qui impactent la protection des données et de poser les bases d'une régulation au plus proche des besoins des acteurs et donc plus « acceptable ». Cette expertise technique lui permet de dialoguer avec les grands acteurs de l'internet ou les startups mais aussi de rendre plus visibles aux yeux du grand public des écosystèmes complexes qui s'apparentent parfois à des boîtes noires.

La CNIL devra aussi poursuivre ses réflexions sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques. Comme elle l'a fait, dès 2017, sur le thème de l'intelligence artificielle et des algorithmes.

Dernière priorité, la CNIL doit conserver un rôle moteur au niveau européen en défendant les positions françaises au sein du Comité européen de protection des données (CEPD) et en participant activement à l'ensemble des groupes de travail. Elle entend porter au niveau européen les cadres de référence et les outils de conformité notamment sectoriels qu'elle développe et les partager avec ses homologues. La CNIL restera mobilisée sur les dossiers internationaux à forts enjeux tels que les nouveaux outils de transferts internationaux, les instruments de coopération avec nos homologues non-européens et le suivi des normes européennes et internationales en matière d'accès transfrontières aux preuves électroniques.

Voici donc résumées les actions prioritaires de la CNIL en 2019. Elles seront précisées dans un plan stratégique triennal 2019-2021 qui sera finalisé avant l'été, après échanges avec les membres et les agents de la CNIL.

Enfin, un maître mot doit guider l'action de la CNIL en 2019 : **la confiance**. Les citoyens aspirent à voir leurs données personnelles collectées et exploitées de façon transparente et pour des usages qu'ils acceptent. Les entreprises doivent s'efforcer de vivre la « contrainte régulatoire » comme une exigence pouvant leur procurer un avantage concurrentiel distinctif. Enfin, les pouvoirs publics, dans le champ d'action transversal qui est le leur, doivent avoir le souci permanent de la protection des données dans la mise en œuvre des politiques publiques. La CNIL sera, pour toutes ces parties prenantes, un interlocuteur ouvert, fiable et exigeant.

« Un maître mot doit guider l'action de la CNIL en 2019 : la confiance.»

MOT DU SECRÉTAIRE GÉNÉRAL

DES ÉQUIPES SUR TOUS LES FRONTS POUR FAIRE FACE À UNE ANNÉE HORS NORME

Jean LESSI
Secrétaire général

Les agents de la CNIL ont été, une nouvelle fois, sur tous les fronts en cette année 2018 hors norme. La Commission s'était préparée de longue date à ce basculement du 25 mai 2018, le plus important depuis l'année fondatrice 1978, vers le nouveau cadre juridique issu du Règlement général sur la protection des données ainsi que de la directive dite « police-justice ». Cependant, une chose est de se préparer, une autre est de pratiquer au quotidien ce texte et, plus encore, de devoir répondre à des attentes désormais tout sauf théoriques ou hypothétiques des particuliers et des professionnels. Les sollicitations sont d'autant plus importantes qu'à l'effet de nouveauté du RGPD, s'est ajouté un indéniable effet « coup de projecteur » sur des obligations et droit préexistants. Dans ce contexte, le travail des équipes en 2018 s'est concentré sur quatre axes : application, pédagogie, innovation, démultiplication.

APPLICATION

C'est évidemment le fait marquant de 2018 : passer de l'anticipation du nouveau cadre à son application, dans tous les métiers. Le défi était d'autant plus grand que cette transition s'est déroulée dans un contexte d'augmentation continue des volumes, retracé par le rapport, concernant notamment les plaintes ou les demandes d'information et de conseil adressées par les professionnels et particuliers à la CNIL. Cette double contrainte a supposé une mobilisation considérable des équipes, ainsi qu'une adaptation des techniques de traitement qui avait été amorcée avant 2018 et se poursuivra dans les prochaines années. Elle pose aussi, naturellement, la question des effectifs devant pouvoir être mobilisés sur des missions de plus en plus exposées à l'heure d'une numérisation croissante de notre société.

Par ailleurs, la CNIL a rapidement investi en 2018 les nouvelles compétences qui sont les siennes, en faisant usage de ses nouvelles prérogatives (élaboration du premier règlement type sur la biométrie en milieu professionnel, publié en mars 2019, adoption des premières sanctions dans le nouveau cadre répressif, publication du premier référentiel de certification, *etc.*) et en entrant de plain-pied dans les mécanismes de coopération avec ses homologues européens.

« Le travail de l'année 2018 a été marqué par un souci d'innover dans les outils ou les pratiques. »

PÉDAGOGIE

L'année 2018 a vu la quasi-finalisation du cadre juridique avec l'adoption de la loi du 20 juin, du décret du 1er août et de l'ordonnance du 12 décembre. Mais écrire un texte n'est pas tout. Il faut désormais en donner toutes les clés de lecture. Ce travail a débuté depuis plusieurs années sous la forme des lignes directrices du G 29. Mais plusieurs notions clés restent à clarifier, au niveau de la CNIL ou du collectif européen, et le seront d'autant plus utilement à la lumière des premiers mois de pratique : articulation des différentes bases légales, clarification des frontières entre responsable, responsables conjoints, sous-traitants, simples fournisseurs de solution, *etc.*

Pour être complet et surtout utile, ce travail juridique d'interprétation doit aussi s'accompagner d'outils pratiques d'aide à l'application, très nombreux sur le site (FAQ, infographies pédagogiques, registre simplifié à l'attention notamment des PME-TPE, *etc.*), et d'une capacité, à laquelle la CNIL est attachée, à résoudre les problèmes concrets qui nous sont soumis par les professionnels et particuliers dans le cadre des permanences juridiques, les plaintes, etc. La CNIL cherche en outre à fournir aux professionnels des formats nouveaux, tenant compte de la fin des formalités préalables, du besoin de sécurité juridique dans un contexte de sanctions renforcées, du besoin de simplification exacerbé des petits acteurs notamment : le guide PME-TPE en partenariat avec la BPI (Banque Publique d'Investissement) en est un exemple, tout comme le futur guide dédié aux collectivités territoriales.

La CNIL a eu le souci de toucher tous les publics, y compris les plus éloignés du numérique. Pour ces derniers, elle a ainsi élaboré en 2018 des recommandations pour les professionnels du secteur social (Professionnels du secteur social : comment mieux protéger les données de vos usagers ?) et pour les usagers (Sur un ordinateur public, je protège mes données).
Un dernier mot sur ce que signifie « appliquer » un texte en matière numérique. En donner les clés de lecture, ce n'est pas la fin du processus. Cette démarche doit être prolongée par un travail, technologico-juridique, de prise en compte fine de la manière dont les professionnels et les particuliers interagissent avec les technologies. C'est cette préoccupation que traduit, entre autres, le cahier publié en janvier 2019, consacré à la « forme des choix » : la CNIL s'est intéressée à la manière dont le design des interfaces numériques peut, très concrètement, contribuer à de bons ou mauvais usages de nos données personnelles.

INNOVATION

Parce qu'il s'agit de l'une des valeurs de la CNIL, le travail de l'année 2018 a, comme les années précédentes, été également marqué par un souci d'innover dans les outils ou les pratiques, pour mieux toucher la cible. L'année 2018 a vu le passage à la deuxième version enrichie du logiciel, en code source ouvert, développé par la CNIL pour aider gratuitement les professionnels à rédiger leurs analyses d'impact relatives à la protection des données (AIPD), désormais traduit en 18 langues. Ce logiciel a été récompensé par deux "Global Privacy and Data Protection Awards 2018" à l'occasion de la conférence mondiale des autorités de protection des données. La CNIL a par ailleurs travaillé tout au long de l'année sur une formation en ligne ouverte à tous (MOOC), mise à disposition en mars 2019, qui permet de démultiplier son action de montée en compétence des professionnels et qui rencontre, depuis son ouverture, un grand succès.

Autre innovation, dans les outils juridiques : la CNIL va progressivement publier des « référentiels » pour guider les professionnels dans le pilotage de leur conformité, qu'elle a commencé à élaborer en 2018. Ce recours au « droit souple », comme d'autres autorités de régulation le mettent en œuvre, est un exercice délicat dans le champ du RGPD. En effet, les traitements de données d'une même catégorie (gestion des ressources humaines, gestion de la clientèle, *etc.*) sont en réalité très variés dans les organismes : il est impossible de tout couvrir. Et il ne s'agit pas de se substituer aux professionnels, compte tenu de l'esprit de responsabilisation qui anime le RGPD. La construction en cours des référentiels cherche donc à tenir cette ligne de crête.

« Les communautés professionnelles ont un rôle à jouer pour favoriser la montée en compétence sur la vie privée. »

DÉMULTIPLICATION

L'année 2018 a enfin été marquée par un dernier objectif : encourager, par de multiples canaux, la montée en compétence Informatique et Libertés du tissu administratif et économique. La CNIL est et reste une référence, pour les Français, sur un plan juridique et éthique, et dispose de l'ensemble des pouvoirs d'accompagnement et de sanction lui permettant de jouer son rôle de régulateur. Mais la bonne application du cadre juridique, le respect plein et entier des droits des personnes, doivent avant tout reposer, à la racine, sur une parfaite appropriation de ces règles et des principaux réflexes, dans chaque secteur d'activité, dans chaque entreprise ou administration.

Dans cet objectif, la CNIL a mis l'accent en 2018 sur l'accompagnement de la nouvelle fonction de délégué à la protection des données. Elle a également immédiatement investi sa nouvelle compétence en matière de certification, qui permettra un essaimage du souci de qualité en matière Informatique et Libertés, en adoptant son premier référentiel – précisément consacré à la certification des compétences des délégués. Elle a également poursuivi sa stratégie d'appui aux « têtes de réseau », en incitant les organisations professionnelles du secteur public et du secteur privé à se structurer sur les sujets Informatique et Libertés, afin d'être un premier point de contact pour les professionnels, et un interlocuteur à part entière pour la CNIL. Elle a incité, dans ses travaux sur le design, à l'émergence d'une communauté de designers partageant leur regard, technique et éthique, sur leurs pratiques professionnelles dans ce contexte.

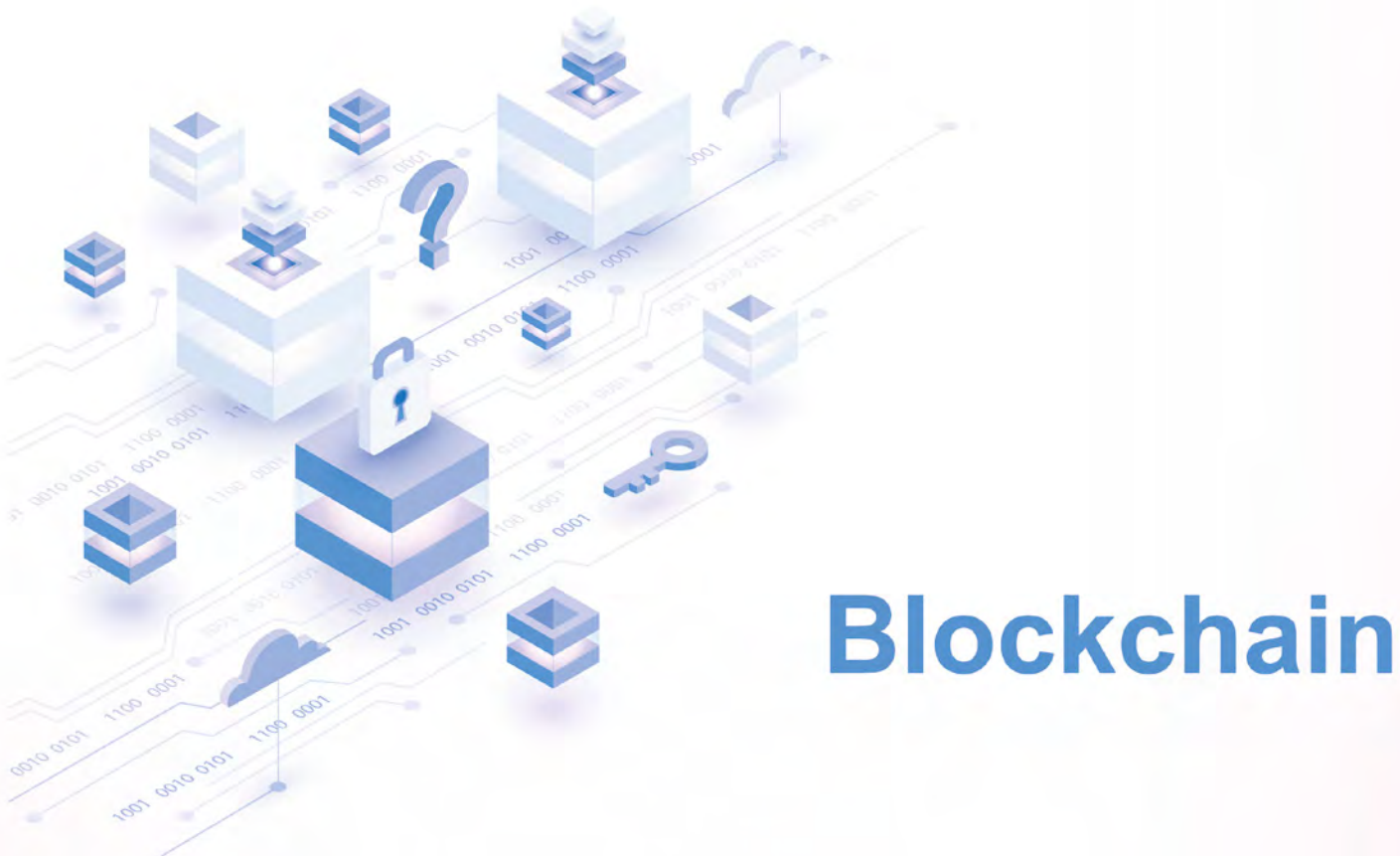
De manière plus générale, la CNIL est convaincue du rôle joué par les communautés professionnelles, regroupant délégués ou organismes, pour favoriser la montée en compétence sur la vie privée dans un univers numérique fondamentalement hétérogène et atomisé. C'est une condition de réussite du RGPD !

« La bonne application du RGPD repose sur l'appropriation des règles et des réflexes dans chaque secteur. »

Analyses

Premiers éléments d'analyse sur la chaîne de blocs (*blockchain*)

La chaîne de blocs, connue également par le terme anglais « *blockchain* », est une technologie au potentiel de développement fort et qui suscite de nombreuses questions, dont parfois celle de sa compatibilité au Règlement général sur la protection des données (RGPD). En tant que technologie sur laquelle peut reposer un traitement de données à caractère personnel, son architecture et ses caractéristiques posent des questions réelles au regard de la protection des données. Toutefois, la CNIL considère que cette innovation et la protection des droits fondamentaux des personnes ne sont pas deux objectifs antagonistes.
Ce contexte a amené la CNIL à se saisir du sujet et à publier sur son site des premiers éléments d'analyse à destination des acteurs qui souhaitent recourir à cette technologie.



QU'EST-CE QUE LA CHAÎNE DE BLOCS (*BLOCKCHAIN*) ?

La *blockchain*[1] est une base de données dont le contenu est distribué sur un grand nombre d'ordinateurs possédés par des personnes ne se connaissant pas. Les informations envoyées par les utilisateurs pour y être stockées y sont regroupées dans des blocs reliés entre eux par un mécanisme cryptographique. Cela forme ainsi une chaîne de blocs, d'où le terme *blockchain*.

Les écritures qui y sont effectuées, appelées « transactions », sont visibles de l'ensemble des utilisateurs de la *blockchain*, depuis sa création. La distribution de la base de données du registre augmente sa robustesse : la base est répartie entre ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier qu'elle n'est modifiée que par l'ajout de nouveaux blocs.

Une des caractéristiques notables des technologies de la chaîne de blocs est que les transactions effectuées entre les utilisateurs du réseau sont regroupées par « blocs ». On appelle ainsi des conteneurs numériques contenant chacun plusieurs transactions validées. Les blocs sont chaînés entre eux (d'où le nom) dans l'ordre chronologique de traitement, au moyen de techniques cryptographiques qui les rendent solidaires les uns des autres : il est alors mathématiquement très difficile de falsifier un bloc (c'est-à-dire, modifier son contenu sans que cela ne « rompe » la chaîne et donc que cette tentative de falsification ne soit détectée[2]). L'ensemble des blocs forme donc une base de données distribuée et répliquée, mise à jour de façon chronologique.

Quelles sont les caractéristiques et les différents types de chaînes de blocs ?

La CNIL distingue trois types d'acteurs dans une chaîne de blocs :

- les « **accédants** » qui ont un droit de lecture et d'obtention d'une copie de la chaîne ;
- les « **participants** » qui ont un droit d'écriture (la création d'une transaction qu'ils soumettent à validation) ;
- les « **mineurs** » qui valident une transaction et créent les blocs en appliquant les règles de la *blockchain* afin qu'ils soient acceptés par la communauté.

La *blockchain* possède les propriétés suivantes :

- **transparence** : tout participant, voire toute personne intéressée dans le cas de certaines *blockchains*, peut voir l'ensemble du contenu du registre, c'est-à-dire l'ensemble des transactions stockées sur la *blockchain* ;
- **partage et décentralisation** : il n'y a pas de serveur centralisé. De nombreux exemplaires de la chaîne existent simultanément sur différents ordinateurs interconnectés. Par défaut, toute personne ou organisme qui participe à une *blockchain* peut conserver la copie intégrale de la base de données, comprenant l'ensemble des transactions enregistrées depuis l'origine de la chaîne ;
- **irréversibilité** : une fois que le bloc auquel est intégré une transaction a été accepté par un grand nombre de participants, elle ne peut plus être modifiée ou supprimée ;
- **désintermédiation** : toute décision se fait par consensus entre les participants, sans arbitre centralisé.

En pratique, plusieurs sortes de *blockchains* coexistent, mettant en œuvre des niveaux de permission différents en fonction de : qui peut lire la *blockchain* ? Qui peut écrire les blocs ? Comment est effectuée leur validation ?

La classification suivante permet de distinguer les types de *blockchains* existants :

- les ***blockchains* publiques**, accessibles à n'importe qui dans le monde, permettent à toute personne d'effectuer une transaction, de participer au processus de validation des blocs ou d'obtenir une copie de la *blockchain* ;
- les ***blockchains* à permission** pour lesquelles un groupe de personnes physiques ou morales ayant des intérêts communs décident de construire une chaîne pour leur seul usage. Celles-ci sont accessibles à tous ou en accès limité, intègrent des règles définissant quelles personnes peuvent participer au processus d'approbation ou même effectuer des transactions ;
- les ***blockchains*** dites **privées** sont sous le contrôle d'un acteur qui assure seul la vérification de la participation et de la validation. En pratique, elles sont similaires à des bases de données distribuées et ne soulèvent pas de question de conformité particulière.

Chacun de ces rôles peut être porté par des personnes physiques ou morales.

« La chaîne de blocs et la protection des droits fondamentaux des personnes ne sont pas deux objectifs antagonistes. »

1 Le terme *blockchain* est parfois accompagné d'une expression désignant une famille de technologies plus large : celle des registres distribués, ou DLT pour « distributed ledger technology ». Si la CNIL s'intéresse au développement de ces registres, qui incluent les *blockchains*, elle a néanmoins choisi de concentrer son analyse sur la seule technologie *blockchain*, dans la mesure où les solutions DLT qui ne sont pas des *blockchains* sont encore trop récentes et rares pour permettre une analyse générique.

2 Le nouveau bloc est construit sur la base du bloc qui le précède dans la chaîne.

« La chaîne de blocs n'est pas un traitement de données à caractère personnel mais une technologie sur laquelle repose un traitement. »

À quoi une chaîne de blocs peut-elle servir ?

Une *blockchain* sert à enregistrer des transactions entre des parties. Le type de transactions possibles dépend de chaque chaîne, mais celles-ci sont généralement de trois ordres[3] :

- un **transfert d'actifs** (ex : Bitcoin ou titres de propriété.) ;
- une **inscription d'une information sur la chaîne en tant que registre horodaté assurant une traçabilité** (ex : certification de diplômes) ;
- une **demande de lancement d'un contrat intelligent ou *smart contract*** : il s'agit de programmes autonomes qui « figent » dans la *blockchain* l'accord trouvé par deux parties. Lorsque tous les engagements préalables à l'exécution d'une obligation ont été respectés, cette dernière s'auto-exécute, sans qu'aucune des parties ne puisse s'y opposer. La souscription à un contrat demeure « classique », mais l'exécution de l'engagement par l'une des parties devient automatisée.

Quels sont les usages qui impliquent, directement ou indirectement des données personnelles ?

Deux catégories de données à caractère personnel peuvent être trouvées dans une *blockchain* :

- **l'identifiant des participants et des mineurs :** chaque participant et chaque mineur dispose d'une paire de clés cryptographiques, l'une étant publique et l'autre étant privée. La clé privée sera utilisée par un participant pour signer[4] une transaction et ainsi prouver qu'il en est l'émetteur. Un mineur utilisera la sienne pour signer le bloc qu'il a validé et ainsi prouver à tous qu'il est celui qui l'a validé. Pour les participants comme pour les mineurs, la clé publique correspondante aura une double fonction : tout d'abord elle permet de vérifier qu'une signature a bien été émise par la personne qui la revendique. Par ailleurs, elle est utilisée comme identifiant, notamment pour désigner le destinataire d'une transaction ;
- des **données complémentaires**, inscrites dans une transaction (ex : diplôme, titre de propriété) qui peuvent être relatives à des personnes physiques, éventuellement autres que les participants, directement ou indirectement identifiables.

Quels sont les enjeux de conformité ?

Certaines mises en œuvre de cette technologie sont susceptibles de soulever des difficultés au regard du RGPD. Ainsi, les obligations liées à la sous-traitance ou les règles encadrant les transferts internationaux de données personnelles, nécessitent une vigilance particulière des acteurs ayant recours à la *blockchain*, notamment lorsqu'il s'agit d'une *blockchain* publique.

C'est également le cas du respect des durées de conservation ou de l'exercice des droits d'effacement, de rectification et d'opposition, pour lesquels des solutions techniques relatives au format de stockage de la donnée permettent, dans certains cas, d'apporter des solutions. Enfin, le droit à une intervention humaine dans le cadre de la prise d'une décision entièrement automatisée (article 22 alinéa 3 du RGPD) ainsi que le droit à la limitation doivent être pris en compte dans le cadre des *smart contract*.

Ces points d'attention nécessitent donc d'**apprécier l'intérêt réel de la *blockchain* et de sa mise en œuvre concrète au regard des objectifs et des caractéristiques de chaque traitement.**

FOCUS

Anonyme la *blockchain* ?

L'utilisation de clés publiques pour désigner les comptes des utilisateurs amène certains à parler à tort de l'anonymat de la *blockchain*. En effet, ces suites de caractères alphanumériques qui semblent aléatoires correspondent à un numéro de compte. Il faudrait plutôt parler de pseudonymat associé à une très forte traçabilité de l'historique des transactions effectuées avec chaque compte depuis sa création. C'est l'équivalent d'un compte en banque à numéro, pour lequel toutes les transactions sont enregistrées dans la chaîne et visibles de tous ceux qui y ont accès. Ainsi, si le compte utilisé dans une transaction est relié, un jour, à une personne physique, alors il sera possible de retrouver l'ensemble des transactions effectuées par cette personne avec ce compte depuis sa création.

3 Source : *blockchain* France https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

4 https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

QUELLES PISTES DE SOLUTIONS ?

Responsabilité et sous-traitance

La *blockchain* n'étant qu'une technologie, la responsabilité des acteurs s'analyse en fonction du traitement considéré. Il apparait que le participant détermine les finalités (les objectifs poursuivis par le traitement) et les moyens mis en œuvre (format de la donnée, recours à la technologie *blockchain*, *etc.*).

Ainsi, le participant peut être responsable de traitement lorsqu'il est une personne physique et que le traitement de données personnelles n'a pas lieu dans un cadre strictement personnel ou domestique. Une personne morale qui inscrit des données à caractère personnel sur la *blockchain* dans le cadre de son traitement pourra également être responsable de traitement.

Par exemple, *une personne physique qui procède à la vente ou à l'achat de Bitcoin pour son propre compte n'est pas responsable de traitement. Elle peut en revanche être considérée comme responsable de traitement si elle procède à ces transactions dans le cadre d'une activité professionnelle ou commerciale, pour le compte d'autres personnes physiques, comme par exemple un huissier qui enregistre les constats réalisés pour ses clients dans une blockchain.*

De même, lorsqu'un groupe de participants décide de mettre en œuvre un traitement ayant une finalité commune, il est nécessaire d'identifier un ou plusieurs responsables de traitements. Par exemple, les participants peuvent créer une personne morale sous la forme d'une association ou d'un GIE. Elles peuvent également choisir d'identifier un participant qui prend les décisions pour le groupe et de le désigner comme responsable de traitement. À défaut, tous les participants pourraient être considérés comme ayant une responsabilité conjointe.

FOCUS

Les développeurs de *smart contracts*

Comme pour tout logiciel, le concepteur de l'algorithme d'un *smart contract* est un simple fournisseur de solution. Toutefois, lorsqu'il participe au traitement, il peut être qualifié de sous-traitant ou de responsable de traitement s'il traite des données à caractère personnel, en fonction de son rôle dans la détermination des finalités.

INFOSPLUS

Comment la CNIL a-t-elle travaillé ?

Dès 2016, la CNIL a exploré les enjeux de la *blockchain*, en publiant des analyses d'articles et rapports sur LINC (le média d'innovation et prospective de la CNIL).

L'intérêt pour cette technologie a conduit à poursuivre ces travaux par une analyse juridico-technique. Dans une démarche de co- construction, la CNIL s'est appuyée sur des demandes concrètes d'acteurs privés (grandes entreprises, start-ups, *etc.*) comme publics, provenant en particulier du secteur de la santé et des institutions financières. Ces nombreux échanges ont permis à la CNIL de constater la diversité des usages et les réalités très variables que recouvre cette technologie.

« Pour la CNIL, les participants qui soumettent des données à caractère personnel à validation des mineurs sont responsables de traitement. »

La qualification des mineurs

Il est possible de considérer, dans certains cas, **les mineurs comme des sous-traitants** au sens du RGPD, car ils exécutent les instructions du responsable de traitement lorsqu'ils vérifient que la transaction respecte des critères techniques.

Par exemple, *supposons que plusieurs compagnies d'assurance décident de créer une blockchain à permission pour leur traitement ayant pour finalité le respect de leurs obligations légales de connaissance client et qu'elles choisissent de s'écarter de la solution par défaut, la responsabilité conjointe, en donnant à l'une d'entre elles la responsabilité du traitement. Dans ce cas, les autres compagnies d'assurance, qui valident les transactions seraient des mineurs susceptibles d'être considérés comme sous-traitants. Elles devraient donc établir avec la compagnie d'assurance*

responsable de traitement, un contrat précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du RGPD.

Il va sans dire que la qualification de mineurs en tant que sous-traitant dans la *blockchain* publique peut soulever quelques difficultés ; la CNIL mène actuellement une réflexion approfondie sur cette question.

Transferts internationaux

S'agissant plus particulièrement des transferts internationaux de données, il est important de se rappeler que toute transaction sur une *blockchain* implique :

- un envoi à tous les mineurs de la *blockchain* d'une demande de validation d'une transaction (et donc potentiellement de données personnelles) ;
- une mise à jour de la *blockchain* par l'ajout du nouveau bloc dans la *blockchain* auprès de tous les participants.

S'il apparaît qu'**il existe des solutions pour encadrer les transferts dans une *blockchain* à permission**, telles que les clauses contractuelles types, les règles d'entreprises contraignantes, les codes de conduite ou encore les mécanismes de certification, la CNIL constate qu'elles sont plus difficiles à mettre en œuvre dans le cadre d'une *blockchain* publique, dans la mesure où le responsable de traitement peut difficilement exercer un contrôle sur la localisation des mineurs.

> « Au-delà de la question du recours ou non à la chaîne de blocs, le responsable de traitement doit aussi s'interroger sur le type de *blockchain* à privilégier et sur ses choix de mise en œuvre. »

Minimisation et durée de conservation

S'agissant des identifiants des participants et des mineurs, l'architecture même de la *blockchain* rend ces données toujours visibles, car elles sont indispensables à son bon fonctionnement. Ainsi, la CNIL considère qu'il n'est pas possible de les minimiser davantage et que leurs durées de conservation sont, par essence, alignées sur celles de la durée de vie de la *blockchain*.

S'agissant des données complémentaires, afin d'assurer le respect des obligations de protection des données dès la conception et par défaut, et de minimisation des données, la CNIL recommande de :

- **privilégier les solutions dans lesquelles les données personnelles sont traitées en dehors de la *blockchain*** (comme par exemple sur le système d'information du responsable de traitement) ;
- **ne stocker dans la *blockchain* qu'une information prouvant l'existence de la donnée.**

Il est donc recommandé de ne stocker sur la *blockchain* que les éléments suivants (par ordre de préférence) :

- un engagement cryptographique ;
- une empreinte de la donnée obtenue par une fonction de hachage à clé ;
- un chiffré de la donnée.

Néanmoins, si la finalité du traitement le justifie et qu'une analyse d'impact a démontré que les risques résiduels sont acceptables, il pourrait être envisageable que des données puissent exceptionnellement être enregistrées sur une *blockchain* sous la forme d'une empreinte classique (sans clé) voire en clair. En effet, certains responsables de traitement peuvent avoir une obligation légale de rendre publiques et accessibles, sans limitation de durée, certaines informations.

DÉFINITION

Un « **engagement cryptographique** » est un mécanisme qui permet de figer une donnée de telle sorte qu'il soit possible, avec des éléments supplémentaires, de prouver ce qui a été figé, et à la fois impossible de la retrouver ou de la reconnaître à partir de cette seule version « engagée ».

Pour certains engagements cryptographiques, ceux dit parfaitement indistinguables (« *perfectly hiding* »), la suppression des éléments stockés hors de la *blockchain* rend mathématiquement impossible de prouver, de vérifier voir même de reconnaître quelle information avait été engagée. L'élément figé dans la *blockchain*, l'engagement en lui-même, perd tout lien avec toute personne physique et perd sa qualification de donnée à caractère personnel.

Exercice des droits à l'effacement, à la rectification ou à l'opposition

Lorsque la donnée inscrite sur une *blockchain* est uniquement engagement, une empreinte issue d'une fonction de hachage à clé ou un chiffré utilisant un algorithme et des clés conformes à l'état de l'art, le responsable de traitement peut rendre la donnée quasi-inaccessible, et se rapprocher ainsi des effets d'un effacement de la donnée.

Par exemple, *la suppression de la clé secrète utilisée pour chiffrer les données les rendra inaccessibles. Il ne sera plus possible d'accéder à l'information tant que l'algorithme utilisé reste robuste et que la clé secrète ne peut être retrouvée.*

En dehors du cas spécifique de certains engagements cryptographiques, ces solutions ne constituent pas un effacement de la donnée au sens strict dans la mesure où les données existent toujours sur la *blockchain* et que certaines attaques pourraient permettre de retrouver ou de reconnaître les données stockées. Néanmoins, la CNIL constate que ces solutions permettent de se rapprocher de l'exercice effectif du droit à l'effacement pour la personne concernée. Leur équivalence avec les exigences du RGPD doit être évaluée.

Concernant le droit à la rectification, l'absence de possibilité de modification des données inscrites dans un bloc doit conduire le responsable de traitement à inscrire la donnée mise à jour dans un nouveau bloc.

« Il est fortement recommandé de ne pas inscrire une donnée à caractère personnel en clair sur la chaîne de blocs. »

Le droit à une intervention humaine

Il apparait que la décision entièrement automatisée provenant d'un *smart contract* est nécessaire à son exécution, dans la mesure où elle permet de réaliser l'essence même du contrat (ce pourquoi les parties se sont engagées). La personne concernée devrait pouvoir obtenir une intervention humaine, exprimer son point de vue et contester la décision après que le *smart contract* a été exécuté. Il convient donc que le responsable de traitement prévoie, au moment de la rédaction du programme, la possibilité d'une intervention humaine qui permette de remettre en cause la décision en permettant à la personne concernée de contester la décision.

Le droit à la limitation

Le droit à la limitation du traitement fait partie des nouveaux droits institués par le RGPD. Il permet à une personne de demander provisoirement la suspension du traitement de ses données lorsqu'elle conteste, par exemple, l'exactitude des données. Celui-ci pourrait être techniquement difficile à mettre en œuvre dans le cas des *smart contracts* existants dans la mesure où il n'y a pas d'intervention humaine dans leur fonctionnement et qu'il s'agit uniquement d'un logiciel. Il convient donc de le prévoir en amont avant sa mise en œuvre, en tenant compte du fait que seule une réflexion préalable sur le format de stockage des données permettrait de limiter l'accès à celles-ci lors d'une telle demande.

Les autres droits

Le droit à l'information des personnes ne pose pas de difficultés particulières : le responsable de traitement participant devra ainsi fournir une information concise, aisément accessible et formulée en des termes clairs à la personne concernée avant de soumettre à validation des mineurs une donnée à caractère personnel. Il en va de même en ce qui concerne le droit d'accès et le droit à la portabilité : la CNIL considère que l'exercice de ces droits est **compatible avec les propriétés techniques de la *blockchain***.

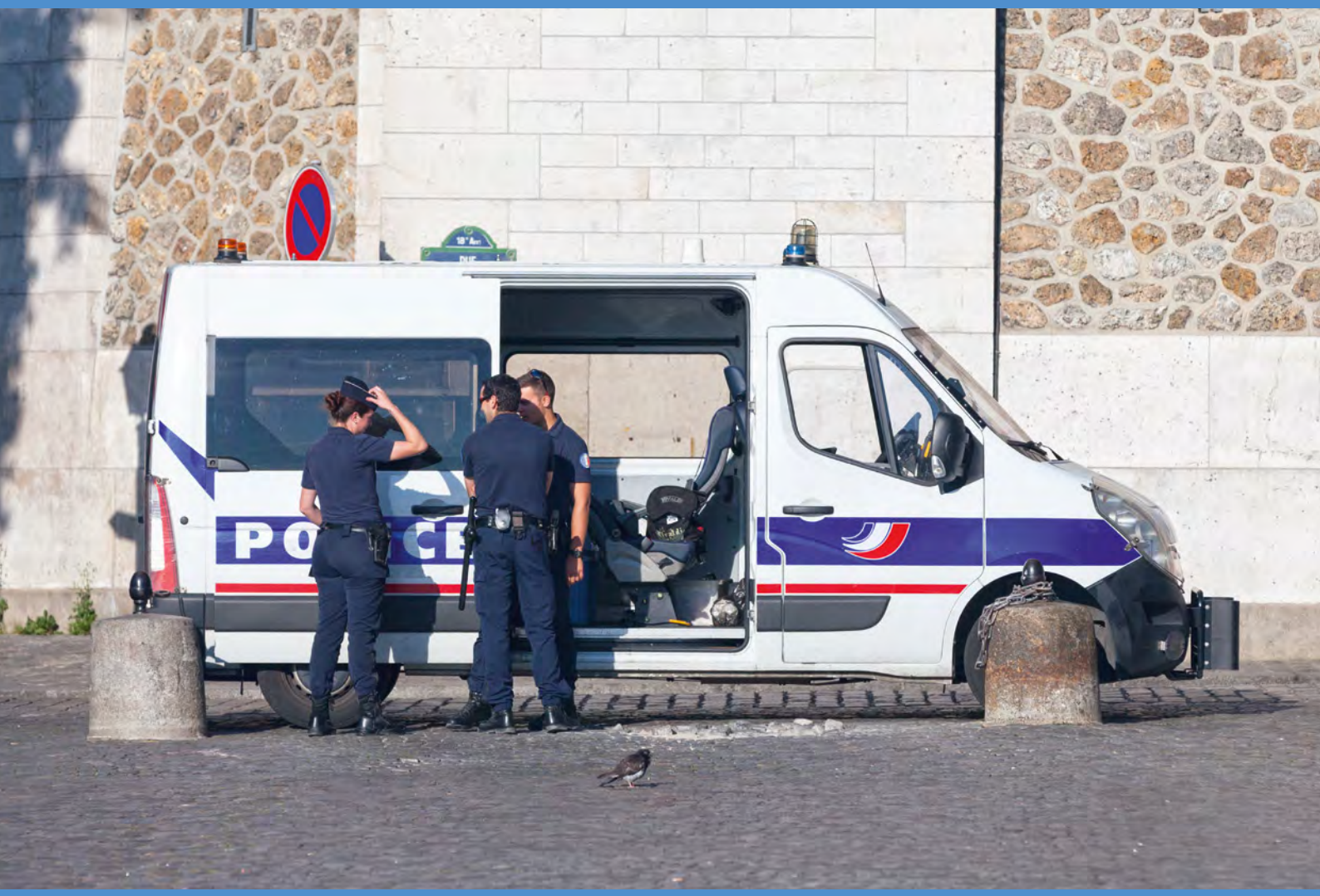
Quel plan d'action pour la CNIL ?

Les enjeux que présentent la *blockchain* en termes de respect des droits et libertés fondamentaux appellent nécessairement une réponse au niveau européen. La CNIL est l'une des premières autorités à s'être saisi officiellement du sujet et va porter ces premiers éléments d'analyse auprès de ses homologues européens pour proposer une approche solide et harmonisée.

Par ailleurs, la CNIL est également sollicitée par les pouvoirs publics dans le cadre du développement de l'écosystème français de la *blockchain*.

Droit d'accés indirect : modification importante des modalités d'exercice des droits pour certains fichiers

L'année 2018 a été marquée par une évolution majeure dans les modalités d'exercice des droits pour les fichiers relevant du champ de la directive européenne « police-justice », à savoir ceux ayant pour finalité « la prévention et la détection d'infractions pénales, les enquêtes ou poursuites en la matière y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ». Cela concerne un nombre très important de fichiers relevant, à titre principal, du ministère de l'Intérieur.



L'INSTAURATION DU PRINCIPE DE L'EXERCICE DIRECT DES DROITS POUR LES TRAITEMENTS RELEVANT DU CHAMP DE LA DIRECTIVE EUROPÉENNE DITE « DIRECTIVE POLICE-JUSTICE »

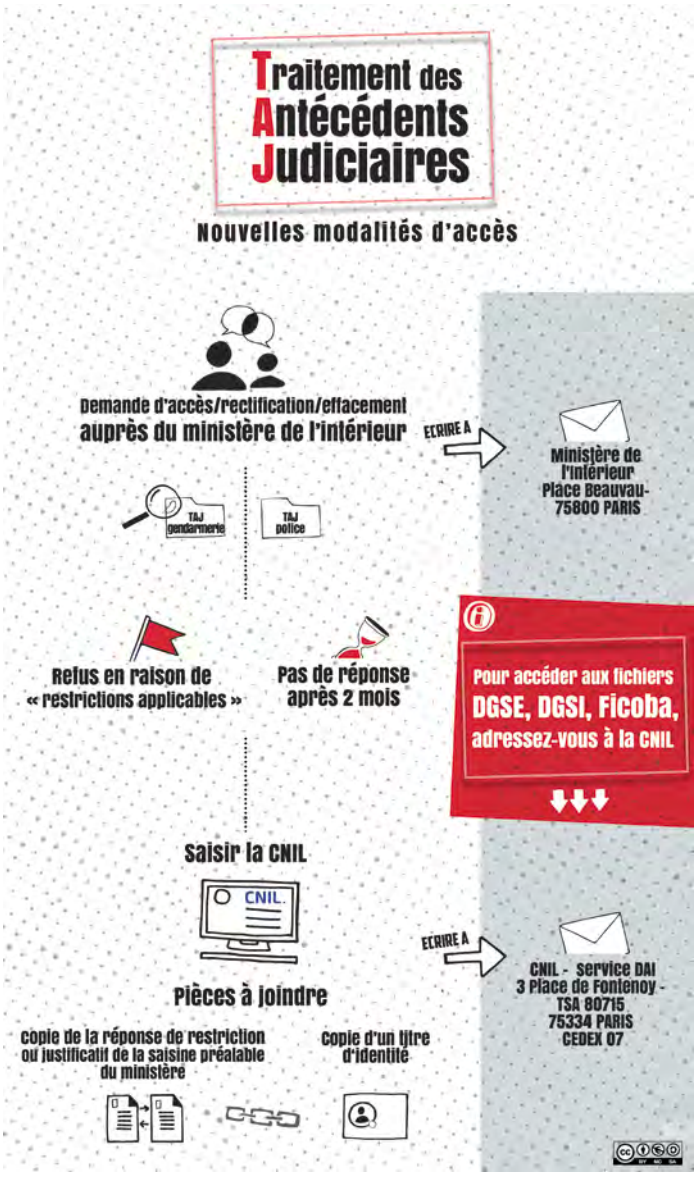
Auparavant, ces fichiers étaient pour la plupart soumis au principe du « droit d'accès indirect ». Les personnes qui souhaitaient faire vérifier les données les concernant susceptibles d'être enregistrées dans ces fichiers pouvaient adresser une demande à la CNIL, accompagnée d'une copie d'un titre d'identité et, pour les fichiers « police-justice », de tout élément prouvant la restriction du responsable du traitement dans le cadre de l'exercice direct et préalable des droits.

Le nouveau cadre législatif et règlementaire, issu de la loi du 20 juin 2018 relative à la protection des données personnelles et du décret du 1er août 2018 en portant application prévoit désormais, pour les fichiers concernés, **le principe de l'exercice direct des droits** (accès, rectification, effacement voire limitation) auprès du responsable du traitement, **sous réserve des restrictions applicables** à chacun d'entre eux qui doivent être définies par le décret les régissant.

La CNIL n'est donc plus en principe l'interlocutrice première des personnes pour la majeure partie des fichiers qui étaient jusqu'à présent soumis au régime du droit d'accès indirect tel que le Traitement d'Antécédents Judiciaires (TAJ) de la police et de la gendarmerie nationales, successeur depuis le 1er janvier 2014 des fichiers STIC et JUDEX.

Toute personne souhaitant exercer ses droits pour les fichiers concernés doit désormais effectuer directement une demande auprès de l'administration gestionnaire. Ce n'est que si, au terme d'un délai de deux mois, ce dernier lui oppose une restriction ou ne lui apporte aucune réponse, qu'elle a alors la possibilité, en deuxième ligne, de saisir la CNIL au titre de l'exercice indirect des droits. Elle peut également engager un recours auprès des juridictions administratives contre la décision de restriction opposée par le responsable du traitement.

Nouvelles modalités d'exercice des droits pour les fichiers relevant du champ de la directive européenne « police-justice » : l'exemple du Traitement d'Antécédents Judiciaires (TAJ)



À ce stade, seuls les décrets instaurant le TAJ et le fichier GENESIS de l'administration pénitentiaire ont été modifiés à la lumière des dispositions législatives nouvelles. Ce nouveau principe s'applique également à tous les fichiers relevant du champ de la directive « police-justice » tant que le Gouvernement n'a pas formellement modifié les décrets créant ces fichiers pour prévoir d'éventuelles restrictions (c'est-à-dire la possibilité d'un exercice indirect des droits auprès de la CNIL).

Cette évolution majeure dans l'exercice des droits s'est par ailleurs accompagnée d'une obligation, pour la CNIL, de procéder au transfert de toutes les demandes qui étaient en cours relatives aux fichiers concernés à chaque responsable de traitement (article 32 du décret). La Commission avait cependant relevé dans son avis sur ce projet de décret qu'il aurait été préférable, en termes de simplicité administrative, qu'elle puisse poursuivre le traitement des demandes des personnes ayant engagé une telle démarche auprès d'elle avant cette réforme pour ne pas les pénaliser en termes de délais. L'absence de dispositions transitoires n'a ainsi pas permis à la CNIL d'aller au terme des vérifications engagées pour ces demandeurs majoritairement concernés par des problématiques d'emploi (refus d'agrément en raison de leur inscription dans le TAJ).

1 573 demandes de droit d'accès indirect (dossiers en cours de traitement et demandes reçues après le 1er août 2018) ont été transférées au ministère de l'Intérieur et, dans une moindre proportion, aux ministères de la Justice et de l'Action et des Comptes publics en informant chaque personne de cette transmission. Au 31 décembre 2018, 124 personnes sont revenues vers la CNIL pour l'exercice indirect de leurs droits après restriction du responsable du traitement ou à défaut de réponse.

La CNIL reste, en revanche, l'interlocutrice unique au titre du droit d'accès indirect pour les traitements intéressant la sûreté de l'État qui sont en dehors du champ d'application des textes européens (fichiers de la DGSI, de la DGSE, de la DRSD, *etc.*), ainsi que pour certains fichiers auxquels s'appliquent les limitations à l'exercice des droits prévus par l'article 23 du RGPD, tel que le fichier FICOBA de l'administration fiscale pour les données relatives à l'identification des comptes bancaires.

> « La mise en place du principe d'exercice direct des droits constitue, en soi, une avancée importante pour les personnes. »

Les points d'attention de la CNIL sur le nouveau dispositif d'exercice direct des droits

La mise en place du principe d'exercice direct des droits constitue, en soi, une avancée importante pour les personnes. Toutefois, il faut que soit trouvé un équilibre entre cet objectif de renforcement des droits des personnes et la faculté ouverte aux administrations gestionnaires d'opposer, au cas par cas, une restriction.

La CNIL estime qu'il sera nécessaire d'en établir un bilan au terme d'une première période d'application.

Il conviendra en particulier de veiller à ce que le nouveau dispositif ne conduise pas, pour certains fichiers ou certaines catégories de données, à ce que des restrictions soient quasi-systématiquement opposées par les responsables de fichiers aux demandes d'accès. Si un tel scénario se concrétisait, les délais de traitement des demandes s'en trouveraient en effet allongés inutilement : l'étape de la demande préalable auprès du responsable de fichier s'intercale en effet désormais obligatoirement avant la saisine éventuelle de la CNIL ou du juge (2 mois d'attente pour la réponse du responsable du traitement auquel s'ajoute, au moins, un délai équivalent de traitement par la CNIL en cas de restriction). Ainsi, dans les hypothèses où **la nature du fichier et de tout ou partie des données qu'il contient ne pourrait en réalité qu'aboutir à une telle situation, la piste du rétablissement d'un exercice immédiat du droit d'accès indirect auprès de la CNIL ne devrait pas être écartée de la réflexion. A tout le moins, les délais de traitement de la demande d'accès par le responsable de traitement devraient être raccourcis au maximum, quel que soit le sens de la réponse à cette demande.**

La CNIL a également relevé, dans son avis sur le décret du 1er août 2018, que le dispositif nouveau complexifie la compréhension, par les personnes, des modalités d'exercice de leurs droits et qu'il est nécessaire que les ministères puissent mettre à disposition du grand public toute information utile sur les différents fichiers concernés en désignant notamment pour chacun d'entre eux, les services auxquels les personnes doivent s'adresser pour exercer leurs droits.

L'intelligence artificielle, nouvelle étape de la société numérique

Partout dans le monde, les initiatives et stratégies dédiées à l'intelligence artificielle (IA) se sont multipliées. La CNIL voit dans cette tendance autant la quintessence d'une innovation numérique prolifique, où les données personnelles occupent une place majeure, que la confirmation de l'impératif, quelques mois après l'entrée en application du RGPD, de l'ancrer dans un substrat juridico-éthique exigeant. Après la formulation de propositions à l'issue d'un débat public national multi-acteurs, la CNIL continue à contribuer à la construction de ce nouveau cadre, par des actions de sensibilisation et une participation aux discussions européennes et internationales.

LES PROGRÈS RÉCENTS DE L'INTELLIGENCE ARTIFICIELLE (IA) : UNE RÉVOLUTION

En 2017, un sondage réalisé par l'IFOP pour la CNIL sur les algorithmes et l'intelligence artificielle révélait que seulement 31 % des interrogés estimaient « savoir précisément de quoi il s'agit ».

La CNIL souhaite participer à la pédagogie sur le nouveau potentiel technologique de croisement et d'analyse de données que constitue l'intelligence artificielle, dans des champs aussi variés que la médecine, la sécurité publique ou la justice.

Au titre de sa mission de réflexion sur les questions éthiques et les enjeux de société soulevés par les technologies numériques, elle avait mobilisé en 2017 une soixantaine de partenaires dans le cadre d'un débat public ayant abouti à la publication d'un rapport sur les algorithmes et l'intelligence artificielle. Cette réflexion, qui a mobilisé une diversité de parties-prenantes (institutions publiques, entreprises, société civile), a permis de confirmer que l'intelligence artificielle constitue une étape majeure pour nos sociétés. Si le concept, né dans le milieu de la cybernétique dès les années 1950, n'est pas nouveau, un changement d'échelle important est observable depuis quelques années. Il s'explique par la conjonction de plusieurs facteurs : l'abondance des données personnelles dans nos sociétés numérisées, l'accroissement des capacités de calcul et de stockage, et les progrès considérables de l'algorithmie.

Les différents types d'IA

Bien que l'IA recouvre un ensemble de concepts et de technologies, le bouleversement actuel repose principalement sur le développement d'une nouvelle classe d'algorithmes dits d'apprentissage ou de *machine learning*.

En effet, les systèmes d'IA existants peuvent être répartis en deux catégories :

- **d'une part les systèmes à base de règles prédéfinies** (anciennement appelés « systèmes experts ») : ces systèmes sont capables de résoudre des problèmes précis et prédéterminés, en analysant des faits nouveaux à partir de faits et de règles connus. Ces systèmes d'IA peuvent être qualifiés de déterministes, dans la mesure où la réponse qu'ils apportent à une question peut être précisément déterminée en fonction des données d'entrée ainsi que de faits et de règles objectives intégrés dans le système.

- **d'autre part, les systèmes basés sur l'apprentissage automatique** (ou *machine learning* en anglais) : leurs résultats ne sont plus issus d'une programmation explicite par un développeur humain, mais d'une programmation générée par la machine elle-même qui « apprend » à partir des données qui lui sont fournies. Ces systèmes sont ainsi capables de résoudre des problèmes complexes en analysant des données fournies en entrée à l'aide d'algorithmes paramétrés à partir de données d'apprentissage. Ces systèmes d'IA peuvent être qualifiés de statistiques, dans la mesure où leurs résultats sont statistiquement déduits des données d'apprentissages fournies au système. Ils suscitent en conséquence de riches promesses en matière de personnalisation de services, de réduction de certains taux d'erreur, d'optimisation des ressources ou d'aide à la décision voire de prédiction.

Les systèmes utilisant des techniques d'apprentissage automatique peuvent eux-mêmes être répartis en deux catégories :

- les systèmes non-supervisés qui élaborent des classifications et regroupement en fonction de caractéristiques des données sans que celles-ci soient qualifiées[5] par des humains,
- les systèmes supervisés qui utilisent des données d'entrée préalablement qualifiées par des humains pour s'entraîner et ensuite pouvoir classer des données d'entrée non-qualifiées.

Un système d'apprentissage non-supervisé n'est pas capable de qualifier des données, il ne peut que faire des regroupements ou des segmentations d'objets. À l'inverse, un système d'IA supervisé peut qualifier des données, mais uniquement à l'issue d'une phase d'apprentissage nécessitant des données qualifiées par des humains.

Les progrès récents de l'IA

Les progrès récents de l'IA reposent pratiquement exclusivement sur les systèmes d'apprentissage automatique et beaucoup d'entre eux reposent sur des systèmes utilisant des réseaux de neurones artificiels et des nouvelles techniques d'apprentissage dit profond. Ces réseaux de neurones sont constitués d'un assemblage de neurones, qui sont des unités de calcul élémentaires réalisant une opération simple (le terme neurone est donc un peu trompeur car il s'agit d'une simple analogie formelle avec les fonctions réelles des neurones en biologie). L'apprentissage profond consiste quant à lui à modéliser les données traitées avec un haut niveau d'abstraction et à utiliser un nombre de couches de neurones important.

Ces techniques ont permis une progression spectaculaire de l'efficacité des systèmes d'IA et ont, dans une certaine mesure, rendu les systèmes à bases de règles prédéfinies obsolètes dans beaucoup de domaines. Une illustration de cette évolution et de cette nouvelle suprématie est la transition entre **Deep Blue**, super ordinateur d'IBM qui a battu Kasparov aux échecs en 1997, et **AlphaGo**, qui a battu Lee Sedol en 2016 au jeu de Go. Deep Blue utilisait un système à base de règles prédéfinies basées sur l'expérience des meilleurs joueurs d'échecs mondiaux, tandis qu'**AlphaGo** utilise des réseaux de neurones profonds à qui l'on a fait apprendre des millions de parties de Go.

5 Qualifier des données consiste à leur attribuer une ou plusieurs caractéristiques, qui peuvent être de nature très différentes : « est un chat », « est un chien », « est un fraudeur », « est un salarié à haut potentiel », *etc.*

L'autonomie des systèmes d'IA est souvent surestimée

Un premier point qui nécessite clarification est le concept « d'algorithme auto apprenant », souvent cité dans les média comme l'une des révolutions moderne de l'IA. S'il est vrai que les systèmes d'IA basés sur l'apprentissage automatique sont effectivement capables de définir seuls une partie du paramétrage de leur modèle lors de la phase d'apprentissage, il faut relativiser le caractère autonome de cet apprentissage : avant qu'un système d'IA puisse distinguer un chat d'un chien sur une photo, il est nécessaire de l'alimenter avec des milliers de photos de chats et de chiens précisément identifiés. En aucun cas un système d'IA ne sera capable de dire qu'un chat est présent sur une photo sans aucune intervention humaine.

Afin que la phase d'apprentissage soit efficace, les données utilisées pour l'apprentissage supervisé doivent être fournies par des humains. Certaines entreprises utilisent le *crowdsourcing* pour collecter ces données d'apprentissage, comme Google à travers les différents outils de captcha proposés par la société.

Illustration des systèmes de captcha de Google.
(Source : Google)

Recaptcha[6] est offert gratuitement aux sites web mais permet en réalité à Google **d'entraîner les systèmes d'IA qui seront utilisés dans les véhicules autonomes de la société** ainsi qu'à valider les analyses de reconnaissance automatique de caractères réalisées par la société à partir de son programme de numérisation des livres.

Les systèmes d'IA ne conceptualisent pas les objets qu'ils manipulent

Un deuxième point nécessite une clarification : les systèmes d'IA ne conceptualisent pas les objets qu'ils manipulent. Un enfant qui aura appris à reconnaitre les chats comprend intrinsèquement ce qu'est un chat : il est pour lui évident qu'un chat est un animal, qu'un chat a besoin de dormir, de manger, *etc.* *A contrario*, un système d'IA est incapable de conceptualiser ce qu'est un chat : le terme « chat » n'est pas associé à un concept précis, mais est simplement la meilleure réponse statistique d'un problème mathématique complexe que le système a été entraîné à résoudre. Cela signifie notamment qu'un système d'IA ne peut pas « avoir conscience » qu'il est en train de se tromper.

Les systèmes d'IA sont vulnérables

Les systèmes d'IA restent des systèmes informatiques comme les autres qui sont donc susceptibles de présenter des failles ou de subir des dysfonctionnements. Les systèmes d'IA présentent des vulnérabilités spécifiques, notamment celles qui consistent à modifier très légèrement les données d'entrée, d'une façon pratiquement imperceptible pour les humains mais qui modifie complètement le fonctionnement des réseaux de neurones.

Dans l'exemple ci-contre, la photo du panda a été mélangée à une image pseudo aléatoire spécifiquement créée pour interférer avec le fonctionnement d'un système d'IA de reconnaissance d'image, mais qui semblera aléatoire aux humains. La résultante est une photo qu'un humain ne peut différencier de la photo d'origine, mais qui va induire en erreur le système d'IA.

Ce type de manipulation peut être effectué sur des objets physiques, sur des panneaux de signalisation par exemple.

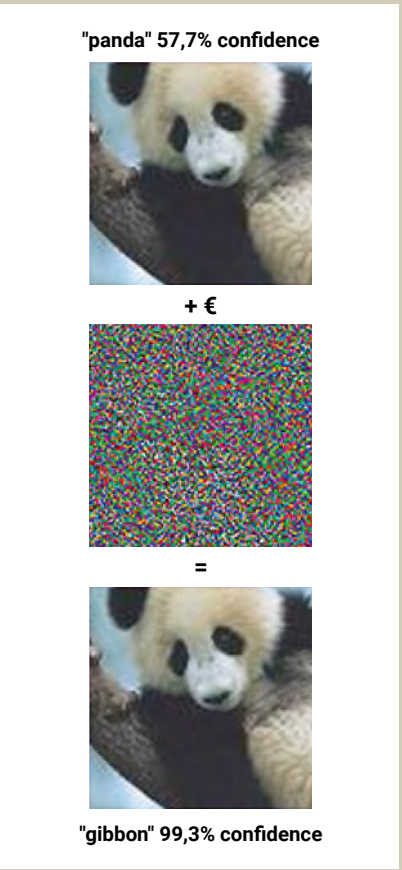


Illustration d'une attaque sur un système d'IA de reconnaissance d'image afin de lui faire prendre un panda pour un gibbon.

(https://spectrum.ieee.org/cars-that-think/transportation/sensors/slight-street-sign-modifications-can-fool-machine-learning-algorithms)

6 https://www.google.com/recaptcha/

Dans ces exemples ci-dessous, des autocollants ont été rajoutés sur les panneaux pour perturber les systèmes de reconnaissance d'image utilisés par des véhicules autonomes en cours de test. Ainsi ces systèmes d'IA ne voient pas de panneau stop, mais voient à la place un panneau de limitation de vitesse à 45 miles par heure[7]. Un humain par contre ne sera que très peu gêné par ces autocollants, qui peuvent ralentir la reconnaissance du panneau, mais qui ne l'empêchent pas. Pour l'heure ces exemples restent anecdotiques et n'engendrent pas de conséquences significatives pour les personnes, mais il est essentiel que ces questions soient traitées avant la généralisation des véhicules autonomes.

Les systèmes d'IA basés sur l'apprentissage automatique commettent des erreurs qu'un humain ne commettrait pas

Les systèmes d'IA sont généralement présentés comme étant capables de meilleures performances que les humains dans certains domaines. Le cas des véhicules autonomes est une illustration de ce qui est présenté comme un axiome : pour les promoteurs des véhicules autonomes, le fait de remplacer tous les conducteurs humains par des systèmes d'IA entraînera une baisse très importante des accidents de la route. Il faut cependant relativiser cette idée en ajoutant qu'une machine peut faire des erreurs qu'un humain ne commettrait jamais.

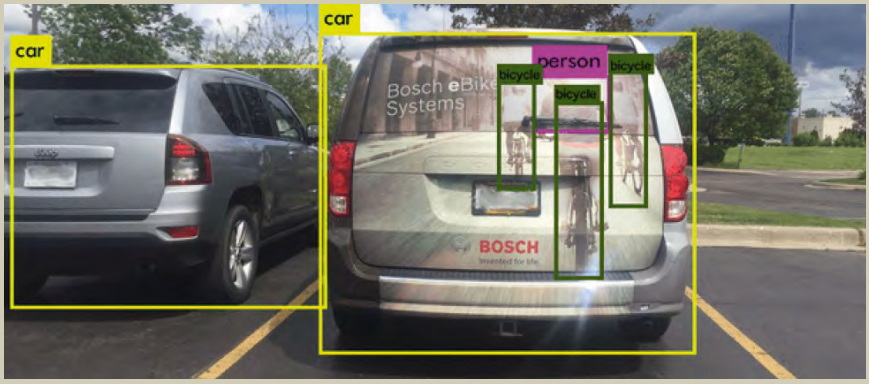


Illustration d'un système de reconnaissance d'image croyant détecter des cyclistes sur le hayon arrière d'un véhicule.

(https://www.theguardian.com/technology/2017/aug/30/self-driving-cars-hackers-security)

L'exemple ci-dessous en est une illustration : une décalcomanie publicitaire a été apposée sur le hayon arrière d'un véhicule, représentant des cyclistes utilisant des vélos électriques. Pour un humain il est évident qu'il s'agit d'une décoration, tandis que pour certains systèmes de reconnaissance d'image il peut s'agir de la juxtaposition d'une voiture, de trois vélos, et d'une personne.

Un autre exemple récent illustre le propos : le 20 mars 2018, une voiture autonome d'une société de VTC a renversé et tué un piéton traversant devant la voiture. La société a immédiatement stoppé les tests de ses voitures autonomes afin de déterminer les causes de cet accident. Il semblerait[8] que celles-ci aient été identifiées et qu'elles soient intégralement imputables au logiciel pilotant la voiture. Les capteurs de la voiture auraient parfaitement bien détecté le piéton traversant la rue, mais le système de conduite aurait délibérément choisi de considérer cela comme un faux positif, et aurait donc décidé de ne pas réagir.

7 https://spectrum.ieee.org/cars-that-think/transportation/sensors/slight-street-sign-modifications-can-fool-machine-learning-algorithms

8 https://www.theinformation.com/articles/uber-finds-deadly-accident-likely-caused-by-software-set-to-ignore-objects-on-road

LA CONSTRUCTION D'UN MODÈLE D'INTELLIGENCE ARTIFICIELLE DURABLE, À L'ÉCHELLE NATIONALE, EUROPÉENNE ET INTERNATIONALE, SUPPOSE UNE RÉFLEXION ÉTHIQUE

Les initiatives sur l'« éthique de l'intelligence artificielle » se sont multipliées cette année. Dans son rapport de décembre 2017, la CNIL avait recensé les questions éthiques les plus fondamentales posées par les algorithmes de nouvelle génération : déresponsabilisation et perte d'autonomie de l'Homme face à des outils techniques gagnant en sophistication ; enfermement algorithmique et discriminations ; hyper-personnalisation susceptible d'affecter des logiques collectives essentielles à la vie de nos sociétés (préservation d'un espace public pluriel, atteinte à la logique de mutualisation dans le champ de l'assurance). Le débat public avait donc mis en lumière certains enjeux sociétaux.

À l'échelle française, dans le sillage des conclusions de la mission du député Cédric Villani présentée en mars 2018, le Gouvernement français a identifié l'éthique comme une priorité dans sa stratégie pour une intelligence artificielle humaniste. La CNIL se félicite de la prise en compte de ces questions.

À l'échelle européenne, l'année 2018 a été celle de l'entrée en application du RGPD. La CNIL est convaincue que cette réponse régulatoire met en place, autant pour les individus que pour les entreprises, un cadre de confiance sur les données personnelles qui sont au cœur des outils d'intelligence artificielle.

Pour les individus, le règlement répond à la crise de confiance en encadrant les conditions de la collecte des données personnelles alimentant ces algorithmes, en renforçant les obligations de transparence, et en reconnaissant des droits aux personnes de contester une décision automatique qui les affecte significativement. Pour les entreprises et autres acteurs de l'écosystème de l'intelligence artificielle, il offre un cadre suffisamment ouvert pour soutenir une recherche et une politique industrielle ambitieuse en la matière. Le RGPD offre en effet, d'une part, la possibilité de constituer de larges entrepôts de données et, d'autre part, une certaine flexibilité quant aux finalités d'utilisation desdites données. Le RGPD pose donc les jalons d'une innovation numérique pérenne, et constitue une base solide pour le développement futur de l'intelligence artificielle en Europe.

L'intelligence artificielle pose toutefois des enjeux plus larges. C'est la raison pour laquelle l'Europe entend compléter sa réponse sur ces sujets. La Commission européenne a notamment constitué un groupe d'experts de haut niveau sur le sujet, qui publiera en 2019 des lignes directrices pour le développement éthique de l'intelligence artificielle. La CNIL participe aux réunions du groupe en tant qu'observateur.

Enfin, sur le plan international, dans le cadre de sa présidence de la Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC), la CNIL a participé à l'adoption d'une déclaration sur l'éthique et la protection des données dans l'intelligence artificielle[9]. Par ce texte, les autorités de protection de données du monde entier sont parvenues à une position commune pour un cadre juridico-éthique à la hauteur de cette révolution. Les deux principes proposés par la CNIL en décembre 2017, la loyauté et la vigilance, ont été repris et adoptés à l'unanimité par les membres du réseau.

9 https://icdppc.org/wp-content/uploads/2018/10/20181023_ICDPPC-Declaration-AI_Adopted-FR.pdf

Bilan d'activité

INFORMER
le grand public

La CNIL 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. Elle est également présente dans la presse, sur internet, sur les réseaux sociaux où elle met à disposition des outils pédagogiques et pratiques adaptés aux publics variés auxquels elle s'adresse. La CNIL a été très sollicitée en 2018, notamment par les professionnels, à l'occasion de l'entrée en application du Règlement général sur la protection des données (RGPD). Le record de demandes reçues témoigne de l'intérêt des professionnels et de la sensibilité croissante des particuliers mais aussi du fait qu'ils identifient la CNIL comme une source de référence.

Samuel
Animateur de communautés (community manager)

La CNIL a décidé dès 2010 d'être présente sur les réseaux sociaux pour être au plus près des usages numériques et se rapprocher des communautés qui partagent le même intérêt pour la protection des données et de la vie privée. Sur Facebook, nous parlons à des prescripteurs du quotidien, souvent des parents/enseignants en recherche d'informations sur la bonne « hygiène numérique » ou des citoyens qui rencontrent des problèmes liés à leurs données personnelles. Sur Twitter, ce sont les influenceurs - souvent technophiles - avec lesquels nous pouvons entrer en contact ou dialoguer. Sur LinkedIN, ce sont des experts, le plus souvent des délégués à la protection des données ou RSSI qui se font « les ambassadeurs » de nos messages auprès de leur réseau professionnel. Sur ce dernier réseau, nos statistiques d'engagement démontrent chaque jour que le RGPD a décuplé l'intérêt des professionnels pour la protection des données.

Si la CNIL est souvent citée ou interpellée, nous sommes loin d'avoir réponse à tout ! En revanche nous traitons en lien avec l'ensemble des services internes de la CNIL la plupart des retours pertinents - parfois sans langue de bois - des utilisateurs. Le rôle de l'animateur de communautés est d'utiliser cette matière pour construire quelque chose de positif, soit en répondant aux problèmes rencontrés par les citoyens, soit en créant un contenu d'information sur cnil.fr qui pourrait profiter à d'autres usagers. Ainsi, des 1 500 messages privés/publics auxquels nous répondons naissent des dizaines de contenus de sensibilisation tels que des fiches pratiques, des infographies, vidéos, visuels et autres threads Twitter (fils de messages).

8 098 232

visiteurs sur cnil.fr en 2018

+80%

de visiteurs par rapport à 2017

89

actualités et communiqués publiés en 2018

LE RGPD, UN EFFET SANS PRÉCÉDENT SUR CNIL.FR ET LES RÉSEAUX SOCIAUX

Le site de la CNIL

Le RGPD a eu un effet sans précédent sur le site de la CNIL. En effet, le nombre de visiteurs a pratiquement doublé en une année pour passer à plus de **8 millions en 2018, contre 4,4 millions en 2017, qui représentait déjà une augmentation de l'audience de 59 %.** La majorité des internautes visitent les contenus et outils pratiques sur le RGPD.

Le menu professionnel a été refondu pour appréhender « pas à pas » le RGPD, en fonction de ses besoins et savoir comment passer à l'action pour se mettre en conformité grâce à l'onglet « Ma conformité au RGPD ». De nouveaux téléservices ont été créés tels que la désignation du DPO ou de l'autorité chef de file, la notification de violation de données et l'envoi de l'AIPD. Des outils pratiques, comme un modèle de registre simplifié ou des exemples de mentions d'information ont été proposés ainsi que des mises à jour régulières de l'outil PIA. Enfin, un certain nombre de contenus existants ont également été mis à jour.

4 consultations en ligne ont été publiées, avant l'adoption de référentiels ou d'un règlement type. Ces consultations seront systématiques avant l'adoption de nouveaux cadres de référence.

2 premiers bilans du RGPD (4 mois et 6 mois après le 25 mai) ont été publiés permettant de faire le point sur les contenus et outils existants ainsi que sur les initiatives à venir.

TOP 10 des contenus RGPD

- RGPD : se préparer en 6 étapes (888 604 vues)
- Règlement européen sur la protection des données : ce qui change pour les professionnels (377 630 vues)
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (389 363 vues)
- Cartographier vos traitements de données personnelles (275 130 vues)
- Outil PIA : téléchargez et installez le logiciel de la CNIL (284 989 vues)
- RGPD : par où commencer (249 250 vues)
- RGPD : exemples de mentions d'information (270 457 vues)
- Le registre des activités de traitement (204 600)
- RGPD : comment la CNIL vous accompagne dans cette période transitoire ? (148 407 vues)
- RGPD : passer à l'action (185 661 vues)

Exemple de registre

Guide pratique pour les TPE/PME

Se préparer en 6 étapes au RGPD

Les réseaux sociaux

Environ 215 000 comptes suivent la CNIL de près ou de loin sur les réseaux sociaux. En 12 mois, l'audience de la page LinkedIN de la CNIL a été multipliée par trois. Les publications qui génèrent le plus d'engagement des professionnels sont celles relatives à la compréhension des principes du RGPD mais aussi aux outils de conformité (logiciel AIPD, guide PME-TPE, fiches *etc.*). Sur Facebook, la sensibilisation contre les arnaques en ligne ou contre les fake news sur le thème des données et les astuces pour protéger ses données sont les contenus les plus populaires. Sur Twitter, l'explication en « thread » et le recours aux infographies est l'occasion d'offrir un niveau de lecture plus accessible aux communautés plus éloignées du thème du numérique.

Nombre de followers sur Twitter au 12 mars 2019

108 000
@CNIL

2500
@Educnum

4000
@LinCNIL

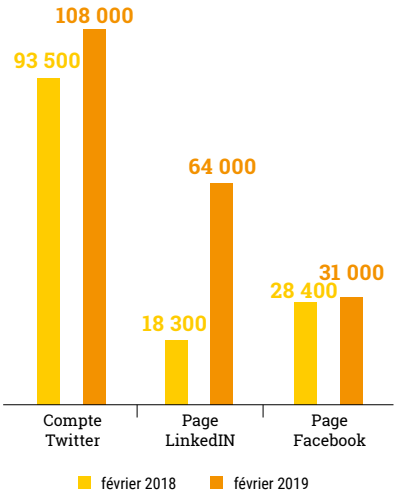
2800
@CNIL_en

31 000
fans CNIL

2 100
fans Educnum

64 000
abonnés sur LinkedIN

Évolution de l'audience des principaux comptes de la CNIL (nombre d'abonnés)

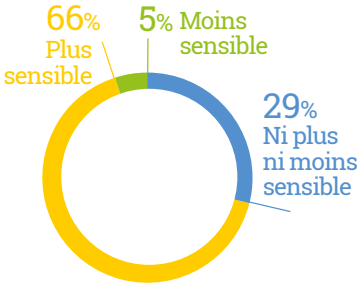


UNE SENSIBILITÉ DES FRANÇAIS EN NETTE AUGMENTATION

Selon un sondage IFOP[1] réalisé en octobre pour la CNIL, **66 % des Français se disent plus sensibles que ces dernières années à la protection de leurs données personnelles**. Cette hausse de la sensibilité s'explique principalement par des facteurs anxiogènes exprimés par les personnes interrogées : la peur du piratage ou du vol de données et les scandales de piratages sur les réseaux sociaux. Les spam et les sollicitations commerciales émergent également dans les principaux motifs de cette sensibilisation accrue.

Face à ces inquiétudes, **la connaissance du RGPD apparaît globalement bonne,** 65 % des Français en ayant déjà entendu parler. Néanmoins, seule une courte majorité (54 %) estime à ce stade comprendre ce que le RGPD a changé sur les droits des personnes et les obligations des professionnels. Une fois mieux informés sur ce règlement, les Français portent un regard largement positif sur celui-ci, puisque 73 % considèrent qu'il est efficace pour mieux protéger les données personnelles.

Diriez-vous que vous êtes aujourd'hui plus, moins ou ni plus ni moins sensible à la question de la protection de vos données personnelles qu'au cours de ces dernières années ?

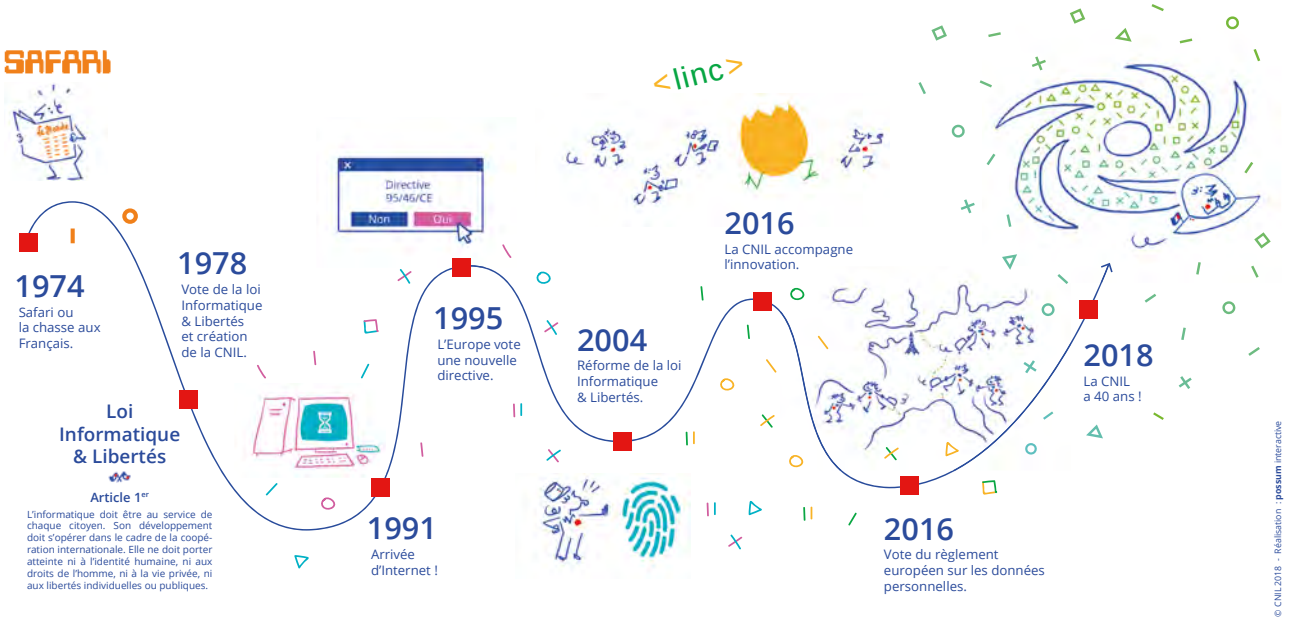


46 % des personnes interrogées ont déjà constaté des abus sur l'utilisation de leurs données personnelles. Et parmi celles-ci, 16 % ont signalé ces abus.

Le passage de cette attitude positive à des comportements réellement actifs de la part des associations et de la CNIL, nécessite un travail d'accompagnement, de formation et de pédagogie concernant des outils existants dont les Français, s'ils les connaissent, ont encore une idée trop approximative de la manière dont ils peuvent s'en saisir.

1 Sondage réalisé en ligne, du 30 au 31 octobre, auprès d'un échantillon de 1003 personnes, représentatif de la population française âgée de 18 ans et plus.

1978-2018 : 40 ANS, PLUS QUE JAMAIS DANS L'AIR DU TEMPS



À l'occasion de son quarantième anniversaire, la CNIL a conçu une courte vidéo de 3 minutes pour revisiter son histoire et proposer un condensé de 40 ans de protection des données. Une sélection d'archives télévisuelles conçue par l'INA retrace également l'action de la CNIL et les grands sujets qui ont marqué son histoire.

Le dessinateur de presse Plantu a réalisé spécialement pour cette occasion un dessin.

Le journal le MONDE, à l'initiative de la révélation, en 1974, de l'affaire Safari, a publié un cahier spécial. Safari ou la chasse au Français, publié dans le


Le Monde

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

« Safari » ou la chasse aux Français

Monde en mars 1974 est l'article qui a révélé au grand public le projet SAFARI. Celui-ci qui prévoyait d'identifier chaque citoyen par un numéro et d'interconnecter sur la base de cet identifiant tous les fichiers de l'administration.

À la suite de cette affaire, une commission parlementaire est alors chargée de réfléchir à une réglementation pour garantir le respect de la vie privée face au développement de l'informatique. C'est ainsi que naîtra le 6 janvier 1978, la loi Informatique et Libertés qui créera la CNIL.

LES RÉPONSES AU PUBLIC

Le service des relations avec les publics (SRP) informe et conseille les particuliers et les professionnels désireux d'obtenir un renseignement juridique ou une aide à l'accomplissement des démarches auprès de la CNIL. On peut le contacter 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 2018, l'impact du RGPD sur le volume d'activité du service a été puissant. Dès le premier trimestre 2018, le nombre des sollicitations a augmenté de manière significative pour atteindre sur certaines périodes des chiffres inédits (+ de 25 000 appels pour le seul mois de mai). Les responsables de traitement, en particulier les petites et moyennes entreprises, désireux de se conformer à la nouvelle réglementation souhaitent de plus en plus être accompagnés et rassurés, en raison notamment du renforcement des pouvoirs de sanction de la CNIL. Au dernier trimestre 2018, la CNIL a reçu de nombreuses demandes de particuliers désireux d'exercer leurs droits (droits d'accès, d'opposition, droit à la portabilité) et d'obtenir des conseils pour faire aboutir leur demande.

Les usagers s'adressent prioritairement à la CNIL par voie électronique via le service « Besoin d'aide », disponible 24h/24. L'augmentation du nombre des requêtes effectuées en ligne est constante (en moyenne + 15 % chaque année). L'effet RGPD est également incontestable si l'on se réfère au nombre de consultations des Questions/Réponses proposée par ce même service « Besoin d'aide » (+ 59 % cette année).

Un important travail de mise à jour des Questions/Réponses du service en ligne « Besoin d'aide » a été réalisé : certaines ont été supprimées, d'autres actualisées et de nombreuses questions ont été créées pour répondre aux préoccupations concrètes des usagers et les sensibiliser à la nouvelle règlementation relative à la protection des données (voir les 10 questions les plus consultées).

Si, à l'approche de l'entrée en application du RGPD, la majorité des questions a porté sur la nécessité ou pas d'effectuer des formalités auprès de la CNIL, les problématiques ont évolué depuis et deviennent de plus en plus complexes. À titre d'exemple, la CNIL est régulièrement interrogée sur les paramétrages des cookies, la conformité de logiciels au RGPD, l'interprétation de certaines dispositions du RGPD (base légale, consentement, modalités d'information des personnes, *etc.*), sans oublier tout ce qui a trait aux modalités concrètes d'exercice du droit des personnes.

189 877

appels reçus au 01 53 73 22 22
(+ 22 % par rapport à 2017)

283 742

consultations des Questions/Réponses en forte hausse (+ 59 %)

71 410

appels pour la permanence téléphonique
(+ 6 % par rapport à 2017)

16 877

requêtes reçues par voie électronique
(+ 15 % par rapport à 2017)

INFOSPLUS

Le service Besoin d'aide ? en 2018

500 Questions/Réponses publiées dont 38 sur le RGPD

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

- Que vont devenir les dispenses, normes simplifiées et autorisations uniques de la CNIL?
- Quelles formalités pour les transferts hors UE ?
- C'est quoi un « conflit d'intérêts » pour un délégué à la protection des données ?
- Le consentement est-il obligatoire ?
- Une analyse d'impact sur la protection des données, c'est quoi ?
- Le délégué à la protection des données, c'est obligatoire ?
- Que devient la Loi Informatique et Libertés avec l'entrée en application du RGPD ?
- Le registre des traitements doit-il être rendu public ?
- Le délégué à la protection des données peut-il être une personne morale ?
- Un « traitement à grande échelle », c'est quoi ?

INFOSPLUS

Pratiques abusives « Mise en conformité RGPD »

Des sociétés se prétendant mandatées par les pouvoirs publics ont profité de l'entrée en vigueur du RGPD pour opérer du démarchage auprès des professionnels, parfois de manière agressive, afin de vendre un service d'aide à la mise en conformité au règlement. La CNIL, et la Direction Générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF) ont diffusé, à l'attention des professionnels, des recommandations sur la conduite à tenir en cas de démarchage.

Un guide pratique à destination des TPE PME élaboré avec Bpifrance

En avril 2018, la CNIL s'est associée à Bpifrance pour produire un guide pratique à destination des quelques 4 millions de TPE et PME françaises. Ce guide s'attache à simplifier la compréhension du RGPD et, ainsi, à faciliter la mise en conformité de ces entreprises. Il reprend sous forme de fiches pratiques les principales étapes à respecter pour monter en maturité sur la question de la protection des données, tout en adaptant les moyens déployés à la sensibilité et au volume des données personnelles traitées au sein de chaque entreprise.

Afin de mettre en application ces principes s'agissant des traitements les plus courants, le guide est complété par des fiches pratiques sur le traitement des données des salariés, des clients ou plus généralement nécessaires à la communication externe de l'entreprise.

Les TPE et PME ne disposant pas de personnes spécialisées dans la protection des données peuvent ainsi s'appuyer sur un vadémécum de réflexes et bonnes pratiques permettant de partir du bon pied pour s'approprier le RGPD. En fixant des objectifs clairs, ce guide aide les entrepreneurs à progresser dans la maîtrise et la valorisation de leur patrimoine informationnel, tout en renforçant la confiance de leurs clients et partenaires. Il s'inscrit dans la volonté constante de la CNIL d'accompagner les entreprises vers une meilleure maîtrise de leurs données, par la prise en compte des principes du RGPD, de manière à transformer cet exercice en avantage concurrentiel pour les acteurs économiques impliqués.

À suivre... un plan de sensibilisation à destination des collectivités

En 2019, la CNIL développera de nombreuses actions de sensibilisation à destination des collectivités territoriales et tout particulièrement des petites communes. Elle proposera au premier semestre un guide pratique, une rubrique dédiée sur son site avec des fiches thématiques permettant d'aller plus loin dans sa conformité et elle poursuivra ses échanges avec les têtes de réseau et les associations telles que l'ADF, l'AMRF, l'AMF, *etc.*

DES ACTIONS D'ÉDUCATION AU NUMÉRIQUE VERS TOUS LES PUBLICS

En 2018 la CNIL s'est appuyée sur de nombreux partenaires relais nationaux pour développer ses actions de sensibilisation et démultiplier ses messages vers tous types de publics. Au plan international, les travaux de la CNIL et de ses homologues ont, cette année, été consacrés aux enjeux soulevés par les plateformes éducatives en ligne. L'expertise de la CNIL a été aussi sollicitée dans le cadre des groupes de travail de l'OCDE, de la Commission européenne et du Conseil de l'Europe portant notamment sur l'apprentissage de la citoyenneté numérique.

Un partenariat structurant avec le ministère de l'Éducation nationale et de la Jeunesse

Dans le prolongement des actions de collaboration engagées depuis 2016, la CNIL et le ministère de l'Éducation nationale et de la Jeunesse ont signé en décembre 2018 une nouvelle convention « portant sur l'intégration de la protection des données personnelles dans les usages numériques de l'éducation ». Celle-ci prévoit notamment l'accompagnement du ministère à sa mise en conformité au RGPD.

Le référentiel international de formation des élèves à la protection des données personnelles conçu par la CNIL et adopté en 2016 a fait l'objet d'une première déclinaison en France. À l'occasion de la mise en application du RGPD le 25 mai 2018, un premier module destiné au cycle 3 (8-11 ans) a été mis en ligne sur le portail eduscol. Des cas pratiques de classe et des ressources pédagogiques incarnent ce module pour donner envie aux enseignants de parler de protection des données à l'école.

La CNIL a participé au lancement de la 3e édition des Trophées des classes initiée par le ministère, aux côtés de Radio France. En 2019, les établissements scolaires du cycle 3 pourront participer au concours en proposant une ressource numérique portant sur le thème « Les données personnelles, ça compte. Protégeons-les ! ».

Les formations de formateurs, un levier efficace pour toucher les publics au plus près des territoires

Tout au long de l'année 2018, la CNIL a formé des jeunes en service civique de l'association e-Enfance et de la Défenseure des enfants, qui ont par la suite sensibilisé 150 000 jeunes au sujet de la protection des données personnelles. Les animateurs des clubs de football professionnels et des pôles Espoirs ont suivi à la CNIL un atelier interactif sur les réseaux sociaux, qui a ensuite été déployé auprès des jeunes joueurs. En 2019, ce dispositif sera étendu aux animateurs de l'association Génération Numérique. Des ressources ont été mises à disposition des Voyageurs du numérique, programme initié par l'association Bibliothèques sans frontières, afin de toucher les publics en difficulté avec le numérique.

La CNIL et le Défenseur des Droits ont participé à l'opération Educapcity, une course citoyenne pour sensibiliser les jeunes de 9 à 15 ans aux enjeux de la citoyenneté. Les enfants ont testé leurs connaissances en matière d'éducation au numérique en répondant à des questions extraites du quiz Les incollables « Ta vie privée, c'est secret ! ».

La CNIL a participé au Forum sur la gouvernance de l'Internet (IGF) à l'UNESCO. Présente dans des ateliers, elle a valorisé sur son stand des publications clés sur ses activités en matière d'innovation, d'intelligence artificielle, d'éducation au numérique et autres ressources qui, au-delà de son action de régulation, contribuent aux débats sur les enjeux reliant éthique, libertés, données et usages du numérique.

Des actions en synergie avec le collectif educnum

En 2018, la CNIL a participé activement au salon Educatice : participation à une conférence sur le RGPD pour la communauté éducative, animation d'un atelier pour des enseignants autour du référentiel de formation des élèves au sein du Carrefour pédagogique, réponse aux nombreuses questions des enseignants, associations et parents sur le stand de la CNIL, où des membres du collectif sont venus présenter leurs ressources et actions en matière d'éducation au numérique.

Le collectif a contribué à la consultation menée par le conseil national du numérique dans le cadre des États généraux des nouvelles régulations numériques, en publiant une contribution « Pour un numérique plus inclusif » à l'attention des pouvoirs publics. Les propositions opérationnelles ont été adressés au secrétaire d'État au numérique.

La CNIL et les membres du collectif ont travaillé ensemble sur de nouvelles ressources pédagogiques à destination des familles : Guide de la Famille tout-écran avec le Clemi, affiche sur les réseaux sociaux avec Génération Numérique et Radio France, *etc.* Ces ressources sont valorisées sur le site www.educnum.fr

Des initiatives coordonnées à l'international

À l'échelle internationale, la CNIL a organisé la mise en commun de plans de cours « clés en main » enrichis avec des cas pratiques variés et des ressources ciblées par niveau de classes (primaire, secondaire) pour décliner le référentiel de formation des élèves et faciliter son insertion dans les programmes scolaires.

Elle a co-rédigé avec l'autorité fédérale du Canada et l'autorité de l'Ontario, une résolution sur les services de plateformes éducatives en ligne, adoptée par la Conférence internationale des autorités de protection des données en octobre 2018. Sa mise en œuvre pourrait se traduire par l'adoption de codes de conduite nationaux garantissant le développement de services numériques à l'école, respectueux de la protection des données scolaires.

Enfin, la CNIL a contribué à des programmes et campagnes éducatives lancées par la Commission Européenne et le Conseil de l'Europe pour sensibiliser les mineurs à la protection de leurs données personnelles et à leurs droits dans l'univers numérique.

L'initiative Cyber Chronix à laquelle la CNIL s'est associée avec le Centre de Recherche JRC – l'Unité cyber sécurité de la Commission Européenne- propose un outil ludo-éducatif destiné à sensibiliser les jeunes aux enjeux et aux droits à la protection de leurs données, lancé le 25 mai 2018 dans le cadre du nouveau RGPD. Des liens vers des ressources pédagogiques en français sur les thématiques du RGPD destinées aux éducateurs comme aux élèves ont été mis en ligne avec la CNIL.

L'Unité protection des données et la

Division des droits des enfants du Conseil de l'Europe ont lancé en 2018 un travail réunissant des experts internationaux et des représentants des autorités de protection des données française et belge. L'objectif est d'offrir aux autorités de protection des données une «boîte à outils» pour sensibiliser les enfants et les jeunes à la protection de leur vie privée et de leurs données personnelles. La «Boîte à outils» envisagée pour 2019 déclinera, à destination des mineurs, en termes pratiques et dans des formats adaptés, les principes consacrés par la Convention 108+ du Conseil de l'Europe, avec l'aide des lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique publiées en juillet 2018 ainsi que des multiples expériences et réalisations existantes provenant des autorités de protection des données.

PROTÉGER
les citoyens

La CNIL a reçu un nombre record de plaintes en 2018, avec 11 070 plaintes reçues.
Le plus souvent, la CNIL intervient auprès du responsable du fichier pour l'informer des manquements soulevés 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. Les plaintes concernant des cas transfrontaliers font l'objet d'une coopération européenne entre les autorités de protection des données. Enfin, la CNIL a reçu des plaintes collectives concernant plusieurs milliers de personnes.

Guillaume
Juriste au service des plaintes

Le secteur « régalien » du service des plaintes, traite les réclamations concernant des fichiers utilisés par les ministères de la Justice, de l'Intérieur, de la Défense, des Affaires étrangères ou de l'Économie et des finances.
Je traite aussi les réclamations concernant les collectivités territoriales, au titre des missions qu'elles exercent pour le compte de l'État (tenue de l'état civil, des listes électorales, recensement de la population…) ou en propre. Il s'agit chaque fois d'assurer la conciliation du cadre juridique de la protection des données avec les multiples textes qu'elles doivent également respecter, ce qui permet, par la découverte quotidienne d'autres textes, de renouveler l'intérêt de mon métier.
Dans ces deux domaines, le mouvement dit des « données ouvertes » a des conséquences pratiques immédiates (accès aux décisions de justice et donc à l'identité des acteurs du procès, diffusion des délibérations des collectivités ou des réactions aux enquêtes publiques) qui impose de trouver un équilibre entre volonté de transparence et protection de la vie privée, tout en aboutissant à une application pragmatique du droit.
Je suis également en charge de réclamations relatives à l'exercice des libertés publiques (association, fichiers des églises et groupements à caractère religieux, fichiers des partis politiques, articles de presse en ligne, etc.), qui touchent bien souvent à l'intimité de l'être des personnes.
À ce titre, je m'occupe aussi de réclamations pour refus de déréférencement opposés par les moteurs de recherche, notamment en matière de presse en ligne. Ces demandes impliquent de trouver un équilibre entre la protection des données et d'autres libertés fondamentales, selon les critères définis par les juridictions nationales et européennes.

2018 : UN NOMBRE RECORD DE PLAINTES SUITE À « L'EFFET RGPD »

L'entrée en application du RGPD a marqué une prise de conscience inédite des enjeux de protection des données. Cela s'est logiquement traduit par une hausse considérable des plaintes adressées à la CNIL. Un nouveau record du nombre de plaintes reçues a ainsi été atteint.

1 767 plaintes (+ 11,8) ont fait l'objet d'un traitement rapide par le service des relations avec les publics. Les personnes reçoivent ainsi des réponses sur :

- Leurs droits Informatique et Libertés et leurs modalités d'exercice ;
- Les obligations des responsables de fichiers ;
- Les autres administrations susceptibles de leur venir en aide au regard de leur demande.

9 310 plaintes plus complexes (+ 37,3 %) ont été orientées vers le service des plaintes qui intervient auprès du responsable du fichier mis en cause, par écrit, pour l'interroger sur les conditions de mise en œuvre de son traitement de données, lui rappeler ses obligations et demander le respect des droits des personnes. Ces plaintes peuvent également donner lieu à un contrôle sur place et / ou à une mesure correctrice (mise en demeure, injonction, sanction pécuniaire *etc.*).

Lorsque les traitements de données personnelles sont transfrontaliers au sein de l'Union Européenne, les plaintes sont désormais traitées en coopération avec les autorités de protection de données des autres pays concernés.
Pour exercer ses droits, la personne doit d'abord s'adresser au responsable du traitement, ou à son délégué à la protection des données (DPO) s'il y en a. Ce n'est qu'en cas de refus ou d'absence de réponse dans un délai d'un mois que la CNIL peut intervenir.
Avec l'entrée en application du RGPD, la CNIL a constaté la mise en ligne de plus en plus fréquente par les administrations et les entreprises de « Politique de protection des données », « Politique de confidentialité » ou autre *Privacy Policy*. La CNIL conseille aux responsables de fichiers de bien traiter les demandes des personnes qui exerceraient leurs droits sans recourir aux modalités prévues (ex : adresse électronique dédiée aux droits). Elle appelle également les particuliers à prendre connaissance de manière plus systématique des informations délivrées par les organismes, notamment sur leur site internet.

- **35,7 % des plaintes concernent la diffusion de données sur internet**

La suppression de ses données (nom, prénom, coordonnées, commentaires, photographies, vidéos, comptes, *etc.*) sur internet restent le premier sujet de plainte, traduisant le souci des per-

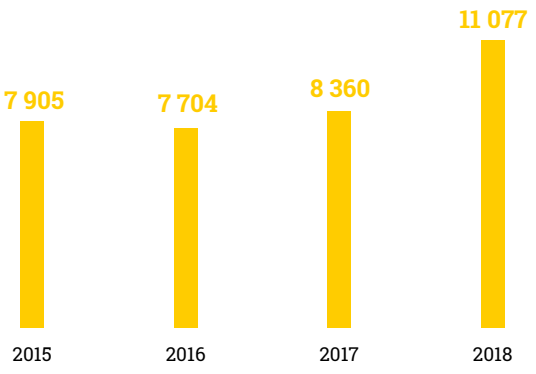
Histoires vécues...

INTERNET / COMMERCE

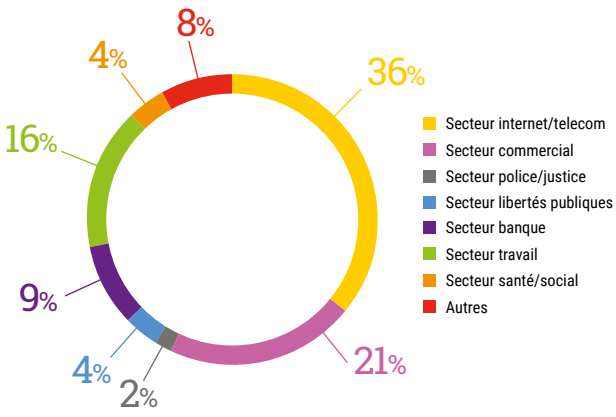
MONSIEUR M., se rend en magasin pour retirer son colis après une commande en ligne. Il présente une pièce d'identité, qui est scannée par l'agent d'accueil. Monsieur M. demande la destruction de cette copie numérique, ce que le salarié refuse, arguant des consignes strictes de sa hiérarchie. La CNIL est intervenue pour rappeler que la simple consultation du titre d'identité suffit. L'enseigne a donc modifié ses pratiques, ne réalise plus de copie des pièces d'identité et a diffusé les nouvelles directives dans ses magasins. Les copies de pièces d'identité réalisées ont été supprimées.

MADAME B., saisonnière dans un établissement de tourisme, voit des photos d'elle publiées sur le site internet et la page Facebook de l'établissement. Elle en demande sans succès la suppression. Après intervention de la CNIL, qui a rappelé que les personnes doivent consentir à la publication de leur photographie sur internet, l'établissement a supprimé ces images.

Évolution du nombre de plaintes depuis 2015



Répartition des plaintes par secteur d'activité (2018)



sonnes de maîtriser leur vie numérique, et notamment leur réputation en ligne.
En 2018, la CNIL a notamment reçu **373 plaintes relatives au déréférencement (+ 11,3 %)**.

Ce droit, désormais consacré par le RGPD, permet de demander à un moteur de recherche de supprimer certains résultats de recherche associés à ses nom et prénom. En cas de refus, la CNIL saisie par un particulier, fera la balance entre les intérêts du public à avoir accès au contenu via les moteurs de recherche et les droits fondamentaux de la personne. 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.
Par ailleurs, plusieurs centaines de plaintes ont été reçues contre l'association belge « EU Disinfolab » à l'occasion de son étude portant sur les tweets concernant « l'affaire Benalla ». Ces plaintes sont traitées, dans le cadre du mécanisme de coopération introduit par le RGPD, par l'autorité belge de protection des données.

Vidéosurveillance au travail : la CNIL interpelle la ministre du Travail

La vidéosurveillance est l'outil dont l'usage est le plus contesté par les employés qui saisissent la CNIL. Ces plaintes ont notamment conduit la CNIL à adresser un courrier à la ministre du Travail en décembre 2018 l'alertant sur les risques qu'induisent le visionnage à distance des images issues de caméras de surveillance (via le smartphone de l'employeur) et le développement de l'enregistrement du son associé aux images.

En effet, ces pratiques, en cas de mésusage, peuvent conduire à placer les personnes sous une surveillance permanente considérée comme disproportionnée au regard des règles de protection des données personnelles mais aussi potentiellement constitutive de harcèlement moral.
La CNIL appelle ainsi à une adaptation de la réponse publique à ce phénomène au regard des enjeux en matière de santé mentale des travailleurs.

- **21 % des plaintes concernent le secteur commerce/marketing**

La CNIL a constaté une très forte hausse des plaintes concernant la prospection par SMS. Les personnes se plaignent de recevoir des sollicitations sans que leur consentement préalable n'ait été recueilli et que l'envoi de « STOP » à l'expéditeur fasse cesser la réception de publicités. La publicité par courrier électronique reste une source importante de plaintes. Le travail mené par la CNIL en lien avec l'association « Signal Spam » devra porter ses fruits dans les mois à venir, notamment en raison des nouveaux pouvoirs de la CNIL créés par le RGPD et la nouvelle loi Informatique et Libertés.

Au-delà de la réception de publicités, les plaintes portent également sur la conservation des données bancaires des consommateurs, la mauvaise gestion des mots de passe lors de la création de comptes en ligne ou la suppression de données après la fin de la relation contractuelle.

Enfin, les plaintes concernant le compteur d'électricité Linky ont encore été nombreuses en 2018. La CNIL reste vigilante sur ce dossier.

- **16,5 % des plaintes concernent le secteur Travail**

La surveillance technologique (vidéosurveillance, géolocalisation, cybersurveillance) constitue toujours un facteur d'inquiétude pour les salariés des secteurs privé et public. Le nombre de plaintes reçues reste élevé.

- **8,9 % des plaintes concernent le secteur Banque/Crédit**

Plus de 500 plaintes concernent l'inscription des personnes dans les fichiers d'incidents de la Banque de France (FICP et FCC). La CNIL constate une méconnaissance et une incompréhension des personnes quant aux objectifs de ces fichiers et aux rôles respectifs des établissements financiers, de la Banque de France et de la CNIL. Un nombre important de personnes se plaignent du maintien de leur inscription, indiquant avoir pourtant régularisé leur situation auprès de l'établissement concerné. Les difficultés dans l'exercice du droit d'accès ont également généré près de 200 plaintes.

- **4,2 % des plaintes concernent le secteur Santé/Social**

Les personnes rencontrent des difficultés pour obtenir l'accès à leur dossier personnel (dossier médical, dossier CAF, Pôle emploi, *etc.*). Depuis la sanction de 10 000 € prononcée en 2017 à l'encontre d'un professionnel de santé, une amélioration des pratiques est perceptible puisque le nombre de plaintes relatives au droit d'accès au dossier médical a baissé de près de 30 % par rapport à 2017. Les questions de sécurité, et plus particulièrement de confidentialité, ont été plus importantes en 2018 (+100 %) dans ce secteur, démontrant une préoccupation nouvelle des plaignants à ce sujet.

- **3,7 % des plaintes concernent le secteur Libertés publiques/ Collectivités**

Les plaintes mettent en cause principalement les dispositifs de vidéoprotection de la voie publique et la collecte excessive de données personnelles dans le cadre de démarches administratives (par exemple, pour l'accès aux déchetteries ou l'inscription de son enfant à des activités).

En 2018, la CNIL a également reçu près d'une centaine de plaintes relatives à des demandes d'effacement de contenus concernant des articles de presse publiés en ligne (retrait de l'article, anonymisation, désindexation).

Histoire vécue...

BANQUE

M. Y, est inscrit au Fichier national des Incidents de remboursement des Crédits aux Particuliers (FICP) alors qu'il avait remboursé son prêt par anticipation par chèque. Grâce à l'intervention de la CNIL, l'établissement de crédit a fait procéder à la levée de l'inscription de M.Y dans ce fichier, reconnaissant qu'elle résultait d'une erreur dans la prise en compte de son remboursement anticipé de prêt, qui avait été « mal interprété ».

Histoire vécue...

BANQUE

Trois prélèvements sur le compte bancaire de Mme P. sont rejetés faute de provision suffisante sur son compte. Mme P. est inscrite au Fichier Central des Chèques (FCC) et doit restituer sa carte bancaire à sa banque. Après intervention de la CNIL, la banque a fait procéder à la levée de l'inscription injustifiée de Mme P. La CNIL a rappelé à la banque que l'inscription d'un client au FCC pour utilisation abusive de sa carte bancaire ne peut être effectuée que si l'utilisation de la carte bancaire est à l'origine du découvert ou si elle a été utilisée alors que le compte était déjà à découvert.

Histoires vécues...

TRAVAIL/SOCIAL/SANTÉ

L'EMPLOYEUR DE M. F., chauffeur dans une société de transport, demande à ses employés une copie de leur permis de conduire dans le cadre de la gestion des contraventions au code de la route qu'il reçoit. L'intervention de la CNIL a conduit la société à mettre à jour les dossiers du personnel afin de ne pas conserver une copie des permis de conduire. En effet, la conservation d'une telle copie est excessive et non pertinente, y compris dans le cadre du recouvrement des contraventions au code de la route. L'employeur peut en revanche demander à ses employés de présenter ponctuellement leur permis de conduire.

MONSIEUR P., signale à la CNIL un questionnaire mis en ligne par une association, concernant des mineurs, sans garantie d'anonymat. La CNIL a rappelé à l'organisme que son questionnaire pouvait être anonyme en supprimant la collecte de la date de naissance, du sexe, du code postal et de la situation scolaire ou professionnelle des personnes concernées, tout en permettant d'atteindre l'objectif poursuivi qui était de mieux connaître les attentes d'une partie de la population sur un territoire donné. En réponse, le questionnaire a été suspendu le temps de le corriger.

FOCUS

La coopération européenne sur les plaintes

Les autorités de protection des données de l'UE doivent coopérer lorsqu'elles examinent des traitements « transfrontaliers », c'est-à-dire ayant lieu dans le cadre des activités d'entreprises établies dans plusieurs États membres ou dont les activités affectent des personnes résidant dans plusieurs pays européens. Cette coopération s'inscrit dans le cadre du mécanisme dit du « guichet unique » lorsque l'organisme dispose d'un établissement principal dans l'UE. Le RGPD prévoit que l'organisme a pour unique interlocutrice l'autorité de protection des données du pays dans lequel est situé son établissement principal, appelée autorité « chef de file ». Les autorités se déclarent « concernées » par un cas si leurs ressortissants peuvent se trouver affectés par le traitement. Elles sont informées par l'autorité « chef de file » des suites données à une ou plusieurs plaintes et donnent un avis sur le projet de décision de la chef de file. En cas de désaccord, une décision s'imposant à toutes les autorités pourra être prise par le Comité européen à la protection des données, qui remplace l'ancien groupe de travail « G29 ». Afin de coopérer efficacement, des procédures de transmission des dossiers et d'échange d'informations ont été mises en place. La coopération s'effectue en langue anglaise. Ces nouveautés ont conduit la CNIL à revoir de manière approfondie ses propres procédures.Entre le 25 mai et le 31 décembre 2018, 257 procédures de coopération européenne ont été introduites par les autorités de protection des données sur des plaintes. La CNIL est « chef de file » sur 24 cas et concernée dans 132 autres cas.

À SUIVRE

Les tendances émergentes

Les plaintes reçues permettent à la CNIL d'identifier de nouvelles tendances :

- **Le visionnage à distance des images issues des dispositifs vidéo**, notamment par l'employeur (depuis son ordiphone ou tablette), pointant un risque de surveillance excessive des employés ;
- **L'installation de caméras dans des unités de soin**, filmant ainsi des personnes vulnérables (patients, personnes dépendantes, mineurs, *etc.*) pour leur « sécurité » ;
- Le souhait des clients d'utiliser leur **droit à la portabilité** de leurs données, notamment auprès de banques ou de services en ligne de contenus ;
- **La sécurité de ses données personnelles**, et pas seulement sur internet (accès à ses données par des collègues dans des établissements hospitaliers ou par un ancien conjoint lors d'un conflit familial ; documents papiers jetés non broyés dans les poubelles ; confidentialité de ses données en qualité de copropriétaire gérées par un syndic, *etc.*) ;
- **Des craintes quant aux données auxquelles les applications mobiles** accèdent dans son téléphone.

LE DROIT D'ACCÈS INDIRECT

Les personnes qui souhaitent faire vérifier les données les concernant susceptibles d'être enregistrées dans les fichiers intéressant la sûreté de l'État ou la défense nationale (article 41), le fichier FICOBA de l'administration fiscale (article 42) ou les fichiers relevant du champ de la directive européenne « police-justice » (article 70-22), peuvent adresser une demande à la CNIL. Elle doit être accompagnée d'une copie d'un titre d'identité et, pour les fichiers « police-justice », de tout élément prouvant la restriction du responsable du traitement dans le cadre de l'exercice direct et préalable des droits.

4 264 demandes de droit d'accès indirect ont été adressées à la CNIL en 2018 représentant initialement un volume global de 6 609 vérifications à mener et portant majoritairement sur le TAJ et le fichier FICOBA. 1 344 d'entre-elles reçues avant le 1er août 2018 (soit 31,50 %) ont fait l'objet (selon les fichiers) d'un transfert total ou partiel vers les différents gestionnaires à la suite de l'entrée en vigueur du décret du 1er août 2018.
Le nombre de vérifications menées en 2018 est en diminution sensible par rapport aux années précédentes (6 331 soit - 20 % par rapport à 2017) en raison de l'interruption à compter du 1er août 2018 des vérifications pour les fichiers « police-justice » et du transfert des demandes les concernant aux différents ministères **(voir partie I - droit d'accès indirect : modification importante des modalités d'exercice des droits pour certains fichiers).**

Les vérifications menées ont majoritairement portées jusqu'au 1er août 2018 sur le Traitement d'Antécédents Judiciaire (47 %). Celles conduites pour les procédures établies par la policenationale se sont traduites par :

- la suppression de 14 % des fiches examinées concernant des personnes mises en cause ;
- la mise à jour par mention des suites judiciaires favorables intervenues dans 21 % des cas, ce qui a eu pour effet de rendre les personnes « inconnues » de ce fichier dans le cadre d'une consultation administrative (enquêtes pour l'obtention d'un agrément ou d'une habilitation pour l'exercice d'un emploi par exemple).

La proportion d'effacements ou de mises à jour est, de manière constante, 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 souvent facilitée.

4 264
demandes

6 609
vérifications à mener

1 344
d'entre-elles reçues avant le 1er août 2018 (soit 31,50%)

INFOSPLUS

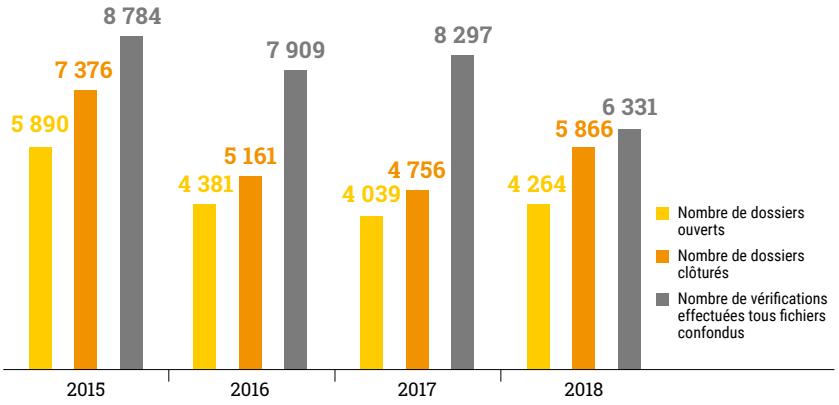
Le droit d'accès indirect comment ça marche ?

À réception d'une demande comportant tous les éléments indispensables à son traitement, 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.

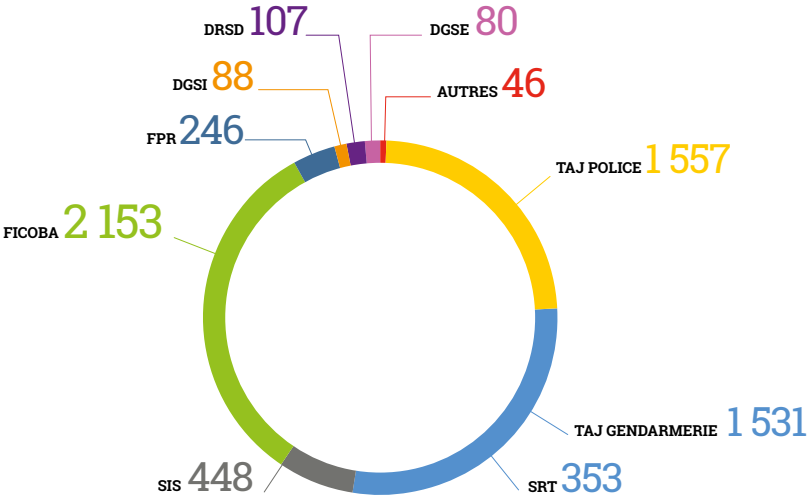
Les données ou l'information sur l'absence de toute donnée peuvent être portées à la connaissance de la personne concernée sous réserve de l'accord du responsable du traitement qui peut s'y opposer si cela est de nature à :

- porter atteinte à la finalité du fichier,
- porter atteinte à la sûreté de l'État ou la défense nationale,
- gêner des enquêtes, recherches, procédures administratives ou judiciaires,
- nuire à la prévention ou la détection d'infractions pénales ou l'exécution de sanctions pénales
- porter atteinte à la sécurité publique, la sécurité nationale ou les droits et libertés d'autrui.

Évolution des demandes de droit d'accès indirect 2015/2018



Demandes de « droit d'accès indirect » adressées à la CNIL en 2018 : fichiers concernés par les demandes



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

FOCUS

Nouvelle extension en 2018 des possibilités d'effacement anticipé du Traitement d'Antécédents Judiciaires (TAJ)

Les conditions d'effacement du TAJ, avant le terme du délai de conservation, sont définies par l'article 230-8 du code de procédure pénale.

À la suite de la décision du Conseil constitutionnel n°2017-670 QPC du 27 octobre 2017, la possibilité d'effacement anticipé des données de TAJ a été étendue par la loi n° 2018-493 du 21 juin 2018 aux personnes condamnées avec des conditions de recevabilité particulières selon l'existence ou non d'inscription au bulletin n°2 du casier judiciaire (cf tableau infra).

L'article 230-8 du code de procédure pénale permet désormais aux personnes condamnées de formuler une demande d'effacement auprès du procureur de la République - ou du magistrat référent si elles font l'objet d'enregistrement pour des faits commis dans plusieurs ressorts territoriaux - qui ont désormais un délai de 2 mois pour y répondre.

Résultats des vérifications relatives au Traitement d'Antécédents Judiciaires (TAJ) effectuées jusqu'au 1er août 2018

	TAJ (procédures établies par la police nationale)	**TAJ** (procédures établies par la gendarmerie nationale)
Nombre de vérifications individuelles effectuées	1 718	1 281
Nombre de personnes inconnues	279	838
Nombre de personnes enregistrées uniquement en tant que victimes	224	124
Nombre de fiches de personnes « mises en cause » vérifiées	1 215	319
- dont pourcentage de fiches supprimées	14 %	19 %
- dont pourcentage de fiches mises à jour par mention de la décision judiciaire favorable intervenue (acquittement, relaxe, non-lieu, classement sans suite) rendant la personne inconnue du fichier sous le profil de consultation administrative (enquêtes administratives)	21 %	33 %
- dont pourcentage de fiches rectifiées ayant eu pour effet de réduire le délai global de conservation de l'enregistrement	1 %	0 %
- 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 %	485 %

Possibilités d'effacement de TAJ avant le terme du délai de conservation

Nature de la décision judiciaire	Délai dans lequel une demande en effacement peut être formulée auprès du procureur de la République (ou du magistrat référent)	Nature de la décision du procureur de la République (ou du magistrat référent)
Jugement de relaxe ou d'acquittement	Immédiatement	Effacement ou, à défaut, mention*
Non-lieu ou classement sans suite	Immédiatement	Mention* ou, à défaut, effacement
Condamnation avec dispense de peines	Immédiatement y compris en cas d'autres inscriptions au B2	Effacement ou mention*
Condamnation avec dispense immédiate de mention au casier judiciaire	Immédiatement y compris en cas d'autres inscriptions au B2	Effacement ou mention*
Condamnation avec relèvement ultérieur de l'inscription au casier judiciaire	A compter de la décision de relèvement	Effacement ou mention*
Autres décisions de condamnation	Immédiatement si aucune autre inscription au B2 ou à compter de la disparition de toute mention dans ce même bulletin	Effacement ou mention*

* La mention a pour effet de rendre les faits concernés inaccessibles dans le cadre de la consultation de ce fichier à des fins d'enquêtes administratives (profil de consultation administrative). Ils demeurent uniquement visibles sous le profil de consultation judiciaire de ce fichier.

Histoires vécues...

MADAME A, 29 ANS, a fait une demande d'accès indirect au Traitement d'Antécédents Judiciaires (TAJ) dans le cadre d'un changement d'orientation professionnelle, craignant qu'une affaire de stupéfiants impliquant son compagnon de l'époque et pour laquelle elle avait été mise hors de cause, ne vienne y faire obstacle. Au terme des vérifications de la CNIL, son enregistrement pour des faits « d'importation non autorisée de stupéfiants, trafic de stupéfiants », soumis à un délai de conservation de 40 ans, a été supprimé car elle n'était effectivement pas mise en cause dans la procédure.

MONSIEUR C, 25 ANS, a fait une demande d'accès indirect au TAJ en raison de l'ajournement de sa demande de naturalisation pour une affaire de « mise en danger d'autrui avec risque immédiat de mort ou d'infirmité par violation manifestement délibérée d'obligation règlementaire de sécurité ou de prudence lors de la conduite d'un véhicule terrestre à moteur ». Cette mention a été supprimée du TAJ car l'examen de la procédure a révélé qu'il ne s'agissait pas de son véhicule et qu'il n'était pas le conducteur de celui impliqué.

MONSIEUR M, 26 ANS, a exercé son droit d'accès indirect à TAJ et les vérifications ont conduit à l'effacement de son enregistrement pour une affaire de « détention non autorisée de stupéfiants », soumise à un délai de conservation de 20 ans, car seul pouvait lui être reproché un « usage de stupéfiants » pour lequel le délai de conservation de 5 ans était arrivé à son terme. Il a été rappelé aux services gestionnaires de TAJ que l'incrimination de « détention de stupéfiants » ne peut être appliquée aux personnes ayant en leur possession des stupéfiants s'il est établi que cette détention est uniquement destinée à leur consommation personnelle.

MONSIEUR S, 39 ANS employé au sein d'une entreprise de transport nationale a souhaité, avant de confirmer sa demande de mutation pour exercer d'autres fonctions donnant lieu à une enquête administrative préalable, s'assurer qu'aucune mention dans TAJ ne puisse y faire obstacle. Les vérifications ont conduit à la suppression de 135 affaires (« vol à la roulotte » principalement) commises lorsqu'il était mineur en raison, d'une part, de l'absence d'archives relatives à ces procédures et, d'autre part, de l'expiration du délai de conservation.

MONSIEUR R, 39 ANS, exerçant la profession d'avocat a saisi la CNIL pour s'assurer qu'aucune inscription dans le fichier TAJ ne fasse obstacle à une réorientation professionnelle dans des administrations régaliennes. Un enregistrement (« menace de délit contre les personnes faite sous condition ») auquel s'applique un délai de conservation de 20 ans a été supprimé sur prescription du procureur de la République. Monsieur R. avait bénéficié pour cette affaire d'un classement sans suite pour « rappel à la loi » et le procureur de la République a fait application de la faculté qui lui est ouverte depuis 2016 de prescrire l'effacement pour les faits ayant bénéficié de telles décisions en tenant compte de la finalité du fichier, de la nature ou des circonstances de l'infraction et de la personnalité de l'intéressé.

MONSIEUR D, 54 ANS, confronté depuis plusieurs années aux agissements d'un usurpateur à la suite de la perte de sa pièce d'identité, a exercé son droit d'accès indirect au TAJ. Dans le cadre des vérifications, il a été invité à déposer ses empreintes pour qu'elles soient comparées avec l'auteur des procédures enregistrées sous son identité. 7 enregistrements en qualité de mis en cause ont ainsi été réattribués à son usurpateur et la seule affaire dans laquelle il était effectivement le mis en cause, datant de 1994, a été supprimée pour expiration du délai de conservation.

MONSIEUR B, 27 ANS, a saisi la CNIL en mars 2018 pour qu'il soit procédé à la vérification du fichier de TAJ après s'être vu opposer un refus de délivrance de sa carte professionnelle d'agent de sécurité privée. La CNIL n'ayant pu parvenir au terme des vérifications pour les procédures enregistrées dans ce fichier par la police nationale avant le 1er août 2018, sa demande a été transférée au ministère de l'Intérieur. Faute de réponse de ce ministère dans un délai de deux mois, Monsieur B est revenu vers la CNIL pour exercer son droit d'accès indirect. Les vérifications ont pu être menées en janvier 2019 et ont conduit à la suppression des deux affaires (« outrage à personne dépositaire de l'autorité publique » et « vol par escalade ») pour lesquelles il avait bénéficié de décisions de classement sans suite.

CONSEILLER

Depuis l'entrée en application du RGPD et la modification de la loi Informatique et Libertés les formalités préalables (déclarations, autorisations) ont considérablement diminué. Toutes les formalités n'ont cependant pas disparu (notamment dans le domaine de la santé). Par ailleurs, la CNIL poursuit ses missions traditionnelles consistant à rendre des avis sur des projets de texte d'origine gouvernementale concernant la protection des données personnelles ou créant de nouveaux fichiers. En contrepartie de la suppression de certaines formalités, la CNIL dispose de nouveaux outils de droit « souple » pour aider à la mise en conformité et des outils plus contraignants pour encadrer les traitements les plus sensibles.

Émilie
Chef du service des affaires régaliennes et des collectivités territoriales

Le service des affaires régaliennes et des collectivités territoriales est composé de six juristes et de deux assistantes. Notre mission est d'accompagner les organismes publics et privés dans leur mise en conformité et leur appropriation de la réglementation relative à la protection des données lorsque leurs projets sont mis en œuvre dans la sphère publique (secteurs de la police, de la justice, des collectivités territoriales, des finances publiques, de l'éducation nationale, des données publiques, de la recherche, etc.).

Si l'évolution de la réglementation Informatique et Libertés a conduit à la disparition de la plupart des formalités préalables, l'activité du service reste marquée par un accompagnement poussé de ces différents acteurs au travers de l'examen des demandes d'avis qui peuvent être transmises tant à l'appui de projets de lois, de projets de décrets, etc. que d'analyses d'impact relatives à la protection des données (AIPD).

Le service travaille ainsi de manière transversale notamment avec le service des outils de la conformité, récemment créé pour tenir compte des opportunités offertes en matière de régulation par le RGPD (certification, codes de conduites, etc.).

Les réflexions et observations formulées à l'occasion de l'examen de ces formalités préalables ont vocation à figurer au sein des projets de délibérations transmis au collège de la CNIL en vue de leur examen lors des « séances plénières ». Au-delà de cette activité, le service est également pleinement engagé dans l'accompagnement de ces organismes au travers de différentes actions qui s'échelonneront dans le temps. Les prochains mois seront ainsi consacrés à la publication de contenus dédiés, par exemple, à destination des collectivités territoriales, au suivi de la consultation publique lancée en matière d'Open Data ou encore à la préparation des prochaines échéances électorales.

LES AVIS ET LES AUTORISATIONS DE LA CNIL

Au titre de ses missions de contrôle en amont des fichiers et de conseil, la CNIL est notamment chargée de rendre des avis sur les projets de textes en séance plénière. En 2018, la CNIL a rendu **120 avis** à destination des pouvoirs publics. On peut citer par exemple les avis portant sur :

- le projet d'ordonnance de réécriture de la loi Informatique et Libertés (Ordonnance n° 2018-1125 du 12 décembre 2018) ;
- le décret d'application de la loi Informatique et Libertés (Décret n°2018-232 du 30 mars 2018 qui modifie le décret 2005-1309) ;
- certaines dispositions du projet de loi d'orientation des mobilités.

342

délibérations

DONT PLUS DE

120

avis à destination des pouvoirs publics

110

autorisations

360

autorisations « santé »

30

auditions parlementaires

Une centaine d'autorisations ont également été adoptées en 2018, pour l'essentiel avant le 25 mai 2018. 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.

INFOSPLUS

Ordonnance de réécriture de la loi Informatique et Libertés et sur le décret d'application de la loi Informatique et Libertés.

L'ordonnance n° 2018-1125 du 12 décembre 2018, publiée le 13 décembre 2018, achève, au niveau législatif, la mise en conformité du droit national avec le RGPD et la directive « police-justice », applicable aux fichiers de la sphère pénale. Cette ordonnance améliore la lisibilité du cadre juridique en matière de protection des données. La CNIL a rendu le 15 novembre 2018 un avis sur ce texte.

L'adaptation du droit français au nouveau cadre européen a été principalement réalisée par la loi du 20 juin 2018, sur laquelle la CNIL s'est prononcée dans son avis en date du 30 novembre 2017. Cette loi a substantiellement modifié la loi Informatique et Libertés et a notamment fait usage de certaines des marges de manœuvre ouvertes aux États membres par le RGPD.

Une ordonnance devait ensuite intervenir pour réécrire et remettre en cohérence la loi du 6 janvier 1978 et d'autres lois françaises traitant de protection des données. Dans son avis du 15 novembre 2018 sur le projet d'ordonnance, la CNIL a estimé que ce texte atteignait pour l'essentiel ses objectifs :

- il permet l'application de règles homogènes sur le territoire métropolitain et dans l'ensemble des collectivités d'outre-mer en matière de protection des données personnelles ;
- il modifie plusieurs dispositions extérieures à la loi du 6 janvier 1978, qui améliorent l'articulation globale de la législation applicable en matière de protection des données ;
- surtout, il améliore la lisibilité de la loi Informatique et Libertés, en précisant les différents régimes applicables en fonction de la nature des traitements concernés : traitements relevant du RGPD, traitements « police justice », traitements concourant à la défense nationale ou la sûreté de l'État, *etc.*

Dans son avis, la CNIL a cependant insisté sur la nécessité de clarifier au maximum les obligations imposées aux organismes traitant des données à caractère personnel, et notamment à des petites et moyennes entreprises ou à des organismes publics de taille modeste. Elle a également émis des observations plus techniques, afin de clarifier ou préciser les conditions de l'action collective ou les modalités d'utilisation des données personnelles à des fins de recherche en santé. Plusieurs de ces observations ont été prises en compte par le Gouvernement dans l'ordonnance promulguée.

Cette ordonnance entrera en vigueur au plus tard en juin 2019, en même temps que le nouveau décret d'application de la loi Informatique et Libertés. Dans l'attente, les dispositions actuelles de la loi Informatique et Libertés, dans sa version modifiée par la loi du 20 juin 2018, restent seules applicables.

L'ACCOMPAGNEMENT DES ACTEURS DE LA SANTÉ : SIMPLIFICATION ET CONSEIL

La loi du 6 janvier 1978 modifiée par la loi n°2018-493 du 20 juin 2018, et plus particulièrement son article 54, a confirmé le pouvoir de simplification des démarches attribué à la Commission grâce à une palette d'outils spécifiques au secteur de la recherche dans le domaine de la santé.

L'année 2018 a été concrètement l'occasion de poursuivre et mettre en œuvre cette simplification selon diverses modalités :

Les méthodologies de référence

En juillet 2018, la CNIL a adopté cinq nouvelles méthodologies de référence (MR-001, MR-003, MR-004, MR-005 et MR-006) qui offrent un cadre sécurisé pour la mise en œuvre des traitements de recherche dans le domaine de la santé.

La création et la mise à jour de méthodologies de référence ont été rendues nécessaires par l'évolution des textes législatifs nationaux, par l'entrée en vigueur du RGPD ainsi que par les retours d'expérience formulés par les acteurs de terrain sur les cadres existants, suite à une concertation.

Les MR-005 et MR-006 sont les premières méthodologies de référence concernant une des composantes du SNDS (Système national des données de santé) : le PMSI (Programme de médicalisation des systèmes d'information). Elles permettent l'accès aux données du PMSI par les établissements de santé, les fédérations et les industriels du secteur de la santé aux fins de réaliser des études dans des conditions strictes de confidentialité et de sécurité.

Depuis leur publication, 402 engagements de conformité à la MR-004 ont été réalisés, 340 pour la MR-005 et 56 pour la MR-006.
De nouvelles méthodologies de référence pourront être adoptées en 2019, en fonction des besoins recensés.

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

La CNIL a homologué en avril 2018 des conditions de mise à disposition de l'Échantillon Généraliste des Bénéficiaires (EGB) issu du Système national d'information inter-régimes de l'Assurance maladie (SNIIRAM), permettant, pour certains traitements et sous réserve de conditions précises, un examen unique par l'INDS, sans avis du CEREES ni autorisation de la CNIL.

Les décisions uniques

Le pouvoir de simplification peut s'appliquer également aux demandes d'autorisation. En effet, 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 (article 54 IV de la loi).

En 2018, une dizaine de décisions uniques, nécessitant un accès à certaines composantes du SNDS (PMSI et EGB), ont été délivrées par la Commission. Ces décisions uniques permettent de simplifier les démarches des responsables de traitement réalisant une grande volumétrie de traitements répondant à une même finalité ou devant mettre en œuvre de tels traitements dans des délais très courts.

Le traitement du NIR (numéro de sécurité sociale) à des fins de recherche

En 2018, la Commission a été saisie de plusieurs demandes d'autorisation relatives au traitement du numéro d'inscription des personnes au Répertoire national d'identification des personnes physiques (NIR) dans le cadre de projets de recherche, d'étude ou d'évaluation dans le domaine de la santé.

Ces demandes d'autorisation s'inscrivent dans la continuité du dispositif instauré par l'article 193 de la loi de modernisation de notre système de santé, et précisé à l'article 22 de la loi Informatique et Libertés. Cet article prévoit que les traitements mis en œuvre dans le domaine de la santé, qui portent sur des données parmi lesquelles figure le NIR sont soumis au chapitre IX de la loi Informatique et Libertés.

Cette évolution des textes permet la réalisation d'appariements entre différentes sources de données, à l'aide du NIR, sous réserve d'une autorisation de la CNIL, alors que l'ancienne procédure plus contraignante exigeait un décret en Conseil d'État pris après avis de la CNIL.
Une dizaine d'autorisations nécessitant le traitement du NIR ont été délivrées en 2018, après un examen par les services des conditions de sécurité et de circulation du NIR.

Un accompagnement quotidien des acteurs de la santé

De multiples actions ont ainsi été menées : rencontres avec les fédérations du secteur sanitaire, participation à des salons et à des colloques à destination des professionnels de santé, refonte de la page internet « santé » et mises en ligne de nombreuses fiches thématiques, rédaction d'un guide en partenariat avec le Conseil national de l'Ordre des médecins, *etc.*

Ces actions d'accompagnement incluent également l'élaboration, en concertation avec les acteurs concernés, de nouveaux référentiels pour mettre à jour les anciennes normes simplifiées et autorisations uniques du secteur au regard du RGPD et de l'évolution des pratiques des acteurs. Les travaux relatifs aux vigilances sanitaires, à la messagerie sécurisée et aux professionnels de santé exerçant à titre libéral ont été avancés et devraient aboutir à la publication de nouveaux référentiels courant 2019. Des travaux sont également en cours pour faire émerger les premiers codes de conduite sectoriels.

LES RELATIONS AVEC LE PARLEMENT

La CNIL entretient des rapports réguliers avec le Parlement. Au cours de l'année 2018, elle a participé à une trentaine d'auditions, sous toutes ses formes : auditions de rapporteurs sur des projets de textes, auditions devant des missions d'information ou groupes de travail, table-rondes, contributions écrites.

Le premier semestre de l'année 2018 a été marqué par l'examen du projet de loi relatif à la protection des données personnelles, texte aménageant la mise en œuvre du RGPD et procédant à la réfection globale de la loi Informatique et Libertés de 1978. Ce projet de loi a occasionné, outre une audition avec les rapporteurs des commissions des lois des deux assemblées, de nombreux échanges avec les parlementaires des commissions saisies tant sur le fond que pour avis. La qualité des débats parlementaires a contribué à enrichir ce projet de loi qui marque un tournant pour la CNIL, 40 ans après l'adoption de la loi relative à la protection des données personnelles.

S'agissant des projets de loi, l'expertise de la CNIL a également été sollicitée, toutes chambres confondues, pour l'examen des projets de loi pour un État au service d'une société de confiance, de lutte contre la fraude et d'orientation des mobilités.

La CNIL est également de plus en plus contactée par les commissions permanentes pour des auditions relatives à des propositions de loi qui comportent des dispositions relatives aux données personnelles. En 2018, ces auditions ont porté sur les propositions de loi relative à la lutte contre la manipulation de l'information, à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique, à la reconnaissance des proches aidants.

De manière générale, la diversification des commissions permanentes du Parlement qui désormais souhaitent contacter la CNIL pour son expertise est le résultat d'une double évolution concomitante, la montée en puissance de l'initiative parlementaire dans les ordres du jour des assemblées et la place croissante des sujets numériques dans tous les domaines traités par le législateur.

L'importance de recueillir l'avis de la CNIL, lorsque le sujet le justifie, sur des propositions de loi a été pleinement reconnue par le législateur. La loi relative à la protection des données personnelles, promulguée au mois de juin 2018, ouvre désormais la voie à la possibilité de saisir la CNIL pour avis, à l'initiative des présidents des assemblées, des commissions permanentes ou des présidents des groupes politiques, sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données.

Au cours de l'année 2018, la CNIL a aussi contribué aux travaux de réflexion du parlement sur des sujets variés tels que les missions d'information de l'Assemblée nationale relatives aux fichiers mis à la disposition des forces de sécurité, aux chaînes de blocs, à la déscolarisation. Au Sénat, la CNIL a été auditionnée par la mission d'information sur le vote électronique, les groupes de travail sur l'amélioration des fiches S et sur l'intelligence artificielle.

De même, la CNIL a participé à plusieurs tables-rondes organisées dans les deux assemblées : régulation audiovisuelle et numérique, enjeux juridiques des compteurs communicants Linky, algorithmes.

La CNIL a également répondu aux questions des parlementaires nommés en mission sur l'accueil et l'intégration des étrangers en France, et la lutte contre le racisme et l'antisémitisme sur internet.

Enfin, à l'occasion des quarante ans de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la CNIL a organisé un colloque le 29 mars au Sénat pour dresser le bilan de cette loi et réfléchir aux perspectives d'avenir de celle-ci à l'aune de l'entrée en vigueur du Règlement européen. Ce colloque, qui a réuni une pluralité d'acteurs issus du monde de la recherche, de l'entreprise mais aussi des praticiens du droit Informatique et Libertés, a reçu le haut patronage du président du Sénat qui en a prononcé le discours d'ouverture.

ACCOMPAGNER

la conformité grâce à de nouveaux outils

L'accompagnement des organismes dans la mise en œuvre de leurs traitements fait partie des missions de la CNIL. Bien avant l'entrée en vigueur du RGPD, la CNIL a proposé des outils destinés à aider les responsables de traitement : méthodologie de mise en conformité, guides pratiques, logiciel destiné à réaliser des analyses d'impact sur la protection des données, *etc.* Cette mission d'accompagnement a été renforcée par le législateur dans le cadre de la modification de la loi Informatique et Libertés grâce à de nouveaux outils dont il l'a dotée : référentiels, lignes directrices, recommandations, *etc.* Tous ces outils proposés par le RGPD ou la loi française sont « destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes en vigueur. Au cours de l'année 2018, la CNIL a déjà eu l'occasion de mettre à disposition des organismes concernés des outils de conformité (référentiels de certification des délégués à la protection des données, lignes directrices sur les analyses d'impacts sur la protection des données (AIPD), règlement type en matière de biométrie, méthodologies de référence pour les traitements de santé, *etc.*) et de fournir un accompagnement aux délégués à la protection des données.

Anne
Juriste au service de délégués à la protection des données (DPO)

J'ai rejoint le service des délégués à la protection des données (anciennement le service des correspondants Informatique et Libertés, « CIL ») en 2015. Au sein de cette équipe, j'ai pu être témoin du changement de paradigme lié à l'entrée en vigueur du RGPD et de la transformation du métier de délégué à la protection des données.

Le service des délégués, composé de 6 juristes, est le point de contact privilégié de ces professionnels. Nos activités sont extrêmement variées : réponses à des demandes de conseil, organisation et animation d'ateliers d'information sur le RGPD, permanence téléphonique, développement et animation de réseaux de délégués, mais également et surtout élaboration d'outils (guides, FAQ, modèles de documents) en lien avec les services sectoriels de la direction de la Conformité. Ce service dispose ainsi d'une vision à 360° des problématiques du terrain et des enjeux métiers autour de la protection des données.

L'un des projets dans lequel j'ai été particulièrement impliquée en 2018 concerne les référentiels de la CNIL en matière de certification des compétences du délégué adoptés en septembre. Ce travail a nécessité d'élaborer les projets de référentiels, de les tester en les soumettant à consultation publique, de discuter, d'analyser les commentaires du terrain (associations de délégués et organismes certificateurs) et d'aboutir au juste équilibre entre les exigences de la CNIL, les attentes des professionnels de la protection des données et les réalités du monde de la certification. Cela a été une mission particulièrement enrichissante et qui est loin d'être terminée puisque nous étudions actuellement les dossiers de demande d'agréments qui nous sont soumis et que les attentes sont fortes en ce domaine.

L'ENCADREMENT DES ANALYSES D'IMPACT SUR LA PROTECTION DES DONNÉES (AIPD)

L'analyse d'impact relative à la protection des données (AIPD) est un des éléments centraux du RGPD. La CNIL propose déjà de nombreux outils permettant aux professionnels de mieux comprendre leurs obligations et de les mettre en œuvre en pratique : guides pratiques, logiciel, étude de cas, questions-réponses, *etc.*

En complément des lignes directrices adoptées au niveau européen en octobre 2017, la CNIL a adopté, le 11 octobre 2018, ses propres lignes directrices pour préciser notamment le périmètre de l'obligation d'effectuer une AIPD, les conditions de réalisation de l'AIPD et les cas dans lesquels une AIPD doit lui être transmise.

Conformément à ce que prévoit l'article 35.4° du RGPD, la CNIL a également élaboré une liste de traitements pour lesquels elle estime nécessaire qu'une AIPD soit réalisée.

Ce projet de liste a été soumis avant son adoption définitive à l'avis du Comité européen de la protection des données (CEPD).

Le Comité a rendu fin septembre un avis sur 22 projets de listes élaborés par les autorités nationales de protection des données, dont la liste française, afin de s'assurer de leur bonne cohérence et de l'application homogène du RGPD dans l'Union européenne.
Sur la base de cet avis, la CNIL a adopté définitivement sa liste. Elle comporte quatorze types d'opérations de traitement pour lesquelles elle estime obligatoire de réaliser une analyse d'impact relative à la protection des données. Pour autant, cette liste n'est pas exhaustive, dans la mesure où des traitements qui n'y figurent pas peuvent néanmoins devoir faire l'objet d'une AIPD. C'est le cas des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques au regard des 9 critères issus des lignes directrices du CEPD.
Enfin, la CNIL adoptera prochainement la liste des traitements pour lesquels aucune AIPD n'est requise, conformément à ce que permet l'article 35.5° du RGPD.

UN RÈGLEMENT TYPE « BIOMÉTRIE » EN MILIEU PROFESSIONNEL

L'entrée en application du RGPD a consacré la position protectrice de la CNIL sur les données biométriques, en les incluant désormais à la liste des données dites « sensibles » dès lors qu'elles sont utilisées à des fins d'identification de personnes. Leur traitement devient interdit, sauf à répondre à l'une des exceptions limitativement énumérées par le règlement.

Ce changement de cadre juridique a conduit la Commission à mettre à jour sa doctrine sur la biométrie d'accès aux locaux et dispositifs utilisés en milieu professionnel (autorisations uniques). Elle l'a fait en utilisant une nouvelle prérogative que lui a confiée le législateur français. La loi du 20 juin 2018 a en effet permis à la CNIL d'adopter des règlements types pour, notamment, préciser l'encadrement des traitements de certaines catégories de données « sensibles », dont la biométrie. Un règlement type est un texte à portée réglementaire, juridiquement contraignant pour l'ensemble des acteurs publics et privés. Le premier règlement type adopté par la CNIL porte, précisément, sur les conditions que doivent respecter les employeurs souhaitant recourir à la biométrie en matière de contrôle d'accès sur le lieu de travail.

Publié à la suite d'une consultation publique menée en automne 2018, ce document reprend largement les principes dégagés par la Commission dans ses précédentes autorisations uniques, tout en y intégrant des dispositions relatives aux nouvelles obligations du RGPD (telle que la réalisation d'une AIPD, la tenue du registre des activités de traitement, *etc.*).

L'accompagnement au numérique des personnes en difficulté

La dématérialisation des services publics peut constituer pour, certains usagers, un véritable obstacle à l'accès aux droits et/ou à la réalisation de certaines démarches obligatoires. Les raisons peuvent être multiples : absence de matériel informatique adapté, non-maîtrise des outils informatiques, *etc.* Ces usagers sont donc amenés à se déplacer, lorsqu'ils le peuvent dans des espaces publics numériques (EPN) ou auprès de guichets sociaux, en vue de solliciter un accompagnement leur permettant de réaliser leurs démarches numériques. Les travailleurs sociaux sont ainsi amenés à collecter et utiliser les données des personnes qu'ils accompagnent. C'est dans ce contexte que la CNIL a élaboré un kit d'information à l'attention des professionnels, composé de deux fiches de bonnes pratiques (« 12 conseils pour utiliser un ordinateur public en toute sécurité » et « Professionnels du secteur social : comment mieux protéger les données de vos usagers ») ainsi qu'un modèle de mandat, qui sont autant d'outils leur permettant de contribuer au respect de la vie privée et la confidentialité des données de leurs publics.

LES NOTIFICATIONS DE VIOLATION DE DONNÉES

Les notifications de violations de données à caractère personnel, introduites par le RGPD, permettent de faire émerger et de prendre conscience des fragilités qui pèsent sur les systèmes d'information et des menaces qu'il faut prendre en compte pour sécuriser correctement les traitements.

Bilan 2018 des notifications de violations de données

Une violation de données à caractère personnel est constituée par toute action, intentionnelle ou non, portant atteinte à la confidentialité, l'intégrité ou la disponibilité de ces données. L'entrée en application du RGPD le 25 mai 2018 a imposé, à tous les organismes qui traitent des données personnelles, de mettre en place des mesures pour prévenir les violations de ces données.

Dans le cas où, malgré la vigilance du responsable de traitement, la violation vient à se produire, le RGPD dispose que, en fonction du risque engendré par la violation, trois types de mesures doivent être prises. La violation doit toujours être « documentée ». Lorsqu'elle présente un risque pour les personnes, la CNIL doit être informée de l'incident. Lorsque ce risque atteint un niveau élevé, les personnes concernées doivent elles-mêmes en être informées. Cette palette de réactions permet de prendre les mesures nécessaires et adéquates pour protéger leurs droits et libertés.

Dès le 25 mai 2018, la Commission a été rendue destinataire des premières notifications de violations ; elle a reçu 1 170 notifications au cours de l'année 2018. Ces notifications faisaient suite, en très grande majorité, à des **atteintes à la confidentialité** des données.

2018, les notifications de violation en chiffres

Nature de la violation	Volume
Perte de la confidentialité	981
Perte de la confidentialité, Perte de la disponibilité	50
Perte de la confidentialité, Perte de l'intégrité	35
Perte de la confidentialité, Perte de l'intégrité, Perte de la disponibilité	26
Perte de la disponibilité	52
Perte de l'intégrité	16
Perte de l'intégrité, Perte de la disponibilité	10

Dans le cadre de cette nouvelle mission, la CNIL a adopté, en priorité, une démarche d'accompagnement.

L'objectif est, lorsque cela est nécessaire, d'interagir avec les responsables de traitements déclarant des violations pour les aiguiller :

- d'une part sur l'estimation du niveau de risque engendré, et donc la nécessité ou non d'informer les personnes concernées ;
- et d'autre part, sur les mesures techniques ou organisationnelles à mettre en place, à la suite de la violation, afin de résoudre le problème à court terme et d'éviter que ce dernier se reproduise dans le futur.

En fonction des circonstances, la CNIL peut être amenée à orienter les déclarants vers certains services de l'État, notamment les services de Police ou de Gendarmerie, ou encore vers https://www.cybermalveillance.gouv.fr/.

1 170

Notifications de violations de données reçues en 2018

Secteur d'activité des organismes	Volume
Hébergement et restauration	188
Commerce ; réparation d"automobiles et de motocycles	180
Activités financières et d"assurance	139
Activités spécialisées, scientifiques et techniques	137
Information et communication	100
Administration publique	92
Autres activités de services	61
Industrie manufacturière	48
Enseignement	47
Activités de services administratifs et de soutien	42
Santé humaine et action sociale	41
Activités immobilières	24
Transports et entreposage	23
Autres	48

Histoires vécues...

LES MESURES QUI POURRAIENT ÊTRE PRISES POUR ÉVITER LA VIOLATION DE DONNÉES

Un site de e-commerce se fait pirater, l'attaquant s'installe sur le serveur, injecte une fausse page de paiement lui permettant de capter les données bancaires tout en redirigeant le flux vers la plateforme officielle afin de ne pas se faire démasquer.

- Afin de se protéger, il faut veiller à mettre à jour, de manière régulière, l'ensemble de ses applicatifs, notamment lorsqu'il s'agit de vulnérabilités publiques, critiques et dont les correctifs sont disponibles ;

Une enseigne commerçante voit son système attaqué par des pirates ayant pour objectif de dérober des informations du compte fidélité des clients pour ensuite profiter des avantages de ces derniers au sein des magasins physiques ;

- Afin de limiter le risque, il faut imposer à ses utilisateurs des mots de passe non triviaux et qui ne sont pas basés sur des informations liées directement à la personne ;

Une association chargée du suivi social de personnes subit une effraction de son local et l'ensemble de ses ordinateurs portables sont dérobés. Ces derniers contenaient les dossiers des personnes suivies par l'association ;

- Chiffrer les ordinateurs portables ainsi que les supports amovibles permet d'éviter de voir les données dérobées, utilisées ou divulgues. De même, effectuer des sauvegardes de façon régulière permet de limiter le risque de violations liées à un problème de disponibilité ou d'intégrité ;

À la suite d'une mise à jour, un administrateur système omet de remettre en place une mesure de sécurité sur son serveur ce qui rend la base des clients de l'organisme librement accessible sur Internet.

- Avant une mise en production lors du déploiement de nouvelles versions d'applications, il faut effectuer des tests de non régression afin de s'assurer que le système mis en ligne est toujours sécurisé.

Les tendances de cette première année de RGPD

Deux causes principales émergent au sein des notifications reçues par la CNIL : plus de 50 % des violations ont pour cause un **acte externe malveillant** et 17 % font suite à un **acte interne accidentel.**

Au sein de ces deux principales causes, émergent également des origines principales :

- les actes externes malveillants ont pour origine principale un **piratage** au niveau cyber et pour origine secondaire un **vol** au niveau physique ;
- les actes internes accidentels ont pour origine principale des **données personnelles adressées au mauvais destinataire** et pour origine secondaire la **publication non volontaire** d'informations.

Quels éclairages peuvent apporter ces violations sur la sécurité des systèmes d'information ?

L'analyse des violations reçues met en évidence des faiblesses des systèmes d'information ou des processus mis en œuvre au sein des entreprises. Ces incidents peuvent avoir des conséquences opérationnelles très fortes ainsi que des répercutions réputationnelles très importantes pour les organismes. Dans cette optique, la cybersécurité est une composante essentielle car elle permet, de manière proactive et préventive, de diminuer le risque de survenance de violation ainsi que, dans le cas où l'incident se produit tout de même, de limiter l'impact de ce dernier. Dès lors, afin de protéger les données traitées et de protéger les actifs de l'organisme, il est important, aujourd'hui plus que jamais, d'avoir conscience de la nécessité d'investir dans la sécurité de l'information.

Afin de prévenir la majeure partie de ces incidents, la CNIL rappelle qu'il est essentiel de :

- **intégrer la sécurité dès le lancement d'un projet ;**
- **effectuer régulièrement les mises à jour de sécurité** sur les systèmes d'exploitation, les serveurs applicatifs et les bases de données ;
- **utiliser des mots de passe robustes** et non communs à différents services ;
- effectuer des sauvegardes régulières ;
- **sécuriser les postes de travail mobiles** ainsi que les supports amovibles par du chiffrement ;
- **informer régulièrement le personnel sur les risques et enjeux** de la sécurité.

INFOSPLUS

Cryptolockers et atteinte à la disponibilité :

Bien que les atteintes à la disponibilité ne soient que faiblement représentées dans les notifications reçues, ces dernières persistent et font souvent suite à l'activation d'un *cryptolocker* ou *ransomware* (logiciel crypto-verrouilleur ou rançongiciel, il s'agit d'un type de logiciel malveillant prenant en « otage » les données de sa victime en les chiffrant puis en demandant à leur propriétaire de payer une rançon, le plus souvent en crypto-monnaie, de type Bitcoin, afin d'obtenir, théoriquement, la clé permettant de déchiffrer et récupérer les données). Afin de se prémunir, mettre à jour de façon régulière ses anti-virus, sensibiliser les utilisateurs à cette problématique et mettre en place des sauvegardes régulières permet de limiter le risque et d'atténuer l'impact lié à ces attaques. Leurs effets peuvent être dévastateurs, pour les entreprises ainsi que pour les personnes concernées.

Ces quelques recommandations simples, issues du guide sécurité publié par la CNIL en 2018, permettent d'éviter de nombreuses violations ou limiter leur impact.
Les mesures de ce guide, ainsi que celle émises par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dans son guide d'hygiène informatique, doivent aujourd'hui être le socle minimum sur lequel toute organisation fait reposer son système d'information. Le respect de ces mesures permet d'atteindre un double objectif vital : préserver la continuité d'activité de l'organisme, protéger les données personnelles des employés, clients ou usagers.

L'ACCOMPAGNEMENT DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Le RGPD consacre le rôle du délégué à la protection des données (DPO) dont la désignation est rendue obligatoire dans certains cas. En tant qu'autorité de régulation, la CNIL a fait le choix depuis 2005 avec le correspondant Informatique et Libertés (CIL), son préfigurateur, d'encourager et de veiller au bon développement de ce métier. En proposant un service dédié à l'accompagnement des DPO, la CNIL est en prise directe avec les pratiques « métiers » et dispose ainsi d'une vision globale des enjeux sectoriels.

La transformation d'un métier

L'entrée en application du Règlement transforme le métier des CIL en véritable chef d'orchestre des données dans l'entreprise ou dans l'organisme à laquelle il appartient. Le positionnement du DPO est fortement affirmé ainsi que ses ressources afin qu'il puisse accomplir pleinement son métier qui implique une capacité à se poser en pilote de la conformité.
Il ne doit pas travailler en vase-clos, mais être au contraire pleinement « branché » sur les activités opérationnelles de son organisme. Il devient un maillon essentiel de la gouvernance de la donnée, en lien avec le responsable de la sécurité des systèmes d'information (RSSI) et la direction des systèmes d'information (DSI).
C'est pour cette raison que la CNIL a poursuivi en 2018 son rôle de régulateur de l'écosystème du métier de DPO :

- en travaillant à la reconnaissance du métier : elle collabore à cet effet à une initiative du ministère du travail (DGEFP) sur l'emploi, la formation et les conditions d'exercice de la fonction de délégué au sein des organismes publics ou privés. D'autres initiatives sont identifiées pour 2019 afin de compléter cette démarche ;
- en pilotant le développement de la certification des compétences du DPO et en veillant au respect des référentiels qu'elle a adoptés en septembre 2018.

À SUIVRE

En 2019, afin que ces ateliers soient suivis par le plus grand nombre, certains d'entre eux seront accessibles à distance, en particulier ceux qui traitent de sujets généralistes. Les ateliers en présentiel seront réservés en priorité à des sujets plus ciblés, ou à l'animation des collectifs identifiés nécessitant un soutien spécifique (formation de formateurs ou de relais afin de démultiplier les effets de la formation au réseau concerné).

« Pour exercer son métier efficacement, un délégué doit avoir des moyens et le soutien de sa direction ».

La nécessaire évolution de l'accompagnement des DPO

Avec les cas de désignations obligatoires ainsi que celles issues d'une démarche volontaire, la CNIL s'est préparée à ce changement d'échelle en proposant dès 2017 de nouveaux contenus sur cnil.fr relatifs au DPO ainsi qu'un téléservice en mars 2018 permettant d'anticiper la désignation et de se préparer à l' application du RGPD au plus tôt.

La CNIL a ainsi vu le nombre de ses interlocuteurs augmenter considérablement : elle est passée de 18 000 organismes dotés d'un CIL à 39 500 organismes ayant désigné un DPO, fin 2018. Ces changements rendent indispensables l'adaptation des modalités d'accompagnement des DPO par la CNIL qui les soutient désormais :

- collectivement, dans la constitution et l'animation de réseaux sectoriels, métiers et/ou géographiques de DPO qu'ils sont invités à développer. Ces réseaux répondront à un premier niveau de questions du terrain, la CNIL n'intervenant qu'en second temps avec ces représentants et fédérations,
- individuellement, au stade de leur désignation puis de l'exercice de leurs missions avec une permanence téléphonique et adresse électronique dédiées.

La mission de conseil de la CNIL se traduit notamment pour les délégués à la protection des données par la tenue d'ateliers. En 2018, la CNIL a permis à plus de 2 300 personnes de découvrir plusieurs thématiques :

- généralistes avec l'atelier RGPD et l'atelier sur les grands principes de la sécurité,
- spécifiques avec l'atelier relatif à la réalisation d'une analyse d'impacts,
- et sectorielles avec l'atelier sur la santé.

39 500

organismes ont désigné un délégué en 2018 (dont 1/3 dans le secteur public)

Ce qui représente

16 200

DPO personnes physiques par l'effet des mutualisations

2 300

personnes accueillies à la CNIL lors des ateliers (soit 35 % de plus qu'en 2017)

5 400

appels reçus à la permanence juridique dédiée aux DPO (soit 33 % de plus qu'en 2017)

FOCUS

La certification des compétences du DPO

Avec la loi du 20 juin 2018, la Commission détient une nouvelle compétence en matière d'agrément des organismes certificateurs s'agissant de la certification de personnes. La Commission peut désormais délivrer des agréments et élaborer les critères des référentiels d'agrément et de certification.

Non obligatoire pour être désigné en tant que délégué à la protection des données (DPO), l'enjeu de la certification est de faciliter l'identification :

- des expertises en matière de protection des données, en s'appuyant sur un référentiel d'exigences élaboré par la Commission. La certification permet aux personnes physiques de justifier qu'elles répondent aux exigences de compétences et de savoir-faire du délégué prévues par le règlement. Le délégué doit en effet disposer de connaissances spécialisées du droit et des pratiques en matière de protection des données ;
- des organismes de certification indépendants, agréés par la CNIL.

La CNIL a adopté le 20 septembre 2018 deux référentiels :

- Un référentiel de certification qui fixe les exigences requises pour être candidat à la certification et la liste des 17 compétences et savoir-faire pour être certifié en tant que délégué à la protection des données ;
- Un référentiel d'agrément qui fixe les critères applicables aux organismes de certification pour être agréés par la CNIL en vue de délivrer la certification DPO.

Ces référentiels ont fait l'objet d'une consultation publique sur le site de la CNIL entre le 23 mai et le 22 juin 2018 (176 contributions reçues) et de réunions de travail avec les associations professionnelles de DPO et plusieurs organismes de certification. Cette consultation a permis d'enrichir les référentiels de façon constructive.

LA CRÉATION D'UN NOUVEAU SERVICE

La CNIL s'est dotée, depuis le 14 mai 2018, d'un service dédié aux outils de la conformité dont la principale mission est d'accompagner les organismes qui souhaitent recourir aux vecteurs de conformité que sont les codes de conduites, les analyses d'impact, la certification et les règles d'entreprise contraignantes (BCR). Ces outils sont autant d'instruments contribuant à la responsabilisation des organismes. En effet, dans un contexte de fin des formalités préalables, ils permettent aux organismes tant du secteur public que du secteur privé de mesurer leur conformité avec les exigences du RGPD et de la loi Informatique et Libertés. Ils offrent un éventail de solutions adaptées aux différents besoins des responsables de traitement ou des sous-traitants. Ainsi, les BCR conviennent aux grands groupes internationaux alors que les codes de conduite concernent des secteurs d'activité spécifiques. Des produits, des traitements ou des services pourront faire l'objet d'une certification et les analyses d'impact amènent les responsables de traitement et les sous-traitants à concevoir des traitements respectueux des exigences légales.

La CNIL, avec cette équipe dédiée, accompagne les professionnels sur ces sujets qui sont pour la plupart nouveaux :

• **Un code de conduite** peut être porté par une association, une fédération ou une organisation professionnelle représentant un secteur d'activité. Ce porteur du code va être accompagné et conseillé dans la première phase de conception structurelle afin que ce code réponde aux exigences de contenu prévues par le RGPD. Le service des outils participera également à l'agrément des organismes tiers en charge du contrôle de ces codes ;
• **Les groupes d'entreprises** travaillant à la mise en place de règles d'entreprises contraignantes (BCR) et qui auront choisi la CNIL comme autorité chef de file devront adresser leur dossier à ce service qui sera en charge de l'instruction de la demande et de la coordination avec les autres autorités européennes.

• **La maîtrise de la méthodologie** applicable aux analyses d'impact est un facteur essentiel de la réussite de cet exercice. Depuis 2 ans de nombreux ateliers pratiques ont été organisés sur ce sujet, cette dynamique sera maintenue en 2019 avec une orientation vers le conseil et l'accompagnement méthodologique via les têtes de réseaux.

• **Le RGPD a attribué une nouvelle compétence** aux autorités de contrôle pour la mise en place de mécanismes de certification en matière de protection des données. La CNIL peut ainsi intervenir à toutes les étapes d'une procédure de certification entrant dans le champ d'application du Règlement. La loi Informatique et Libertés modifiée par la loi du 20 juin 2018 lui donne également une compétence spécifique pour la certification de personne.

Au-delà de ces outils spécifiques, la CNIL a créé sur son site un espace permettant de s'informer et de se documenter sur l'ensemble des outils de la conformité prévus par le RGPD poursuivant ainsi sa mission de sensibilisation du public professionnel.

LES CADRES DE RÉFÉRENCE

La CNIL élabore des cadres de référence permettant de guider les organismes dans la mise en conformité de leur traitement. Ces instruments de régulation ont vocation à donner davantage de sécurité juridique aux organismes. Ils sont élaborés en concertation avec les acteurs ou secteurs concernés.

Les lignes directrices de la CNIL

Elles viennent en complément de celles adoptées au niveau européen par le Comité européen à la protection des données (CEPD). Elles donnent des éléments d'interprétation des textes en informant les acteurs des procédures à suivre et règles à appliquer Elles n'ont pas de caractère contraignant (droit souple) mais donnent de la sécurité juridique aux acteurs qui savent qu'en les respectant, ils sont conformes à la réglementation.

***Exemple** : les lignes directrices de la CNIL sur les AIPD (analyse d'impact sur la protection des données) ont été publiées afin de préciser le périmètre de l'obligation d'effectuer une AIPD, les conditions de réalisation de celle-ci et les cas dans lesquels une AIPD doit lui être transmise.*

Les référentiels sectoriels

Ils concernent un secteur ou une thématique particulière et constituent l'interprétation appliquée à un secteur par la CNIL des textes relatifs à la protection des données. Un référentiel constitue un cadre de référence qui va permettre à un organisme de mettre en conformité un traitement de données spécifique et le cas échéant, l'aider à faire l'analyse d'impact ou même pour certains d'entre eux, dispenser de la réalisation d'une analyse d'impact. Ils ont vocation à remplacer les autorisations uniques, normes simplifiées et packs de conformité. Ils n'ont pas de caractère contraignant (droit souple) mais donnent de la sécurité juridique aux acteurs qui savent qu'en les respectant, ils sont conformes à la réglementation.

***Exemple** : les référentiels gestion des clients, gestion des impayés et ressources humaines seront publiés en 2019.*

Les recommandations

Elles portent sur des sujets précis et facilitent la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel en proposant des solutions opérationnelles. Elles n'ont pas de caractère contraignant (droit souple) mais donnent de la sécurité juridique aux acteurs qui savent qu'en les respectant, ils sont conformes à la réglementation.

***Exemple** : les recommandations de la CNIL sur les mots de passe ou celle sur les cookies et traceurs*

Les règlements type

Ce sont des cadres de référence contraignants qui indiquent aux organismes comment encadrer leurs traitements de données biométriques, génétiques, de santé ou d'infraction et assurer la sécurité de leurs systèmes de traitement de données à caractère personnel. Les organismes qui mettent en oeuvre ces traitements sont tenus de respecter les indications données dans le règlement type, sous peine de sanctions.

***Exemple** : règlement type biométrie publié en mars 2019*

Les méthodologies de référence en santé (MR)

Ce sont des guides méthodologiques, dédiés à la recherche en santé qui précisent les règles à observer, notamment quant aux modalités de collecte, de vérification et d'exploitation statistique des données et quant à la nature des données susceptibles d'être collectées. Ces méthodologies sont conçues en concertation avec l'Institut national des données de santé et les représentants du secteur concerné. Elles ont un caractère contraignant et nécessitent la réalisation d'un engagement de conformité sur le site internet de la CNIL. La Commission a entrepris la mise en œuvre d'un programme de simplification des démarches dans le domaine de la santé.

***Exemple** : les 6 méthodologies de référence homologuées et publiées par la CNIL*

Les méthodologies de référence en matière d'anonymisation

La loi Informatique et Libertés permet le recours à des méthodologies de référence en matière d'anonymisation. Ces méthodologies sont constituées d'un ensemble d'exigences spécifiques à un contexte donné, elles vont décrire des critères pratiques à respecter qui permettront de s'assurer de la conformité à la loi de processus d'anonymisation. Elles sont homologuées et publiées par la CNIL.

PARTICIPER
à la régulation internationale

L'année 2018 a été marquée au plan européen et international par l'entrée en application le 25 mai 2018 du Règlement général sur la protection des données (RGPD) et de la Directive dite « police justice ». Ces textes instituent la création au plan européen d'un nouvel organe communautaire le Comité Européen de la Protection des Données et d'un nouveau modèle de coopération entre autorités nationales notamment pour les traitements dits transfrontaliers. Dans ce nouveau cadre règlementaire, la CNIL a participé activement à l'ensemble des travaux du Comité européen et à la gestion quotidienne des dossiers transfrontaliers en étroite collaboration avec ses homologues européens. Au niveau international, la CNIL a présidé la Conférence internationale jusqu'en octobre 2018 et elle a été très active au sein du réseau francophone (AFAPDP).

Émilie
Juriste au service des affaires européennes et internationales

En mai 2018, un nouvel organe communautaire a vu le jour, le Comité Européen de la Protection des Données. Notre service a participé activement dès la première plénière de ce comité à l'élaboration de la doctrine des autorités européennes réunies désormais au sein de ce nouvel organe. Nous assurons aussi un rôle de veille et d'alerte des nouveaux cas transfrontaliers qui sont désormais soumis au mécanisme du guichet unique et sur lesquels nous échangeons régulièrement avec nos homologues et nos collègues en interne.

En 2018, nous avons aussi continué à évaluer le cadre juridique offert par les pays tiers dans le cadre de l'adoption des décisions d'adéquation de la Commission européenne. Pour la première décision adoptée sur la base du RGPD, nous avons examiné en détail la législation du Japon afin de déterminer si celle-ci offre un niveau de protection des données essentiellement équivalent à celui assuré dans l'Union européenne. Pour ma part, j'ai plus particulièrement participé à l'évaluation du droit pénal japonais et des garanties offertes dans ce domaine en matière de protection des données.
En octobre 2018, j'ai aussi participé à la seconde revue annuelle du privacy shield, qui s'est tenue à Bruxelles et qui s'est conclue par l'adoption d'un avis collectif du Comité Européen de la Protection des données en janvier 2019. Dans son avis, le Comité a reconnu les améliorations apportées par rapport à l'année précédente, tout en rappelant que certaines préoccupations quant à l'effectivité des droits des personnes dont les données sont transférées depuis l'Union européenne vers les États-Unis.

Enfin, en 2018, j'ai également participé à l'élaboration de l'avis du Comité européen de la protection des données sur le projet de cadre juridique européen en matière d'accès aux preuves électroniques (dit « e-Evidence »). À la suite de l'adoption de cet avis en septembre, j'ai également pu aller le présenter au Parlement européen dans le cadre d'une audition par la commission LIBE. Mes collègues ont également présenté cet avis dans d'autres enceintes européennes, comme le Conseil de l'Europe.

LES PRINCIPALES ACTIVITÉS DE LA CNIL À L'ÉCHELLE EUROPÉENNE ET INTERNATIONALE

La CNIL au Comité Européen de la Protection des Données (CEPD)

L'année 2018 a été marquée au plan européen et international par l'entrée en application le 25 mai 2018 du RGPD et de la directive dite « police-justice »[2]. Ces textes instituent la création au plan européen d'un nouvel organe communautaire **le Comité Européen de la Protection des Données (« le comité») lequel succède au G29.**

Le Comité a pour mission de **garantir l'application cohérente de ces textes fondateurs**. Il peut, à ce titre, publier des recommandations, des lignes directrices, des bonnes pratiques, des avis destinés à clarifier l'interprétation des principes et à accompagner les entreprises, les pouvoirs publics et les individus dans la mise en œuvre de ces textes. Il a aussi la capacité, à la différence du G29, d'adopter des décisions contraignantes pour trancher les différends entre autorités de contrôle qui lui seraient soumis.

Le Comité est actuellement présidé par la Présidente de l'autorité de protection des données autrichienne, Andrea Jelinek. Lors de ces premiers mois d'existence, le Comité a tenu **5 séances plénières**. Ces plénières sont alimentées par les travaux d'une dizaine de groupes de travail en charge de thématiques définies.

Depuis le 25 mai, le Comité a poursuivi les travaux engagés par le G29 en reprenant pour son compte l'ensemble des lignes directrices que le G29 avait adopté sur un certain nombre de concepts clés ou de nouvelles obligations prévues par le Règlement qui font désormais partie de la doctrine du Comité.

La Comité a aussi adopté **une nouvelle série de lignes directrices** destinées à fournir une interprétation commune et un éclairage pratique pour accompagner les responsables de traitement ou sous-traitants, dans la mise en œuvre du Règlement.

Ainsi, la CNIL a participé activement à l'élaboration de cette nouvelle doctrine notamment en contribuant aux travaux sur les **dérogations** pour les transferts en dehors de l'Union européenne, sur la **transparence**, le **consentement**, l'**accréditation** en matière de certification et les critères de **certification**. La CNIL s'est également investie dans la préparation des lignes directrices sur le **champ d'application territorial** du Règlement qui sont actuellement ouvertes à consultation publique et pour la création d'un nouveau groupe de travail du comité dédié aux questions que soulève **l'utilisation des réseaux sociaux.**

Dans le cadre des missions du Comité à l'égard du législateur européen, la CNIL a fortement collaboré à la rédaction de l'avis du Comité sur le projet de cadre juridique européen en matière d'accès aux preuves électroniques (dit « **e-Evidence** ») proposé par la Commission européenne.

Le point sur les lignes directrices RGPD au 31/12/2018

Autorité chef de file	✓	DPIA et les traitements susceptibles d'engendrer des risques élevés	✓
Délégué à la protection des données personnelles	✓	Sanctions Administratives	✓
Profilage	✓	Dérogations transferts	✓
Notification de violations	✓	Certification	✓
Référentiel d'adéquation	✓	Accréditation	✓
Référentiel BCR responsables de traitement	✓	Transparence	✓
Référentiel BCR sous-traitants	✓	Consentement	✓
Portabilité	✓	Champ d'application territorial	💬
		Codes de conduite	✳

✓ Adoption définitive
💬 Consultation
✳ En cours

2 Directive sur la protection des données pour les traitements à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

La CNIL a aussi participé au travail de mise en cohérence des **projets de listes nationales** relatives aux opérations de traitements devant être soumis à une analyse d'impact sur la vie privée (PIA).

À noter en octobre 2018, la conduite de la seconde revue annuelle d'évaluation de la décision d'adéquation "Bouclier de protection de la vie privée" (***privacy shield***). Ainsi, plusieurs représentants du Comité dont la CNIL ont participé à cet exercice d'évaluation des garanties offertes par cet instrument, organisé à Bruxelles par la Commission européenne. Un projet de rapport a été rédigé et discuté en plénière du Comité en novembre. Son adoption est prévue pour janvier 2019.
La CNIL a aussi contribué de manière importante à l'avis du Comité sur le projet de décision d'adéquation du Japon de la Commission européenne. Ce projet de décision est le premier soumis par la Commission européenne sous l'empire du RGPD. L'avis du Comité a été adopté en décembre 2018. Pour formuler son avis, le Comité s'est appuyé sur le nouveau référentiel révisé et adopté en février 2018, lequel prend en compte l'arrêt de la CJUE[3] qui a conduit à l'annulation du Safe Harbor.

La mise en place de la coopération européenne sur les cas transfrontières

Le RGPD a institué au niveau européen un nouveau modèle de gouvernance et une série de mécanismes de coopération formels entre autorités nationales de protection des données, plus particulièrement pour les traitements dits transfrontaliers. Sur ces aspects, des outils et des procédures ont été mis en place durant l'année 2018 afin de rendre effectif ce nouveau cadre de coopération et organiser en pratique le travail des autorités.

En amont de l'entrée en application du RGPD, le Groupe de l'Article 29 (G29), que présidait la CNIL, avait déjà beaucoup travaillé pour permettre la mise en œuvre du nouveau cadre de coopération européen introduit par le Règlement dès le 25 mai 2018. Des lignes directrices, des procédures internes, un règlement intérieur et des enceintes d'échanges spécifiques ont ainsi été développés au sein du Comité européen de la protection des données (CEPD) pour faciliter la coopération notamment afin de préciser les mécanismes du guichet unique, de l'assistance mutuelle et des enquêtes conjointes ou encore pour établir les modalités d'adoption des positions du CEPD.

Chiffres clés 2018

568

cas introduits par les autorités dans la plateforme de coopération européenne IMI (un « cas » pouvant regrouper plusieurs dossiers liés, par exemple des réclamations similaires contre une même entreprise).

La CNIL est autorité chef de file pour **22** cas et autorité concernée pour

426 autres cas

dont **341** plaintes et **46** violations de données.

Le CEPD a adopté **26** avis dans le cadre du mécanisme de la cohérence et 4 lignes directrices relatives au RGPD.

Depuis le 25 mai, quelques projets de décisions ont été adoptés.

Dans ce contexte, l'année 2018 a permis à la CNIL de rendre ces mécanismes de coopération, procédures et outils opérationnels au plan interne. Ainsi, la CNIL s'est organisée en mettant en place des procédures d'échanges interservices et une instance de décision spécifique sur ces questions pour permettre un suivi des cas transmis par les autorités homologues, aiguiller les cas européens et assurer une information transversale sur les procédures qu'elle initie. Des référents spécifiques ont par ailleurs été désignés et des outils dédiés sont en cours de développement pour permettre une veille efficace du nombre important de cas.

Aussi, la coopération entre la CNIL et ses homologues a pu être rendue effective dès le 25 mai 2018. Depuis cette date, les autorités de protection des données européennes disposent d'une plateforme informatique dédiée, dénommé IMI (Internal Market Information System), mise à disposition par la Commission européenne, leur permettant d'échanger des informations et de communiquer leurs positions dans le cadre des différentes procédures de coopération mentionnées ci-dessus.

Dans ce cadre-là il est essentiel de déterminer d'abord qui est l'autorité chef de file et qui sont les autorités concernées. Dans un premier temps, l'essentiel des cas introduits a donc porté sur la désignation des autorités compétentes et chef de file, et depuis la fin de l'année dernière, à l'issue des premières instructions menées, les premiers projets de décisions ont été soumis au mécanisme de coopération.

Compte tenu du temps normal d'examen des cas, il est normal que les décisions n'aient pas été adoptées plus tôt. L'année 2019 verra l'adoption de plus de décisions, et dans l'hypothèse de cas plus sensibles, les premières décisions du Comité européen de la protection des données pour trancher d'éventuels différends entre autorités de contrôle nationales sur les décisions finales à adopter ne seront sans doute pas adoptées avant l'été.

Outre les échanges sur les cas, les autorités de protection des données ont poursuivi leurs échanges réguliers, notamment au travers de demandes d'assistance mutuelle. La CNIL a ainsi échangé avec ses homologues dans le cadre de l'instruction des plaintes des deux associations « La Quadrature du Net » et « None Of Your Business » contre Google pour lesquelles il n'était pas encore possible de mettre en œuvre le mécanisme du guichet unique (Google ne disposant pas à ce moment-là d'établissement principal en Europe).

3 C-362/14, du 6 octobre 2015 de la Cour de Justice de l'Union Européenne (« arrêt Schrems »).

La CNIL au sein du réseau international des commissaires à la protection des données

En 2018, la CNIL a assuré la Présidence et le secrétariat de la Conférence Internationale des Commissaires à la Protection des Données et à la Vie Privée (ICDPPC). Une année charnière pour ce réseau qui rassemble au niveau international plus de 120 autorités de protection des données et qui, à l'initiative de la CNIL, s'est engagé dans un processus de réflexion sur son avenir avec d'abord le lancement d'une consultation stratégique auprès de ses membres et l'organisation d'une consultation publique ouverte à toutes les parties prenantes externes. Ce processus a conduit à l'adoption, lors de la réunion annuelle d'octobre 2018, d'une feuille de route sur l'avenir de la Conférence Internationale, entérinant les recommandations clés et les actions à mener par la Conférence, pour devenir une organisation plus permanente et structurée.

Cette réforme de l'organisation, le renforcement de son identité et l'amélioration de sa gouvernance, ainsi que la mise en place d'éléments et processus plus pérennes, s'inscrivent dans une volonté de positionner la Conférence sur la scène mondiale en tant qu'organisation de référence dans les débats relatifs à la gouvernance du numérique et à l'accompagnement des évolutions technologiques dans ce domaine.

En 2018, la Conférence Internationale s'est notamment positionnée sur plusieurs sujets majeurs avec l'adoption de deux résolutions initiées par la CNIL : l'une sur l'éthique et la protection des données dans l'intelligence artificielle, l'autre sur l'éducation au numérique et les plateformes d'éducation en ligne.

La francophonie

Dès sa création en 2007, l'Association francophone des autorités de protection des données personnelles (AFAPDP), dont le secrétariat général est assuré par la CNIL. Elle rassemble les autorités existantes et les gouvernements intéressés par la mise en place d'une loi de protection des données qui partagent une langue, mais aussi une tradition juridique et des valeurs communes. En 2018, 67 des 88 États et Gouvernements francophones disposent dans leur arsenal juridique de dispositions relatives à la protection des données personnelles et 52 d'une autorité compétente en la matière. L'association a pour objectif de favoriser leurs échanges et donner une voix à la spécificité francophone, tout en reconnaissant les différences juridiques et culturelles au sein de ses 20 membres. La Commission nationale de protection des données (CNPD) du Cap-Vert est la dernière autorité à avoir rejoint l'AFAPDP.

L'année 2018 a été marquée par une immersion dans le rôle des nouveaux médias sociaux dans les processus électoraux, thématique de la réunion annuelle des membres de l'AFAPDP, qui s'est déroulée dans les locaux de la CNIL le 19 octobre. Les travaux ont bénéficié de l'expertise du Réseau des compétences électorales francophones (RECEF), de Reporters sans frontières (RSF) et du Réseau francophone des régulateurs des médias (REFRAM). Un groupe de travail est en train d'être constitué au sein de l'AFAPDP, en coopération avec le RECEF, le REFRAM et l'Organisation internationale de la Francophonie (OIF), afin de poursuivre les réflexions sur le sujet.

Les membres de l'AFAPDP ont par ailleurs adopté, à l'occasion de la 12ème Assemblée générale, une résolution sur la propriété des données, rappelant que les données personnelles constituent des éléments de la personne humaine, qui dispose, dès lors, de droits inaliénables sur celles-ci.

Pour en savoir plus : www.afapdp.org / twitter : @afapdp

12ème Assemblée générale de l'AFAPDP à la CNIL, Paris, le 18 octobre 2019

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, peut prononcer diverses sanctions dont des sanctions pécuniaires d'un montant maximal de 20 millions d'euros ou 4 % du chiffre d'affaires mondial. Ces sanctions peuvent être rendues publiques.

Rodolphe
Juriste

et Audrey
Assistante au service des sanctions et du contentieux

Le service est chargé de mettre en œuvre l'action « répressive » de la CNIL. À ce titre, les juristes du service assurent la préparation des mises en demeure décidées par la Présidente de la CNIL. Nous analysons ensuite la mise en conformité des organismes visés par la mise en demeure, pour proposer à la Présidente de la CNIL les suites qui peuvent être apportées à la procédure, par exemple la clôture quand les actions requises ont été prises par l'organisme. Lorsque la Présidente de la CNIL initie une procédure de sanction en désignant un rapporteur, nous l'assistons dans la préparation de son rapport de sanction qui sera notifié à l'organisme poursuivi, et dans les échanges qui s'en suivent. Enfin, lorsqu'une décision de la CNIL est contestée devant le Conseil d'État, nous assurons la préparation des mémoires en défense. Enfin, nous préparons les réponses à apporter aux demandes d'avis des autorités judiciaires. Pour mener à bien l'ensemble de ces missions, nous travaillons en étroite collaboration avec le service des plaintes et les services des contrôles.

Les deux assistantes ont un rôle clé au sein du service. Nous sommes garantes du bon déroulement des procédures et assurons différentes tâches centrales pour le fonctionnement du service. Nous procédons ainsi aux notifications puis au suivi des procédures en cours, en veillant notamment au respect des délais. Nous avons un rôle d'alerte auprès des juristes. Dans le cadre des procédures de sanction, nous sommes également en charge de recevoir les responsables mis en cause ou leurs conseils afin de leur permettre de consulter le dossier et leur fournir copie des pièces. Nous sommes également chargées d'organiser la séance de la formation restreinte.

CONTRÔLER

La CNIL a effectué 310 contrôles au cours de l'année 2018, ce qui est conforme à ce qu'elle s'était fixée lors de l'annonce de son programme annuel des contrôles pour 2018.

L'entrée en application du RGPD ne change pas la manière dont les contrôles de la CNIL sont effectués. La CNIL continue de vérifier, sur place, en ligne ou sur audition, la conformité des traitements de données à caractère personnel, aux dispositions de la loi Informatique et Libertés et du RGPD. Ces vérifications concernent les entreprises, les administrations, les collectivités locales et les associations.

Deux nouveautés ont néanmoins été introduites lors de la modification de la loi Informatique et Libertés le 20 juin 2018. Désormais, la CNIL peut d'une part, « inviter » des agents d'autres autorités de protection des données de l'Union européenne à participer à des contrôles sur le territoire français, d'autre part, effectuer des contrôles en ligne sous identité d'emprunt.

L'origine des contrôles réalisés est identique à celle des années précédentes. La CNIL continue d'intervenir sur la base de plaintes reçues et dans le cadre du programme annuel qu'elle s'est fixé pour enquêter sur des grands secteurs d'activité. Elle fait preuve également de réactivité en procédant à des contrôles de sa propre initiative en fonction des sujets d'actualité identifiés au travers d'une veille. Elle procède enfin à des contrôles faisant suite à des procédures de mise en demeure ou de sanction, ou des procédures closes, afin de vérifier l'effectivité des mesures correctrices annoncées par les organismes.

La CNIL a réalisé 51 contrôles en ligne au cours de l'année, parfois en urgence sur des violations de données issues de failles de sécurité, ou alors comme préalable ou complément à des contrôles sur place. Comme en 2017, la CNIL a également continué à procéder, sur la base d'une soixantaine de signalements, à des vérifications en ligne hors contrôle afin de faire rapidement procéder à la sécurisation de systèmes d'information.

Par ailleurs, compte tenu de l'entrée en application du RGPD et d'interrogations sur le cadre juridique applicable, la CNIL a réduit pour cette année le nombre de contrôles portant sur des dispositifs de vidéoprotection, c'est-à-dire situés dans des lieux ouverts au public.

Enfin, à l'image des années précédentes, elle s'est à nouveau investie dans le *Sweep Day* organisé par le *Global Privacy Enforcement Network* (GPEN) pour mener une action coordonnée de vérifications auprès d'organismes avec d'autres autorités de protection des données. Le sujet choisi cette année était la préparation des sous-traitants au RGPD.

Les actions menées par la CNIL en 2018 au titre de ses pouvoirs de contrôles ont notamment porté sur trois axes :

1. La sécurité des données

Comme en 2017, la CNIL a continué à recevoir un grand nombre de signalements concernant des failles de sécurité. Pour chacun d'entre eux, les services vérifient la réalité de l'incident de sécurité et prennent des mesures afin qu'il soit résolu au plus vite. Ce sont presque 90 violations de données qui ont pu être résolues, soit par une prise de contact immédiate avec le responsable de traitement, soit, pour les cas les plus graves, par des contrôles, des mises en demeure ou des sanctions. La majorité des sanctions prononcées en 2018 par la formation restreinte de la CNIL a concerné des incidents de sécurité (7 sur 10). Figurent parmi les organismes sanctionnés sur ce thème : Uber, Bouygues Télécom, Dailymotion ou Optical Center. Ce n'est pas l'incident en tant que tel que la CNIL a sanctionné, mais les carences et insuffisances dans les mesures de sécurité dont cet incident n'a été qu'une traduction.

310
CONTRÔLES

DONT

204
CONTRÔLES SUR PLACE

51
CONTRÔLES EN LIGNE

51
CONTRÔLES SUR PIÈCE

20
CONTRÔLES VIDÉOPROTECTION

INFOSPLUS

L'origine des contrôles

57%
sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;

16%
résultent du programme annuel décidé par les membres de la Commission ;

22%
s'inscrivent dans le cadre de l'instruction de plaintes ou de signalements ;

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

2. La surveillance des usagers sur la voie publique

Au travers de différentes thématiques de contrôle, la CNIL s'est intéressée au cours de l'année 2018 aux données traitées dans le cadre du contrôle des usagers sur la voie publique par les forces de l'ordre. Elle a par exemple effectué des contrôles des radars-tronçons sur les routes. L'objectif a été dans ce cadre de vérifier la durée de conservation des plaques d'immatriculation, l'ensemble des voitures transitant sur la route faisant l'objet d'un relevé, ainsi que les mesures de sécurité apportées. Elle a également procédé à des contrôles des dispositifs de caméras individuelles portées par les forces de l'ordre lors de leurs interventions, afin de vérifier le respect des dispositions légales encadrant la mise en œuvre de ces traitements de données. Les contrôles ont révélé des améliorations à apporter aux durées de conservation et à la sécurité des données. Enfin, elle a mené des contrôles afin de vérifier les conditions dans lesquelles les relevés d'infractions au stationnement gênant (à distinguer du stationnement payant) étaient effectués par les communes grâce à des dispositifs de lecture automatisée des plaques d'immatriculation dans ce cadre.

3. L'utilisation des services en ligne au quotidien

Sur la base de plaintes et de signalements dans les médias, la CNIL a conduit plusieurs séries de contrôles en lien avec des services en ligne du « quotidien », en plus de la quinzaine de contrôles menés sur des sites de commerce en ligne « classiques ». La CNIL a ainsi vérifié des sites permettant de passer son permis de conduire en ligne, d'organiser des obsèques, de rédiger des contrats, de réserver des restaurants ainsi que des plateformes de financement participatif ou *crowdfunding*. La CNIL s'est principalement attachée à contrôler les conditions d'information, de sécurité et les durées de conservation.

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

Bilans du programme annuel 2017

Ces bilans font suite aux premiers éléments présentés dans le rapport d'activité 2017.

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 des 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.

Une série de contrôles a été menée 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. Dans ce cadre, la CNIL a souhaité principalement s'assurer du respect des règles de confidentialité des données de santé et du secret médical dont il est fait état dans le pack de conformité « Assurance ».

Les contrôles ont révélé que les sociétés d'assurance ont, dans la majorité des cas, porté à la connaissance des prospects et des assurés les mentions d'information prévues par la loi Informatique et Libertés. Toutefois, les vérifications effectuées ont permis de constater qu'une grande partie d'entre elles ne recueille pas de manière satisfaisante le consentement exprès des personnes pour le traitement de leurs données de santé. De plus, certaines sociétés conservent des données plus longtemps que nécessaire ou doivent prendre des actions afin d'améliorer la sécurité des données traitées.

Compte tenu de ces éléments, la Présidente de la CNIL a adopté deux mises en demeure afin d'obtenir une mise en conformité des organismes concernés. Dans les cas où les manquements étaient de moindre importance, des courriers de rappel à l'observation de la loi ont été adressés.

Enfin, s'agissant des conditions d'accès aux données de santé, les contrôles ont pu démontrer que, pour la souscription d'un contrat d'assurance, certains personnels non médicaux sont amenés, dans le cadre de leurs fonctions, à accéder aux données de santé aux fins d'appréciation du risque. Ces derniers, spécifiquement habilités, sont placés sous l'autorité fonctionnelle du médecin-conseil de l'assureur et formés à la confidentialité médicale. Des travaux sont en cours avec les représentants du secteur de l'assurance et notamment la Fédération Française de l'Assurance (FFA) afin de parfaitement encadrer sur les pratiques du secteur sur ce point.

Les fichiers de renseignement

Le programme de contrôle des fichiers de renseignement entamé en 2017 s'est poursuivi en 2018. Au total, 5 fichiers ont fait l'objet de vérifications :

- les fichiers PASP et GIPASP, dits de renseignement territorial, mis en œuvre par les services centraux et locaux de police et de gendarmerie,
- le fichier EASP qui a pour objet de centraliser et conserver le résultat des enquêtes administratives réalisées par les services de police à la demande du Préfet compétent,
- le fichier STARTRAC mis en œuvre par le service TRACFIN du ministère de l'Action et des Comptes publics dont l'objectif est la lutte contre le blanchiment d'argent et le financement du terrorisme,
- Le fichier FSPRT, mis en œuvre par le ministère de l'Intérieur, qui centralise les informations relatives aux personnes signalées et suivies pour radicalisation à caractère terroriste.

Une quarantaine de missions de vérification sur place ont été menées tant auprès des services gestionnaires de chaque fichier qu'auprès des services utilisateurs sur l'ensemble du territoire.

Les investigations se sont concentrées sur les modalités de gestion des fichiers par les services centraux et d'exploitation par leurs utilisateurs. En particulier, les doctrines d'utilisation, la pertinence des données enregistrées, le respect des durées de conservation, les mesures de

sécurité ainsi que les modalités de partage des informations ont fait l'objet de constats précis. Des échanges ont eu lieu avec le ministère de l'intérieur et le ministère de l'Action et des Comptes publics concernant un certain nombre de points de conformité mis en lumière par ces contrôles.

Premiers éléments sur le programme annuel 2018

Ces premiers éléments portent sur les contrôles réalisés dans le cadre du programme annuel des contrôles pour 2018, actuellement en cours d'instruction et qui feront l'objet d'un bilan définitif dans le rapport d'activité 2019.

Les pièces justificatives demandées par les agences immobilières

La difficulté d'accès au logement est une des préoccupations majeures de notre époque. À cet égard, le décret n° 2015-1437 du 5 novembre 2015 entend renforcer les droits des locataires en fixant la liste limitative des pièces pouvant être demandées aux candidats à la location ainsi qu'à leur caution.
Trois ans après l'adoption de ce décret, la CNIL a souhaité s'assurer de la conformité des agences immobilières aux règles énoncées par ce texte.
Compte tenu du nombre important d'agences immobilières présentes sur le territoire national, la CNIL a décidé de contrôler tant des agences immobilières structurées sous la forme d'un réseau de franchises ou d'établissements secondaires que des agences indépendantes de moindre envergure. Le choix a également été fait de couvrir l'ensemble du territoire national, de manière à prendre en compte des grandes agglomérations pour lesquelles le marché de l'immobilier est tendu ainsi que des villes de taille moyenne.
D'une manière générale, ces contrôles ont mis en évidence le fait que le cadre juridique prévu dans le décret de 2015 fixant la liste limitative des pièces pouvant être demandées aux candidats est bien connu des agences contrôlées. Ainsi, les vérifications aléatoires de plusieurs dossiers de candidatures n'ont pas révélé la présence de pièces non prévues dans le décret. La CNIL poursuit son analyse afin de déterminer si les durées de conservation et les mesures de sécurité mises en place sont conformes aux exigences légales.

Les traitements liés au recrutement

Avec l'essor du *big data* et de l'intelligence artificielle, le secteur du recrutement mobilise de nouveaux outils destinés notamment à mieux connaître les candidats et prédire leur performance sur un poste. Ces nouvelles méthodes impliquent de mettre en œuvre des traitements de données à caractère personnel à grande échelle.
La CNIL a réalisé des contrôles auprès d'organismes ayant recours à des algorithmes de sélection et d'analyse de profils de candidats afin de s'assurer de la proportionnalité de tels traitements, notamment en lien avec le respect des droits des personnes concernées. Les investigations ont également porté sur la prise de décision automatisée dans un processus de profilage, sur l'information des personnes concernées, les durées de conservation et les mesures de sécurité et de confidentialité des données traitées.
Les contrôles ont concerné principalement les prestataires proposant des solutions innovantes fonctionnant sur le modèle SaaS (« *Software as a Service* » ou logiciel en tant que service) mais également des sociétés utilisant ce type de prestations. Ces contrôles ont relevé une diversité de méthodes utilisées, qu'il s'agisse d'algorithmes d'analyse de CV ou de profils professionnels en ligne, de tests psychologiques ou de comportement, pour sélectionner des profils de candidats.
Il ressort des premières constatations que les organismes contrôlés ont pris conscience de la sensibilité des données traitées et des nouvelles obligations issues du RGPD. Pour autant, certaines pratiques posent difficulté au regard notamment de l'information des personnes, du caractère automatisé de la prise de décision par des algorithmes et du volume important de données collectées.
La CNIL poursuit ses contrôles et son analyse afin de déterminer si les garanties apportées sont suffisantes au regard des exigences légales.

Les traitements liés au stationnement payant

La loi de modernisation de l'action publique territoriale et d'affirmation des métropoles, dite loi « MAPTAM », a modifié, à compter de janvier 2018, les règles de gestion du stationnement payant sur la voie publique.
Depuis son entrée en vigueur, le stationnement payant n'est plus une infraction pénale. Il relève désormais intégralement des collectivités territoriales qui peuvent confier à des prestataires privés la collecte de la redevance de stationnement, le contrôle du paiement de cette redevance et l'établissement des forfaits de post-stationnement (FPS) dus en cas d'absence ou d'insuffisance de paiement de la redevance de stationnement. Ces FPS remplacent ainsi les amendes pénales qui étaient infligées avant la réforme.
La possibilité de confier certaines de ces missions à des organismes tiers de droit privé a favorisé l'émergence de nouveaux services, tels que les dispositifs de lecture automatisée de plaques d'immatriculation (LAPI), les tickets de stationnement électroniques ou encore les applications mobiles permettant de gérer à distance le paiement du stationnement.

Ces nouveaux services reposent sur la collecte d'un grand nombre de données personnelles, susceptibles de révéler des informations détaillées de la vie privée des individus. Afin de vérifier les conditions dans lesquelles ils sont mis en œuvre, la CNIL a décidé de mener des contrôles auprès de l'ensemble de la chaîne des acteurs impliqués : les collectivités territoriales, les sociétés proposant des solutions de paiement et les prestataires d'établissement du FPS.

Les investigations sont toujours en cours et portent en particulier sur la pertinence des données fournies et recueillies, l'information des usagers, les modalités de conservation des données ainsi que sur les mesures sécurité.

GROS PLAN

Le recours à la vidéosurveillance dans les écoles

En 2018, la Présidente de la CNIL a adopté deux mises en demeure publiques à l'encontre d'écoles d'ingénieurs ayant recours à des dispositifs intrusifs de vidéosurveillance, l'association « 42 » et l'Institut des techniques informatiques et commerciales (l'ITIC).

Dans les deux cas, la CNIL a procédé à des contrôles sur place, soit à la suite d'une plainte, soit à la suite d'informations parues dans les médias.

Elle a notamment constaté que des caméras filmaient en permanence les espaces de travail des étudiants, des bureaux dédiés au personnel administratif ainsi que des lieux de vie telle que la cafétéria. En outre, les personnes filmées n'étaient pas correctement informées et l'accès aux images n'était pas suffisamment sécurisé. Sur ce point, au sein de l'association « 42 », la plupart des images issues de la vidéosurveillance étaient accessibles en temps réel aux étudiants sur le réseau intranet de l'école à partir de leur espace personnel.

En conséquence, il a été demandé à ces écoles de redimensionner leur système de vidéosurveillance en cessant de filmer en permanence les salles de cours et lieux de vie. Il leur a été rappelé que la CNIL considère comme excessif tout système de vidéosurveillance plaçant des salariés ou des étudiants sous surveillance constante. Il a aussi été souligné que l'accès aux images issues du dispositif devait être strictement réservé aux personnes habilitées, en raison de leur fonction au sein de l'école.

Ces mises en demeure ont été rendues publiques compte tenu du caractère intrusif du dispositif, de la nécessité d'informer les nombreux étudiants de ces écoles et de rappeler leurs obligations aux responsables d'établissements d'enseignement supérieur déployant de tels systèmes de vidéosurveillance.

Bilan des actions coordonnées au niveau européen et international

Sweep day : la responsabilisation des acteurs en matière de protection des données

En 2018, la CNIL a participé pour la sixième fois aux actions menées par les autorités européennes et internationales de protection des données dans le cadre de l'opération *Sweep* dans le cadre du *Global Privacy Enforcement Network* (GPEN - réseau d'organismes agissant au sein de l'OCDE pour la protection de la vie privée).

L'édition 2018 s'est concentrée sur la responsabilisation des acteurs en matière de protection des données (*Privacy accountability*), principe consacré par le RGPD. En pratique, il s'est agi d'identifier les mesures et outils internes mis en place par les organismes pour garantir la protection des données traitées.

Au niveau national, la CNIL a choisi de s'intéresser plus particulièrement aux mécanismes mis en œuvre par les sous-traitants pour répondre à leurs nouvelles obligations résultant de l'entrée en application du RGPD. Les sous-traitants ont un rôle essentiel auprès des responsables de traitement notamment sur les questions de sécurité des données.

Cette thématique a ainsi permis d'appréhender le niveau de maturité du secteur sur le sujet de la protection des données. Cet audit a été conduit auprès d'un panel d'organismes diversifié : intégrateurs de logiciel et hébergeurs, situés sur le territoire français, comprenant tant des TPE spécialisées que des acteurs majeurs offrant une gamme de services plus large.

En synthèse, l'opération *Sweep* montre que le secteur des prestataires de service en informatique a globalement pris conscience des évolutions attendues à la suite de l'entrée en application du RGPD, mais que des efforts sont encore nécessaires pour répondre aux exigences du texte.

Les plus :

- l'ensemble des organismes sollicités ont mené une analyse afin de déterminer la nécessité de désigner un délégué à la protection des données (DPO) ;
- la grande majorité des entreprises a également étudié la question de leur statut au regard du RGPD, à savoir leur qualité de sous-traitant ou de co-responsable de traitement, la plupart en se basant sur le guide du sous-traitant de la CNIL.

Les moins :

- certaines sociétés interrogées ont mentionné n'avoir mis en place aucune procédure de gestion d'incident de sécurité ;
- peu d'acteurs ont eu l'occasion d'assister leurs clients dans l'élaboration d'analyses d'impact (PIA) ou de procédures de réponse à l'exercice des droits des personnes ;
- plusieurs acteurs ont mis en avant leur difficulté à qualifier leur statut de sous-traitant au sens du RGPD.

La question du rôle et de la responsabilité des sous-traitants à l'ère du RPD fera l'objet de vérifications approfondies au cours de l'année à venir.

SANCTIONNER

La Présidente de la CNIL a prononcé : 49 mises en demeure dont 13 ont été rendues publiques. La formation restreinte a pour sa part prononcé : 11 sanctions (10 sanctions pécuniaires dont 9 publiques ; 1 avertissement non public et 1 non-lieu à sanctionner).

Les mises en demeure

L'année 2018 a été marquée par l'augmentation substantielle du nombre de mises en demeure rendues publiques.
En effet, parmi les 48 mises en demeure prononcées cette année, 13 ont fait l'objet d'une mesure de publicité, qui est décidée par le bureau de la CNIL (composé de la Présidente et des deux Vice-présidents).

Deux secteurs ont été particulièrement concernés :

- celui des assurances, avec 5 décisions adoptées à l'encontre des sociétés Auxia, Humanis Assurances, Grand Est Mutuelle, Malakoff Mederic Mutuelle et Mutuelle Humanis Nationale, pour détournement de finalité des données des assurés, utilisées à des fins de prospection commerciale ;
- celui des entreprises spécialisées dans le ciblage publicitaire par le biais d'une technologie (SDK) installée dans des applications mobiles. Ces mises en demeure visaient les sociétés Fidzup, Teemo, Singlespot et Vectaury.

Deux mises en demeure publiques ont également été prononcées envers des établissements d'enseignement supérieur (Itic et Association 42), pour vidéosurveillance excessive.

Enfin, la CNAM et Direct Énergie ont également été visés par cette mesure, respectivement pour des manquements à la sécurité des données des assurés sociaux et pour une absence de consentement concernant les données issues du compteur communicant Linky.

De manière plus générale, les différentes mises en demeure adoptées par la Présidente de la CNIL font suite à :

- l'instruction de plaintes (19 %) ;
- la réalisation de contrôles sur le fondement de plaintes (19 %) ;
- des missions effectuées sur la base du programme annuel des contrôles défini par la CNIL, ou effectués à l'initiative de la CNIL en lien avec l'actualité (60 %) ;
- pour la première fois, une notification de violation de données à caractère personnel (2 %).

Certaines de ces mises en demeure ont donné lieu à des clôtures, également rendues publiques.

Les mesures prononcées par la formation restreinte

La formation restreinte de la CNIL a prononcé :

- 10 sanctions pécuniaires dont 9 publiques ;
- 1 avertissement non public ;
- 1 non-lieu à sanctionner.

Cette année, 7 sanctions pécuniaires prononcées par la formation restreinte concernaient des atteintes à la sécurité des données personnelles.

Les sanctions adoptées concernent des faits qui se sont déroulés avant l'entrée en application du RGPD. Elles ont été prononcées sur le fondement de la version antérieure au RGPD de la loi Informatique et Libertés issue de la loi du 7 octobre 2016 pour une République numérique, qui permettait déjà un accroissement des montants de sanction en fixant un plafond à 3 millions d'euros.

Les recours devant le Conseil d'État : rappel de l'obligation de coopération des organismes mis en demeure

Dans une décision rendue le 6 juin 2018, le Conseil d'État a rejeté la requête d'une société qui demandait l'annulation d'une sanction pécuniaire prononcée à son encontre par la formation restreinte de la CNIL.

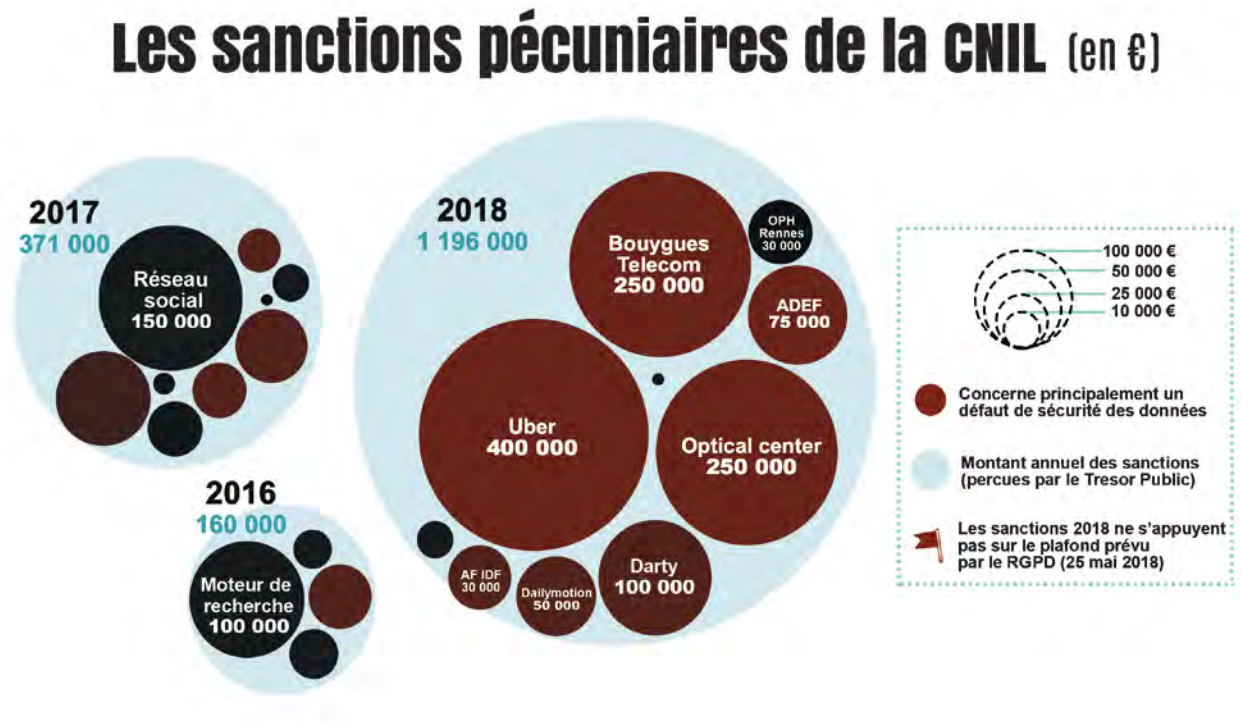
La société avait été mise en demeure par la Présidente de la CNIL en juin 2016 de se conformer dans un délai de 3 mois à la loi Informatique et Libertés.
En l'absence de réponse de sa part, une procédure de sanction avait été engagée. En mai 2017, la formation restreinte de la CNIL avait alors prononcé à son encontre une sanction pécuniaire en relevant notamment qu'elle n'avait pas répondu à la mise en demeure, et ce malgré une lettre de relance.
Devant le Conseil d'État, la société faisait notamment valoir que la CNIL n'avait pas effectué de nouveau contrôle pour constater que, à l'issue du délai fixé par la mise en demeure, elle avait mis en place des correctifs.

Dans son arrêt du 6 juin 2018, le Conseil d'État a confirmé l'intégralité de la décision rendue par la formation restreinte. À cette occasion, il a ainsi précisé que, dans le contexte d'une mise en demeure, la CNIL n'était pas tenue de procéder à un nouveau contrôle pour apprécier la persistance des manquements, mais qu'il revenait aux personnes mises en demeure de communiquer tous les éléments permettant à la CNIL d'apprécier la mise en conformité.

Le Conseil d'État a également indiqué que s'il apparaissait au cours de la procédure de sanction que le responsable de traitement avait remédié aux manquements constatés dans la mise en demeure, cette circonstance ne faisait pas obstacle au prononcé d'une sanction pour méconnaissance de l'obligation de coopérer avec la CNIL, résultant de l'article 21 de la loi du 6 janvier 1978 modifiée.

49
MISES EN DEMEURE, DONT
13
publiques

10
SANCTIONS PÉCUNIAIRES, DONT
9
publiques



INFOSPLUS

Actualisation du protocole de coopération entre la CNIL et la DGCCRF

Le 31 janvier 2019, la DGCCRF et la CNIL ont signé un nouveau protocole de coopération. Les deux autorités ont décidé de mettre à jour la convention initialement signée en janvier 2011 afin de renforcer leur collaboration et de l'adapter aux nouveaux enjeux numériques.

En 2019, les deux autorités ont décidé de poursuivre leur coopération en vue notamment de :

- mieux sensibiliser les consommateurs aux risques encourus lors de la communication de leurs données personnelles et diffuser les bonnes pratiques mises en œuvre par les professionnels ;
- faciliter l'échange d'informations relatives au non-respect du droit de la consommation et de la protection des données personnelles des consommateurs ;
- réaliser des contrôles communs ;
- porter conjointement des propositions d'actions au niveau européen ;
- mutualiser les expertises, notamment en ce qui concerne les outils d'enquête ;
- partager leurs analyses sur les évolutions du cadre législatif et réglementaire en matière de protection des consommateurs et de leurs données personnelles.

INFOSPLUS

Mises en demeure de quatre « data brokers » spécialisés dans les applications mobiles

En 2018, la Présidente de la CNIL a mis en demeure quatre sociétés (Fidzup, Teemo, Singlespot et Vectaury) pour absence de consentement des personnes au traitement de leurs données de géolocalisation à des fins de ciblage publicitaire.

Ces quatre sociétés ont recours à des traceurs, dénommés « SDK », qui sont intégrés dans le code d'applications mobiles de sociétés partenaires et qui permettent de collecter les données de géolocalisation des utilisateurs de smartphones. Ces données sont croisées avec l'identifiant publicitaire de chaque appareil, qui permet d'identifier celui-ci de façon stable dans le temps.

Ces informations permettent ainsi aux sociétés de connaître les lieux où les personnes se sont rendues et notamment de savoir si elles ont fréquenté un des magasins de leurs clients ou d'un de leurs concurrents. L'objectif est d'afficher, grâce aux données collectées, des publicités ciblées sur les téléphones des personnes afin de les attirer dans les magasins de leurs clients.

Dans le cadre de contrôles effectués en 2017 et 2018, la CNIL a constaté que les sociétés collectaient et traitaient les données des personnes sans avoir valablement recueilli leur consentement et sans les avoir correctement informées.

La Présidente de la CNIL a en effet relevé que les personnes n'étaient pas informées, lors du téléchargement des applications mobiles, qu'un SDK y était intégré et qu'il permettait de collecter leurs données de géolocalisation. Elle a notamment rappelé que l'information des personnes doit être effectuée avant toute collecte des données des personnes.

Les mises en demeure ont été rendues publiques afin que les personnes en soient informées et qu'elles soient mises en mesure de garder le contrôle de leurs données. La technicité de ces systèmes rend ces traitements largement inconnus du grand public, alors même qu'ils touchent une part importante de la population française, en possession d'un smartphone. En outre, ces traitements utilisent des données de géolocalisation et ils sont donc particulièrement intrusifs puisqu'ils permettent de connaître précisément les déplacements des personnes et leurs habitudes. La CNIL est particulièrement vigilante vis-à-vis des traitements de cette nature.

Les réponses de trois de ces sociétés (Fidzup, Teemo, Singlespot), fournies en 2018, ont permis de clore les procédures de mise en demeure engagées à leur encontre. En effet, les sociétés ont pris des mesures visant à mettre en place une plateforme de gestion des consentements (CMP - Consent management platform) lors de l'installation des applications mobiles, avant la collecte des données.

Ces bannières qui s'affichent lors de l'installation de l'application contiennent des fonctionnalités permettant aux personnes d'« accepter » ou de « refuser » que leurs données de géolocalisation soient traitées à des fins de publicité ciblée. Les personnes sont désormais informées, avant toute collecte de leurs données de géolocalisation, de la finalité du traitement réalisé grâce aux SDK, de l'identité des responsables de traitement et des données collectées.

Les bannières informent également les personnes, conformément au RGPD, qu'elles peuvent retirer leur consentement à tout moment, celui-ci devant être aussi simple à retirer qu'à donner.

Enfin, si le recueil du consentement des personnes a été considéré comme conforme au RGPD, il est cependant important de relever que la Présidente ne s'est pas prononcée sur la conformité des conditions de recueil du consentement pour les autres finalités présentées sur les bannières utilisées par les sociétés, telles que « le stockage et l'accès aux données » ou encore la « personnalisation ».

Concernant la société Vectaury, la mise en demeure a également fait l'objet d'une clôture. Cette procédure a été initiée postérieurement aux trois autres, et elle contenait une problématique propre. Outre les SDK intégrés aux applications de ses éditeurs partenaires, la société Vectaury recevait et conservait des *bid requests*, qui sont des offres d'enchère en temps réel d'espace pour encarts publicitaires insérés dans des applications ne contenant pas son SDK. Ces *bid requests* contenaient des données à caractère personnel, et notamment des données de géolocalisation. Leur nombre très important permettait à la société Vectaury d'affiner le profilage réalisé sur les profils des personnes dont provenaient les données. Là aussi, le consentement des personnes n'était pas valablement recueilli.

FOCUS

Les nouveautés introduites par le RGPD et la loi Informatique et Libertés modifiée

De nouvelles mesures correctrices

L'article 58.2 du RGPD liste les mesures qui peuvent être prononcées par les autorités de contrôle en cas de méconnaissance par un responsable de traitement ou un sous-traitant de ses obligations.

Parmi ces mesures certaines existaient déjà dans la précédente loi Informatique et Libertés. C'est le cas, par exemple, des mises en demeure, de l'interdiction d'un traitement, ou de la sanction pécuniaire.

D'autres sont nouvelles, comme la possibilité d'assortir l'injonction de mettre en conformité le traitement d'une astreinte financière. La loi Informatique et Libertés modifiée précise qui du Président de la CNIL ou de la formation restreinte a le pouvoir d'adopter les mesures.

Le Président de la CNIL peut désormais :

- avertir un responsable de traitement ou un sous-traitant qu'une opération de traitement est susceptible de violer les dispositions réglementaires ;
- ordonner au responsable de traitement de communiquer à la personne concernée une violation de données à caractère personnel.

La formation restreinte peut quant à elle :

- prononcer une injonction de mettre en conformité le traitement avec les dispositions règlementaire. Cette injonction peut être assortie d'une astreinte financière journalière ;
- retirer une certification ou ordonner à l'organisme de certification de retirer la certification accordée ;
- suspendre partiellement ou temporairement la décision d'approbation des règles d'entreprises contraignantes.

Enfin, la possibilité de prononcer directement une sanction, y compris pécuniaire, sans passer par l'étape préalable de la mise en demeure est confirmée. La CNIL peut choisir, en fonction des circonstances, la ou les mesure correctrices qu'elle estimera appropriées. Ces mesures peuvent être combinées entre elles et être précédées ou non d'une mise en demeure.

Des amendes administratives « dissuasives »

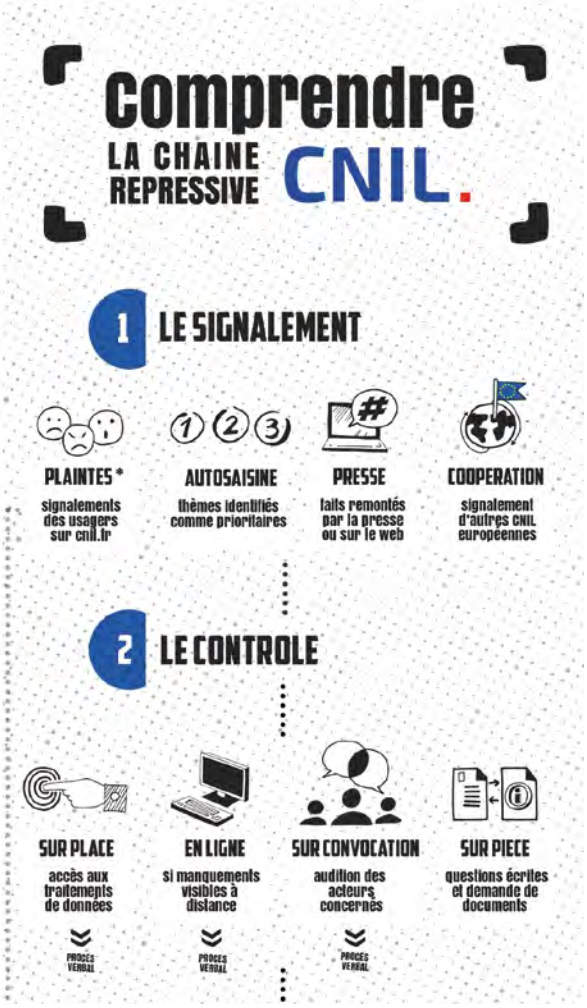
De nouveaux montants pour les sanctions pécuniaires sont désormais définis, sur la base de critères détaillés dans le RGPD.

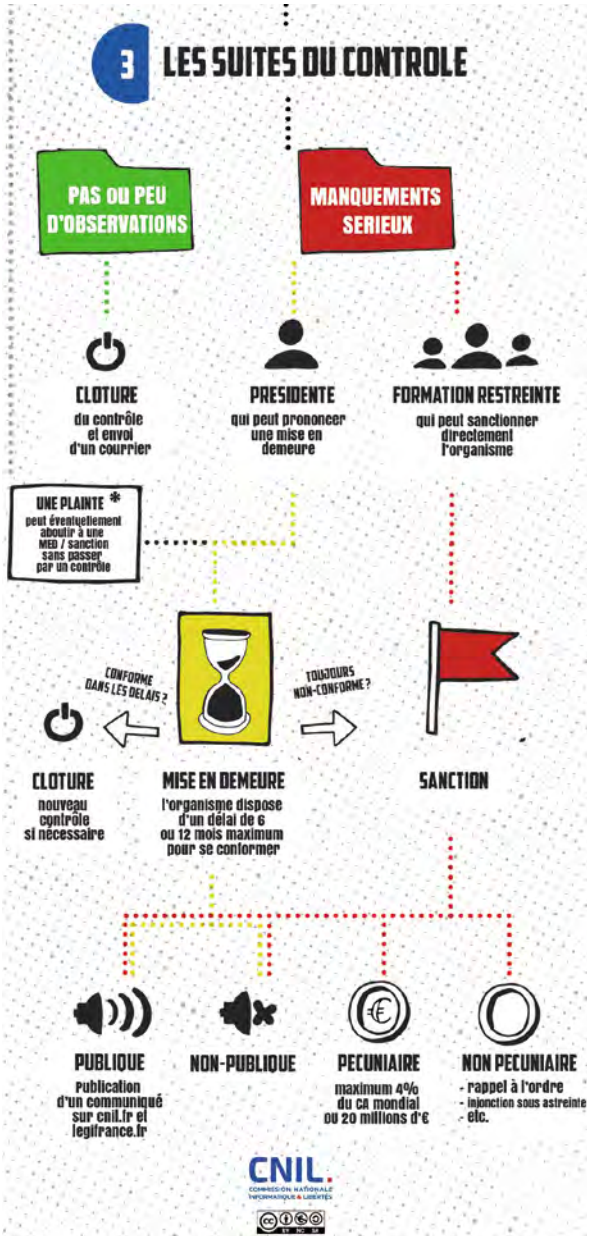
Une amende administrative doit ainsi être effective, proportionnée et dissuasive. Elle est également imposée selon les caractéristiques propres à chaque cas, en prenant en considération différents critères, parmi lesquels figurent par exemple :

- la nature, la gravité, la durée du manquement et le nombre de personnes concernées ;
- le fait que la violation a été commise délibérément ou par simple négligence ;
- les mesures prises par le responsable de traitement ou le sous-traitant pour atténuer le dommage ;
- les catégories de données concernées ;
- le niveau de coopération avec l'autorité de contrôle.

Le montant de l'amende est déterminé en fonction de ces éléments et peut s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial en cas de non-respect des principes fondamentaux du RGPD, des droits des personnes, des dispositions sur les transferts ou de non-respect d'une injonction d'une autorité.

L'amende peut atteindre jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial en cas de non-respect des obligations du responsable de traitement ou du sous-traitant (en matière de sécurité, d'analyse d'impact, de tenue du registre des activités, de désignation d'un DPO, *etc.*) ou de non-respect des obligations incombant à l'organisme de certification ou en charge des codes de conduite.





Les listes des organismes contrôlés, des mises en demeure et des sanctions sont disponibles sur le site de la CNIL

ANTICIPER
et innover

En 2018, le laboratoire d'innovation numérique de la CNIL poursuit ses activités articulées autour de trois grands axes : explorer, expérimenter et échanger. L'objectif est notamment d'explorer le futur de la société numérique, pour mieux anticiper l'impact de l'usage des innovations technologiques sur la vie privée et les libertés.

Régis
Chargé d'études prospectives, Pôle innovation, études et prospective
et Estelle
Designer, service de l'expertise technologique

Les missions du LINC (laboratoire d'innovation numérique de la CNIL) sont réalisées conjointement par le pôle innovation, études et prospective (PIEP) et le service de l'expertise technologique (SET). Nous avons tous des formations et des parcours variés allant de la cybersécurité aux humanités numériques. Cette diversité de compétences et de sensibilités nous permet une exploration à 360° de l'impact des usages des innovations technologiques sur la vie privée et les libertés. Ces travaux se font au-travers de publications, notamment sur linc.cnil.fr ; de la création de liens avec les acteurs de la société numérique (entreprises, institutions, associations, société civile…); de la mise en place des projets d'expérimentation, cela pour mieux cerner les usages numériques émergents.

En parallèle de ces activités, le PIEP est chargé en particulier de la publication de cahier innovation et prospective (Cahier IP) allant à la découverte de champs et sujets émergents produisant de nouveaux enjeux à venir pour la protection des données et des libertés. Ces cahiers sont des ressources utiles, tant aux équipes de la CNIL qu'aux personnes extérieures (toutes les publications sont en licence Creative Commons), pour mieux comprendre et se préparer à ces changements. Cet éclairage passe entre autre par la proposition de recommandations prospectives de régulation. Par exemple, dans le cahier IP consacré à la Smart City (2017), quatre scénarios de partage de données sont esquissés.

Le dernier cahier IP, La Forme des Choix, a été l'occasion d'inclure dans son élaboration une compétence récemment arrivée au sein de la CNIL : celle du design. Issues de cette collaboration, des propositions ont été construites pour la prise en compte du design des interfaces par le régulateur, et pour la création d'une communauté de designers soucieux de proposer des parcours éthiques et conformes au RGPD.

QUAND LE DESIGN DES INTERFACES CHERCHE À INFLUER SUR NOS LIBERTÉS

Le 17 janvier 2019, la CNIL publiait son 6e cahier Innovation et prospective, La Forme des choix - Données personnelles, design et frictions désirables : une exploration des enjeux du design dans la conception des services numériques, au prisme de la protection des données et des libertés.

Le design des interfaces n'a pas attendu le Règlement général sur la protection des données (RGPD) pour influencer nos vies. Nous sommes depuis longtemps guidés dans nos déplacements et actions par des architectures de choix conçues et mise en œuvre par d'autres. La grande distribution a depuis long temps modélisé son hypermarché avec des chemins préétablis visant à maximiser l'acte d'achat, depuis l'emplacement des packs d'eau à l'extrémité du magasin aux friandises disposées sur la caisse. Pourtant ces questions prennent un tour inédit dès lors qu'elles s'appliquent à des services numériques qui usent de méthodes de design pour parvenir à capter notre attention et traiter toujours plus nos données.

Design abusif et *dark patterns*

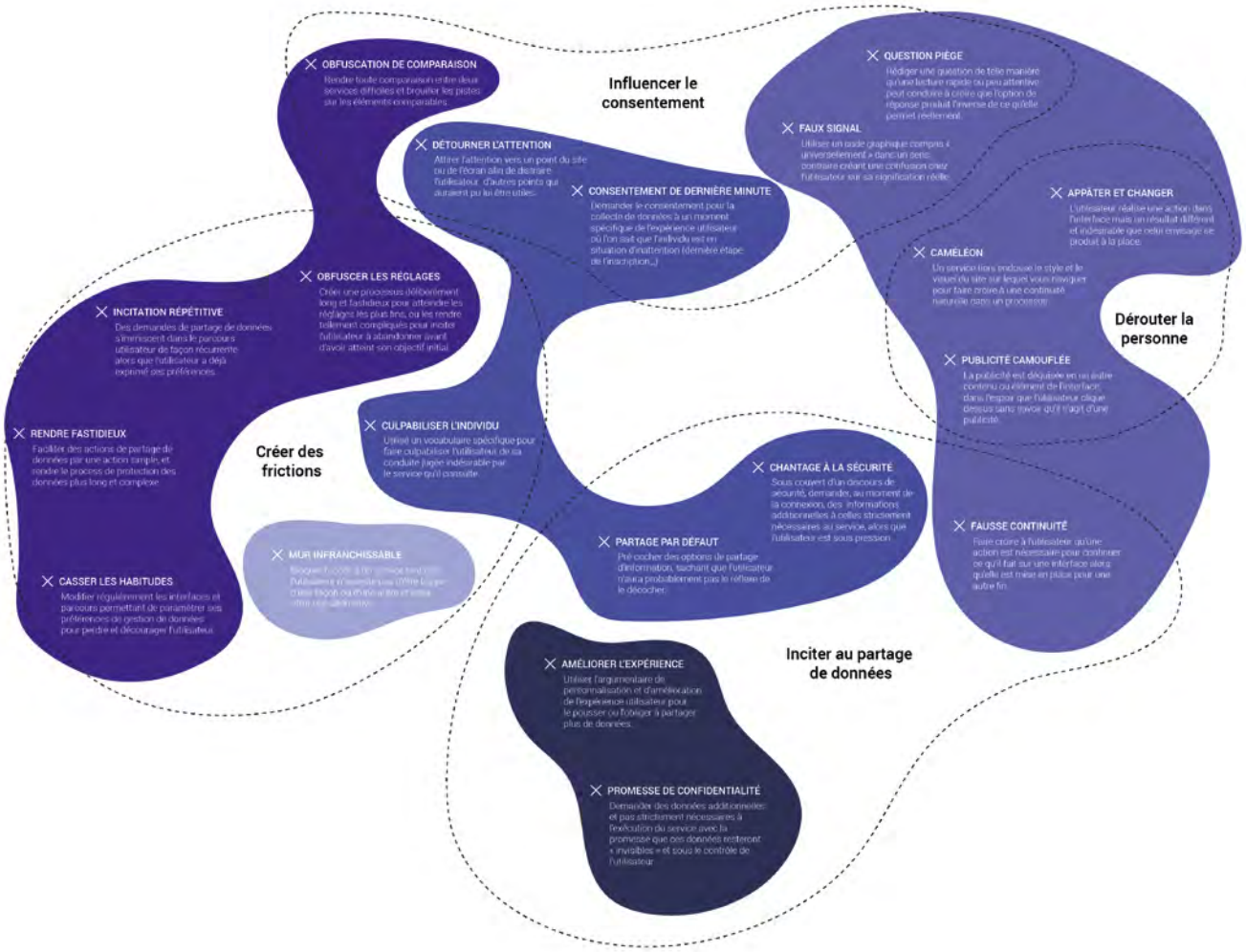
Certains concepteurs de services et plateformes numériques ont développé des méthodes consistant à se jouer de notre attention. Il s'agit d'exploiter nos biais cognitifs par l'utilisation de design abusif ou de *dark patterns*, à travers des interfaces utilisateur soigneusement conçues pour qu'un utilisateur fasse des choix sans qu'il en soit pleinement conscient. Nous sommes ainsi influencés et entraînés à partager toujours plus. Si ces méthodes, appelées incitations douces ou *nudge*, visent généralement à nous faire accepter ou consentir au traitement de nos données, ou bien à nous faire rester le plus longtemps possible sur un service en ligne, ces mêmes méthodes sont parfois utilisées avec pour finalité affichée l'intérêt général ou le bien-être de l'individu. Elles n'en posent pas moins la question de la liberté des individus à exercer leurs propres choix.

L'enjeu de ce cahier est donc de mettre le design des interfaces au centre des préoccupations du régulateur, tout comme il est déjà au centre des relations entre les individus et les fournisseurs de services. L'article 25 du RGPD, impose déjà d'intégrer les mesures appropriées de protection des données dès la conception. Les designers doivent prendre toute leur place et offrir leurs compétences au service de la protection des droits des utilisateurs. C'est par leur action, leur responsabilité et une meilleure prise en compte par les régulateurs, que le *privacy by design* deviendra réellement un concept opérationnel plutôt qu'une approche méthodologique.

Le design et l'analyse des interfaces doit donc entrer plus clairement dans le champ de l'analyse de conformité des régulateurs, dans un triangle de régulation composé également des analyses juridiques et techniques. Une telle approche nécessitera notamment pour le régulateur de développer les compétences professionnelles adaptées à l'analyse rationnelle et professionnelle de ces interfaces.

« Faire entrer le design dans le champ d'analyse de conformité des régulateurs. »

Typologie non exhaustive de designs potentiellement trompeurs et des pratiques qui peuvent poser des questions éthiques et de conformité au RGPD.



Vers la pratique d'un design éthique

Le régulateur peut aussi aider les professionnels à créer des bonnes pratiques et faire du design un levier vertueux du point de vue des droits des personnes. La CNIL souhaite susciter et accompagner le développement d'une communauté de designers soucieux de proposer des parcours éthiques et conformes à la réglementation sur les données personnelles. Cette communauté s'articulera autour d'une plateforme et une communauté en ligne (voir encadré), d'événements et de liens avec les écoles de design. Les acteurs pourront ainsi se saisir des solutions offertes par le design afin de mettre en lumière et accompagner positivement les utilisateurs dans la compréhension du mécanisme des services numériques et de leur droit à la protection de leurs données.

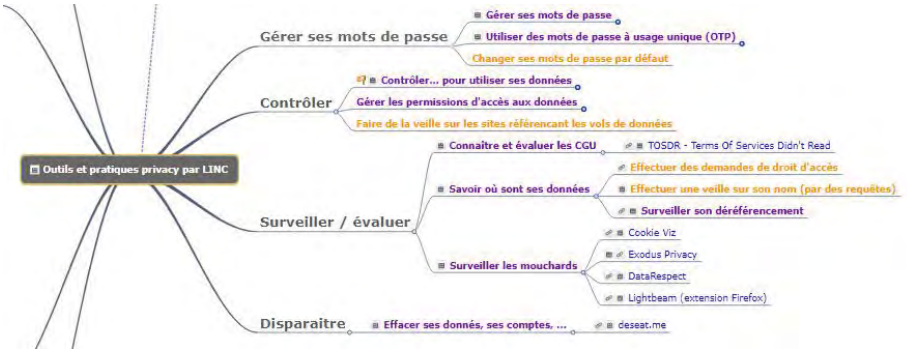
Design Factory
Une plateforme développée par la CNIL permettra aux professionnels du design d'échanger sur leurs pratiques respectives, de partager leur propre approche des enjeux de protection des données, et de co-construire la pratique d'un design éthique de la protection des données. **http://design.cnil.fr**

UNE CARTOGRAPHIE DES OUTILS ET PRATIQUES DE PROTECTION DE LA VIE PRIVÉE

La loi pour une République Numérique affirme la mission de la CNIL de « promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données ». Il s'agit pour la CNIL de donner à voir les différentes possibilités offertes pour que chaque individu soit en mesure d'adopter des outils ou pratiques respectueux de la vie privée, comme autant de pistes pour évoluer dans le monde numérique en adaptant son exposition et ses risques selon sa propre sensibilité, et contribuer à accroitre l'autonomie et la capacité d'agir des individus.

Mais comment promouvoir des technologies protectrices de la vie privée, en s'adressant au plus grand nombre, tout en respectant les pratiques et sensibilités de chacun ? Pour répondre à cette question, la CNIL a choisi de tracer une cartographie des pratiques de protection de la vie privée, disponible sur le site du laboratoire https://linc.cnil.fr, pour rendre compte de la diversité des approches et des outils, sans labelliser tel produit ou service.

https://linc.cnil.fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee



Le logiciel PIA fête sa première année

Publié en novembre 2017, le logiciel PIA, qui permet de réaliser en ligne son analyse d'impact sur la protection des données, a depuis été **téléchargé plus de 150 000 fois, et traduit en 18 langues**.

Ce logiciel *open source* dont le code est disponible sur la plateforme GitHub, a été conçu et développé avec les utilisateurs finaux lors d'ateliers de co-conceptions et avec l'apport des méthodologie du design. L'outil PIA constitue une innovation majeure pour la régulation, par la mise à disposition de méthodes et d'outils dont les responsables de traitement peuvent se saisir, les adapter et même les améliorer.

Le logiciel PIA a été récompensé par deux "Global Privacy and Data Protection Awards 2018" à l'occasion de la conférence ICDPPC 2018 réunissant les CNIL du monde entier.

Le logiciel PIA est aussi référencé sur le site de l'OCDE parmi les initiatives exemplaires en matière d'innovation publique.

18

LANGUES

C'est le nombre de langues dans lesquelles le logiciel PIA a été traduit en moins d'un an.

16

de ces traductions ont été produites par la communauté des utilisateurs.

IOTICS : PLONGÉE DANS L'ÉCOSYSTÈME DES OBJETS CONNECTÉS

Dans la continuité des recherches menées par la CNIL et INRIA lors du projet Mobilitics, qui visait l'analyse des systèmes d'exploitation sur smartphones, INRIA, EURECOM, le RITM de l'Université de Paris-Sud et la CNIL ont choisi de mener le projet ANR IoTics avec un but commun : analyser les objets de l'internet sous le double angle technique et juridique.

Les objets connectés, produits phares des commerces électroniques et physiques depuis plusieurs années, prennent une place de plus en plus importante dans notre quotidien. Le volet technique du projet portera sur l'étude de ces objets dans leur environnement immédiat ainsi que leurs fonctionnalités, tandis que le volet juridique s'attachera à l'analyse des politiques de vie privée. Débuté en 2017, les premiers résultats du projet IoTics seront publiés courant 2019.

STRATÉGIE *START-UP* : 19 ATELIERS ORGANISÉS EN 2019

La CNIL a mis en place une feuille de route afin de décliner une stratégie pour proposer une offre d'accompagnement à destination des *start-up*. La Commission a notamment formalisé un partenariat avec l'espace des services publics *French Tech Central* de Station F, un espace connu et reconnu, ouvert sur l'extérieur, dans lequel sont notamment organisés des ateliers à destinations des *start-up*. En 2018, pas moins de 19 ateliers thématiques ont été organisés, à Station F, mais aussi dans d'autres lieux de l'innovation, pour une audience totale de 423 représentants de *start-up*. Les thèmes abordés y ont notamment été : RGPD, Portabilité, Santé, Sécurité, *Fintech*, *Silver Eco*, PIA ou Objets connectés. En outre, des contenus ciblés seront bientôt proposés sur le site de la CNIL, avec une arborescence orientée utilisateur, adaptée aux besoins et questions que se posent les *start-up*.

LA CNIL ET INRIA ONT DÉCERNÉ LE PRIX « PROTECTION DE LA VIE PRIVÉE » 2018

Ce prix européen, créé par la CNIL et Inria en 2016 dans le cadre du partenariat qui lie les deux institutions, vise à encourager la recherche scientifique sur la protection de la vie privée en récompensant, chaque année, un article scientifique paru sur le sujet. En 2018, Pierre Laperdrix, Walter Rudametkin et Benoit Baudry ont ainsi été récompensés pour leur article : "*Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints*".

Les trois auteurs ont ainsi analysé la manière dont les internautes peuvent être tracés sur Internet par le biais d'une technique d'appareils appelée *browser fingerprinting* : cette technique consiste à collecter des informations relatives à la configuration du navigateur Web de l'utilisateur et de son système d'exploitation lorsqu'il visite un site Web. Ils y démontrent l'accès, via les innovations HTML5, à des critères utilisables pour identifier les internautes, aussi bien sur appareils fixes ou mobiles. Ils ont en parallèle exploré les évolutions possibles que les fournisseurs de technologie web pourraient mettre en place pour réduire les effets du traçage d'appareils sur Internet.

Le jury a considéré qu'il s'agit de résultats d'un grand intérêt pour la communauté des chercheurs, le grand public, les décideurs et tous les acteurs de l'écosystème. Il a également le mérite d'être d'actualité, étant donné les débats autour du règlement *ePrivacy*.

Les sujets de réflexion en 2019

Assistants vocaux, toujours à l'écoute de votre vie privée

Enceintes intelligentes, assistants personnels à commande vocale, agents conversationnels ou encore *chatbots*, la terminologie est vaste et témoigne de la place importance occupée par les assistants vocaux dans l'actualité. D'abord déployés sur les téléphones, puis les enceintes ou les casques audio, les assistants vocaux s'intègrent progressivement dans nos véhicules, nos équipements ménagers, *etc.* Vus comme les majordomes du XXIe siècle, ces assistants ont vocation à apporter leur concours aux utilisateurs dans leurs tâches quotidiennes : répondre à une question, jouer de la musique, donner la météo, régler le chauffage, allumer des lumières, réserver un VTC/Taxi, acheter des billets, *etc.* Toutefois, si l'ambition des industriels est de rendre la technologie invisible et de fluidifier les échanges, force est de constater que des questions bien réelles se posent concernant la vie privée des utilisateurs.

On associe fréquemment assistants vocaux et enceintes intelligentes ou connectées. Il est pourtant essentiel de noter que l'enceinte n'est qu'un vecteur et que les assistants peuvent s'intégrer dans tout type de dispositif. En pratique, un assistant vocal prend la forme d'un équipement embarquant un haut-parleur et un micro, des capacités calculatoires plus ou moins développées en fonction des assistants et, dans la quasi-totalité des cas, une possibilité de connexion à Internet.

Apparus pour la première fois au début des années 2010 dans des objets de grande consommation, de très nombreux assistants vocaux sont désormais déployés. En fonction des activités des sociétés qui les développent, ceux-ci répondent à des besoins bien précis : vente en ligne, écoute de musique, planification de tâches, domotique, *etc.* Des produits sont ainsi proposés par des grands groupes internationaux tels que les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) ou les BATX (Baidu, Alibaba, Tencent, Xiaomi) ou de beaucoup plus petites sociétés (par exemple Snips) avec des positionnements économiques différents.

Comment ces dispositifs fonctionnent-ils ?

Le principe général de fonctionnement d'un assistant vocal se caractérise par cinq grandes étapes. Prenons l'exemple d'une enceinte « intelligente » :

Étape 1
L'utilisateur « réveille » l'enceinte à l'aide d'un mot-clé (« Hey Snips » / « Ok Google / « Hey Alexa » / etc.)
L'enceinte est en permanence à l'écoute du mot clé. Elle n'enregistre rien et ne procède à aucune opération tant qu'elle ne l'a pas entendu. Cette étape est réalisée localement et n'implique aucun échange avec l'extérieur.

Étape 2 (optionnelle)
L'utilisateur est reconnu
Certains modèles d'assistants proposent à l'utilisateur de pré-enregistrer des échantillons de sa voix de manière à créer un modèle de celle-ci et le reconnaître lors de ses interactions avec l'assistant. L'intérêt de cette identification est de proposer des services différenciés selon les utilisateurs de l'appareil (parents, enfants, invités, *etc.*). On parle dans ce cas de biométrie vocale. Il est à noter que les données biométriques étant des données sensibles au sens du RGPD, elles ne pourront être traitées dans ce contexte que sur la base du consentement explicite de la personne concernée.

Étape 3
L'utilisateur énonce sa requête
La phrase prononcée par l'utilisateur est enregistrée localement par l'assistant. L'enregistrement de cette requête audio peut ensuite être :

- conservé dans le dispositif, de façon à laisser la maîtrise de ses données à l'utilisateur (par exemple une enceinte connectée avec l'assistant vocal de la société Snips) ; ou
- envoyé dans le *cloud*, autrement dit sur les serveurs de traitement de la société (ce qui est par exemple mis en œuvre avec les enceintes Amazon Echo, Google Home, *etc.*).

Étape 4 – L'enregistrement audio est transcrit en texte puis interprété afin qu'une réponse adaptée soit fournie
La parole prononcée est automatiquement transcrite en texte (*speech-to-text*) puis interprétée à l'aide de technologies de traitement automatique du langage naturel (*Natural Language Processing*) afin qu'une réponse adaptée soit fournie. Une phrase de réponse est ensuite synthétisée (*text-to-speech*) puis jouée et/ou une commande est passée (monter les stores, augmenter la température, jouer un morceau de musique, répondre à une question, *etc.*).

Que ces différents traitements soient réalisés localement ou sur des serveurs à distance, l'appareil (ou ses serveurs) peut être amené à conserver :
- un historique des requêtes transcrites afin de permettre à la personne de pouvoir les consulter et à l'éditeur d'adapter les fonctionnalités du service ;
- un historique des requêtes audio afin de permettre à la personne de les réécouter et à l'éditeur d'améliorer ses technologies de traitement de la parole ;
- les métadonnées associées à la requête comme par exemple, la date, l'heure, le nom du compte, *etc.*

Étape 5 - L'enceinte repasse en « veille»
L'assistant repasse en écoute passive et attend de reconnaître le mot clé pour être réactivé.

Quels enjeux et quels conseils pour la protection de la vie privée ?

La voix est une composante essentielle pour la construction de l'identité humaine. Elle est de ce fait éminemment personnelle. Des caractéristiques personnelles sont contenues tant au niveau acoustique (identité, âge, sexe, origines géographiques et socioculturelles, physionomie, état de santé et émotionnel, *etc.*) qu'au niveau linguistique (sens des mots prononcés, lexique utilisé, *etc.*). Confier des enregistrements de sa voix n'est donc pas un acte anodin.

De plus, en se développant en dehors des téléphones, les assistants vocaux sont progressivement passés du statut de « personnel » à celui de « partagés ». Ils investissent désormais des espaces intimes et communs à plusieurs personnes comme le salon, la chambre à coucher ou encore l'habitacle du véhicule. Ces changements de paradigme posent de nouvelles questions comme par exemple celle de la collecte et du traitement des données de tiers.

Enfin, comme précédemment décrit, dans la très vaste majorité des cas, les assistants vocaux reposent sur des traitements des signaux de parole effectués sur des serveurs à distance. Par conséquent, alors que la parole est généralement associée à une certaine volatilité, les requêtes vocales restent enregistrées dans le *cloud* au même titre que les requêtes textuelles effectuées dans certains moteurs de recherche.

La CNIL, a identifié trois points de vigilance qui s'ajoutent aux diverses interrogations auxquelles peuvent être confrontés les utilisateurs :

La confidentialité des échanges

En veille permanente, les assistants vocaux peuvent s'activer et enregistrer inopinément une conversation dès lors qu'ils supposent avoir détecté le mot clé. Pour mieux protéger la vie privée des utilisateurs ou éviter ce type de dysfonctionnement, il est donc conseillé de :

- privilégier l'utilisation d'équipements intégrant un bouton de désactivation du microphone ;
- couper le micro / éteindre / débrancher l'appareil lorsqu'on ne souhaite pas être écouté. Certains dispositifs n'ont pas de bouton on/off et doivent être débranchés ;
- avertir des tiers/invités de l'enregistrement potentiel des conversations qui seront tenues (ou couper le microphone en leur présence) ;
- encadrer les interactions des enfants avec ces équipements (rester dans la pièce, éteindre le dispositif lorsqu'on n'est pas avec eux) ;
- vérifier dans ce cas que le dispositif est bien réglé par défaut pour filtrer les informations à destination des enfants.

L'absence d'écran

Le propre des assistants vocaux est d'offrir une interface homme-machine ne reposant sur aucun support visuel.

Toutefois, autant pour la configuration des équipements que pour la gestion des données, il est encore nécessaire d'avoir recours à des outils comme des tableaux de bord. Sans écran tiers ni possibilité d'affichage, il est difficile d'avoir un aperçu des traces enregistrées, de juger de la pertinence des suggestions, d'en savoir plus ou d'avoir accès à des réponses provenant d'autres sources. Pour maîtriser les usages qui sont faits de ces données, il est donc recommandé de se rendre régulièrement sur le tableau de bord (ou l'application) fourni avec l'assistant pour supprimer l'historique des conversations ou questions posées et personnaliser l'outil selon ses besoins ; par exemple, définir le moteur de recherche ou la source d'information utilisée par défaut par l'assistant.

La monétisation de l'intime

Principalement destinés au domicile pour contrôler des objets connectés et des services de divertissement, les appareils dotés d'un assistant à commande vocale se retrouvent aujourd'hui au cœur du foyer. Le profil des utilisateurs se trouve donc alimenté par les différentes interactions qu'ils ont avec l'assistant (par exemple, habitudes de vie : heure de lever, réglage du chauffage, goûts culturels, achats passés, centres d'intérêt, *etc.*). Pour s'assurer des usages qui sont faits de ces données, il est recommandé de :

- connecter des services qui présentent réellement une utilité pour l'utilisateur, tout en considérant les risques à partager des données intimes ou des fonctionnalités sensibles (ouverture de porte, système d'alarme, *etc.*) ;
- être vigilant sur le fait que les propos tenus face à l'appareil peuvent enrichir le profil publicitaire ;
- ne pas hésiter, en cas de questions, à contacter les services supports de l'entreprise fournissant l'assistant.

Quelles évolutions futures et quels travaux de la CNIL ?

Les fabricants mènent de nombreux travaux afin d'améliorer les capacités des assistants vocaux et leur sécurité. Si certains souhaitent ainsi supprimer de plus en plus le recours au mot clé pour le réveil de l'assistant, d'autres travaillent à mettre en œuvre des traitements de séparation des sources sonores afin d'améliorer la capacité d'écoute des systèmes, par exemple pour atténuer le son de la télévision, séparer la parole d'une personne de celle d'une autre, *etc.* Enfin, les professionnels investiguent de nouveaux lieux d'usage, comme le parc hôtelier ou les espaces de travail, renouvelant de ce fait les questions autour des usages effectifs des données.

La thématique des assistants vocaux a été identifiée comme axe de travail par la CNIL dès 2017. Celle-ci est entrée rapidement en contact avec différentes parties prenantes afin d'avoir une parfaite compréhension des systèmes déployés. Elle a mené d'importantes réflexions au sein du laboratoire d'innovation numérique de la CNIL (LINC), sa structure dédiée à l'expérimentation et à l'étude des tendances émergentes d'usage du numérique. Un dossier thématique composé d'articles et d'entretiens avec des professionnels a ainsi été publié sur son site.

En 2019, la CNIL prévoit de prolonger ces travaux, à la fois en continuant d'échanger avec les industriels et les académiques dont c'est l'objet d'étude, mais également en poursuivant des tests sur ces appareils. Il s'agira en particulier d'évaluer comment garantir que les utilisateurs sont bien informés des données collectées, des usages qui en sont faits et des moyens à leur disposition pour exercer leurs droits d'accès, modification, suppression et portabilité, ainsi que d'étudier la sécurité des données traitées et la manière dont est réalisé l'apprentissage des algorithmes d'intelligence artificielle inhérents à ces appareils.

Le *cloud* computing à l'ère du RGPD

Dès 2012, la CNIL et le G29 ont publié des recommandations sur le *cloud* computing (informatique en nuage). Depuis, le recours au *cloud* n'a fait que s'intensifier : Gartner[1] estimait récemment que la croissance du marché du *cloud* public serait de 21,4 % en 2018, et que ce marché atteindrait 300 milliards de dollars en 2021. Dans le même temps, Eurostat[2] indiquait que 55 % des entreprises ont recours au *cloud* pour des fonctions critiques (finances, comptabilité, CRM ou applications métiers). À l'heure du RGPD, qui modernise les obligations applicables aux responsables de traitements comme aux sous-traitants, un état des lieux s'impose sur l'utilisation du *cloud* dans les organisations. Les recommandations de 2012 ont-elles été intégrées ? La protection des données personnelles est-elle maitrisée lors d'une migration vers le *cloud* ?

Une concentration du risque et un pouvoir de négociation limité

En décembre 2018, un sondage[3] publié par l'Independent Oracle Users Group estimait qu'un quart des données des entreprises étaient à présent stockées dans le *cloud*. Il s'agit bien sûr de données industrielles, mais aussi dans bien des cas de données à caractère personnel, parfois sensibles, qui sont généralement hébergées et traitées dans les infrastructures d'un nombre très limité de grands fournisseurs de *cloud* computing. Or, face à ces acteurs, ceux qui souhaitent recourir au *cloud* ont en réalité un pouvoir de négociation contractuelle très limité.

Le déplacement des données dans ces infrastructures peut conduire à l'augmentation du risque systémique, alors même que les entreprises fournissant ces services, qu'elles soient qualifiées de responsables de traitement ou de sous-traitants, sont bien dans le champ d'application matériel du RGPD.

En outre, l'adoption en 2018 du *Cloud* Act par les États-Unis, qui donne aux autorités américaines un cadre juridique leur permettant d'accéder aux données au-delà des frontières, et la proposition européenne de règlement sur les contenus terroristes en ligne, soulèvent des questions sur l'équilibre possible à trouver en matière de vie privée lors du recours à ces services.

Les enjeux de protection des données, et plus largement les enjeux économiques et stratégiques sont considérables. Il est donc essentiel que la CNIL fasse un état des lieux technique et précis sur ces infrastructures et services.

¼ des données des entreprises stockées dans le *cloud*

(selon l'Independent Oracle Users Group)

1 https://www.gartner.com/en/newsroom/press-releases/2018-04-12-gartner-forecasts-worldwide-public-*cloud*-revenue-to-grow-21-percent-in-2018.
2 https://ec.europa.eu/eurostat/statistics-explained/index.php/*Cloud*_computing_-_statistics_on_the_use_by_enterprises
3 « 2019 IOUG databases in the *cloud* survey" par Joseph McKendrick, produit par Unisphere Research, division de Today, Inc. Décembre 2018 https://www.ioug.org/d/do/8551

FOCUS

Recommandations en matière de *cloud* :

1. Cartographier les données et traitements dans le *Cloud*
2. Définir ses exigences techniques et juridiques
3. Conduire un PIA ou au moins une analyse de risque Vie Privée
4. Identifier le type de *Cloud* pertinent pour chaque traitement
5. Choisir un prestataire présentant des garanties suffisantes
6. Mettre à jour la politique de sécurité interne
7. Surveiller les évolutions dans le temps

CNIL et *cloud*, une vieille histoire

La CNIL travaille sur le sujet depuis le début des années 2010, en collaboration avec les autres autorités européennes de protection des données. Après une large consultation, en juin 2012, la CNIL a publié ses premières recommandations en matière de *cloud computing*, suivies par le G29 un mois plus tard. Le concept de responsabilité conjointe faisait alors une entrée dans la doctrine de la CNIL. Aujourd'hui, ce concept est prévu dans le RGPD, et les sous-traitants, qui n'avaient jusqu'alors pas de responsabilité juridique au regard de la loi Informatique et Libertés, ont désormais des obligations.

L'avenir du *cloud* à l'étude par la CNIL

La CNIL souhaite tout d'abord approfondir les aspects techniques pour mieux comprendre le détail des infrastructures des principaux fournisseurs de services de *cloud* et plus généralement de cet écosystème. Dans un second temps, elle analysera les contraintes et les risques auxquels les entreprises clientes sont réellement confrontées aujourd'hui. Enfin, ces travaux lui permettront d'actualiser ses recommandations et d'identifier de nouveaux leviers de régulation de ce secteur à mobiliser.

Dans ce contexte, il s'agira d'approfondir notamment les axes suivants :

- **Les clauses entre les responsables de traitement et les sous-traitants**

Pour les services de *cloud* ayant la qualité de sous-traitants, quelle est la marge de négociation laissée aux clients en matière de sécurité et de protection de la vie privée ? Quelles clauses régissent les relations entre responsables de traitants et sous-traitants ? Couvrent-elles bien l'ensemble des points figurant à l'article 28 du RGPD ?

- **L'impact des législations**

Quel est l'impact de certaines législations spécifiques, à finalité anti-terroriste notamment, sur les contrats de *cloud* et sur la protection de la vie privée ? Qu'il s'agisse du *Freedom act* et du *Cloud* act aux États-Unis ou du projet de règlement « relatif à la prévention de la diffusion en ligne de contenus à caractère terroriste » proposé par la Commission européenne en septembre 2018.

- **Le chiffrement**

Le chiffrement est un des mécanismes les plus puissants pour assurer la confidentialité des données : comment celui-ci est-il utilisé et appliqué en pratique dans les nouvelles architectures de *cloud* ? Dans quelle mesure est-il possible de respecter les bonnes pratiques en la matière en gérant les clés de façon sécurisée ? Par exemple, lorsque les machines virtuelles sont redémarrées aléatoirement, quels sont les moyens mis en œuvre pour permettre un partage sécurisé des clés entre le module matériel de sécurité (HSM) du client et la nouvelle instance ?

- **La fin du contrat**

Lors de ses précédents travaux, les responsables de traitements indiquaient à la CNIL de grandes difficultés dans la récupération de leurs données en fin de contrat et la difficulté de s'assurer que les données étaient correctement supprimées. La gestion de la clôture des comptes s'est-elle améliorée ? En première analyse, il semble que des progrès aient été faits dans ce domaine, mais sont-ils suffisants pour permettre aux responsables de traitements de remplir effectivement leurs obligations ?

- **L'information sur la localisation des données**

De nombreuses améliorations ont été constatées dans l'information fournie aux clients aux responsables de traitements concernant la localisation des données. Pour autant, comment les clauses de localisation des données prennent-elles en compte les situations exceptionnelles, comme les cas de force majeure ou la connexion aux matériels par des administrateurs ou du support à distance ?

- **Les notifications de violations de données**

Comment les fournisseurs de *cloud* ont-ils mis en œuvre les notifications de violations de données à caractère personnel ? Notamment, lorsque ceux-ci ont la qualité de sous-traitants, quels sont les moyens mis à disposition de leurs clients, responsables de traitements, pour respecter leurs obligations (que ce soit pour une violation détectée par le fournisseur de service ou pour une violation dont le client est averti par un tiers) ?

Enfin, à l'heure où la confiance est devenue un impératif pour les fournisseurs de service de *cloud*, les normes, codes de conduite, et autres référentiels se multiplient. Il conviendrait donc d'évaluer leur pertinence au regard de la protection des données. Une cartographie de ces référentiels permettrait aux fournisseurs et à leurs clients de choisir ceux qui sont les plus pertinents pour eux.

Partage de données : des enjeux d'intérêt général

Dans le cahier IP5, la plateforme d'une ville, la CNIL explorait quatre scénarios de partage des données pour engager un rééquilibrage entre acteurs privés et publics par les données. Depuis, le sujet du partage des données tend à s'imposer dans le débat public, apparaissant comme une réponse possible à plusieurs besoins essentiels de la société, notamment en termes de régulation et de recherche.

Depuis 2017, dans le prolongement du mouvement *open data* et de la notion de données d'intérêt général, plusieurs travaux plaident pour un plus grand partage des données. Cette perspective a été décrite par le Président de la République dans son discours sur l'intelligence artificielle en mars 2018. Le Rapport Villani « Pour donner un sens à l'intelligence artificielle », a quant à lui recommandé notamment :

- « d'inciter les acteurs économiques à la mutualisation de données » ;
- « d'organiser l'ouverture au cas par cas de certaines données détenues par des entités privées » ;
- « de mettre en œuvre la portabilité dans une visée citoyenne » ;
- « de faciliter le dialogue entre les acteurs de l'IA et les régulateurs », reprenant ainsi certains des thèmes développés par la CNIL.

Cette question du partage de données a également fait l'objet de travaux dans le cadre des États généraux des nouvelles régulations numériques, lancés en juillet 2018.

Le spectre des données concernées par de telles initiatives de partage concerne pour tout ou partie des données personnelles, et doit se faire dans le respect des droits des individus. Pour cette raison, la CNIL estime nécessaire d'encourager le développement d'un modèle efficace et durable de partage des données, intégrant une forte composante éthique, basé sur le respect des droits fondamentaux, au titre desquels figure naturellement, la protection des données personnelles et de la vie privée.

Des initiatives de partages déjà repérées

Plusieurs initiatives de partage de données voient déjà le jour, par exemple à la Rochelle qui s'inspire du principe de portabilité citoyenne pour accéder à certaines données détenues par des opérateurs privés. Selon une autre logique, le CASD (Centre d'Accès Sécurisé aux Données) étend son offre de service à l'hébergement de données privées (banques, services, transport, santé privée, *etc.*) et à leur mise à disposition, sur une base uniquement volontaire, à des chercheurs ou à des opérateurs privés aux fins de développer des services à valeur ajoutée. En 2018, le rapport de la mission de préfiguration du projet

« *Health data hub* », qui comporte des propositions de modalités d'organisation pour une plateforme d'exploitation et de partage de données de santé, a aussi été remis à la ministre des Solidarités et de la Santé. Il a nourri, début 2019, le dépôt du projet de loi relatif à l'organisation et à la transformation du système de santé, sur lequel la CNIL a rendu un avis en janvier 2019. À l'international, des acteurs privés élaborent des modèles de partage de données : par exemple, la ville de Toronto envisage avec Sidewalk Labs de développer un *civic data trust*, controversé localement, pour une gouvernance des données urbaines.

Définir un cadre plutôt qu'un modèle unique de partage

Le RGPD a été conçu pour concilier à la fois l'innovation technologique et la protection des droits des personnes, pariant que la première serait d'autant plus forte et soutenable que la seconde serait respectée et promue.

À cet égard, le partage de données entre acteurs, publics ou privés, n'est pas contraire en soi au droit à la protection des données personnelles, d'autant plus lorsque des finalités d'intérêt général clairement définies sont concernées. Ces initiatives appellent cependant une clarification du cadre applicable et un accompagnement très en amont des porteurs de projets.

La CNIL a déjà entrepris en interne des travaux en vue de clarifier le cadre juridique applicable au partage des données, en balayant les grandes questions transversales de conformité au RGPD (base légale de la mise à disposition des données, modalités d'exercice des droits des personnes tout au long de la chaîne de partage, *etc.*), afin de pouvoir fournir un appui dans la sécurisation juridique des projets. Un tel cadrage juridique ne peut toutefois que rester très général, tant les questions de respect des droits, de gouvernance, de modalités de partage (direct ou par l'intermédiaire d'un tiers) ne peuvent être examinées qu'à l'occasion d'un projet concret. Mais, de manière générale, au-delà de la stricte conformité aux textes, la CNIL promeut fortement l'intégration de la nécessaire protection des données personnelles dès la conception des démarches de partage, dans une optique tant juridique qu'éthique.

La CNIL poursuivra ses travaux de cadrage, et les doublera d'une politique volontariste d'accompagnement préalable sur des projets sectoriels donnés, y compris dans une dimension expérimentale, dans le cadre de son rôle de conseil aux pouvoirs publics et d'accompagnement des professionnels. Elle vérifiera, dans l'ensemble de ses missions, l'efficacité, du point de vue du droit à la protection des données personnelles, des garanties prévues et, le cas échéant, proposera des aménagements ou correctifs aux dispositifs.

« Le partage des données d'intérêt général constitue une opportunité pour la mise en œuvre d'un modèle européen d'innovation éthique. »

Capitaliser et approfondir les travaux déjà lancés

La CNIL possède une expérience de régulation des plateformes de partage des données montrant qu'il n'existe pas de modèle unique, mais que plusieurs options sont possibles et souhaitables. En particulier, les scénarios proposés dans le cadre du cahier IP 5 pour la réutilisation de données privées par des acteurs publics pourraient être complétés et affinés, notamment s'il était décidé d'ouvrir davantage certaines données personnelles d'acteurs privés au bénéfice d'autres acteurs privés.

En fonction des secteurs ou des projets, il conviendra alors de moduler et combiner l'ensemble des scénarios de partage disponibles. Dans certains cas, le recours à des intermédiaires (plateformes, régie de données), chargés de la mise à disposition des données et, le cas échéant, d'autres fonctions dans le dispositif général, pourrait s'avérer particulièrement adapté, notamment en cas de mutualisation de données par plusieurs acteurs. Le recours à ces intermédiaires ne paraît pas pour autant adapté à tous les dispositifs de partage, notamment lorsque les données proviennent d'un seul acteur et sont mises à disposition d'un ou plusieurs organismes. Dans ce cas, de simples jeux de règles juridiques (licence) et techniques (API), sans intermédiaire, pourraient s'avérer tout à fait adaptés et suffisants à assurer la conformité du dispositif aux règles en matière de protection des données.

C'est par une approche dès la conception des systèmes que les acteurs parviendront à produire des modèles de partage de données vertueux et pérennes, plaçant le citoyen et ses droits au cœur du processus et de la gouvernance des données à des fins d'intérêt général. À ce titre, le régulateur a son rôle à jouer, engagé dans la promotion de modèles innovants et garantissant le niveau le plus élevé de protection des droits des personnes.

Communication politique & RGPD : vers une actualisation des recommandations et une précision des bonnes pratiques

La CNIL accompagne toutes les parties prenantes au processus électoral, qu'il s'agisse des candidats aux élections et de leur parti, des élus ou des électeurs qui la sollicitent et ce, tant dans le cadre de la mise en conformité des traitements mis en œuvre que pour permettre l'exercice des droits des personnes concernées. À la suite de l'entrée en application du RGPD et dans un contexte d'élections européennes et municipales, la CNIL entend poursuivre les travaux engagés sur cette thématique et prévoit notamment de mettre à jour sa recommandation de 2012.

La détermination des règles applicables en matière de communication politique constitue l'une des activités de longue date de la CNIL, sa première recommandation en la matière de communication politique ayant été adoptée en 1991. Cette activité a pris ces dernières années un relief particulier avec le développement des outils numériques combinés à l'utilisation des réseaux sociaux. On observe un enchevêtrement complexe des liens qui existent entre des acteurs d'horizons variés : les personnes qui produisent, par leurs activités, un nombre important de données et les fournissent volontairement à certains acteurs, les plateformes dont le modèle économique repose sur le traitement de ces données, les sociétés de conseil et les structures de recherche, les partis politiques susceptibles d'utiliser ces données.

De plus, plusieurs scandales, en particulier l'affaire Cambridge Analytica, ont permis au grand public de prendre conscience des enjeux liés à l'utilisation de leurs données et, en particulier, de la nécessité d'empêcher l'utilisation abusive de données à caractère personnel lors des campagnes politiques. Au travers de l'année passée, se sont révélés en particulier des enjeux juridiques complexes autour de la notion de profilage, de la localisation des données ainsi que des moyens à employer pour assurer leur sécurité. Enfin, au-delà des seuls enjeux juridiques, ces différentes affaires soulèvent des enjeux éthiques importants en touchant notamment à la sincérité des scrutins.

Dans ce contexte, le rôle de **la CNIL, dans le secteur de la communication politique, consiste à accompagner l'innovation** tout en garantissant **le respect des libertés individuelles dans un contexte où les nouvelles technologies font désormais partie des instruments fréquemment utilisés dans le cadre de campagnes politiques.**

L'impact de la mise en œuvre du RGPD sur la communication politique : principes à respecter et bonnes pratiques.

Si la réglementation relative à la protection des données a évolué depuis le 25 mai dernier, le nouveau cadre juridique n'a pas emporté de changement quant à la qualification des opinions politiques comme des données sensibles, au principe d'interdiction de collecter et de traiter de telles données, ainsi qu'aux exceptions que le responsable de traitement pourrait mobiliser pour déroger à cette interdiction (article 9 du RGPD).

De même, le RGPD ne modifie pas les grands principes qui régissent la protection des données personnelles et dont le respect doit permettre d'encadrer les conditions dans lesquelles les données relatives aux opinions politiques peuvent être utilisées.

Respecter les règles d'or en matière de protection des données

Illustrations au travers de quelques principes clés :

- **Déterminer la finalité du traitement mis en œuvre :** il est indispensable de définir précisément l'objectif poursuivi par le traitement qui repose sur la collecte de données relatives aux opinions politiques.
- **S'assurer de la proportionnalité des données collectées :** seules les données strictement nécessaires dans le cadre de la finalité déterminée doivent être traitées.
- **Sécuriser les données collectées :** le caractère particulier des données traitées justifie que des mesures renforcées soient mises en œuvre afin d'assurer leur sécurité (définition de mesures de stockage appropriées, gestion des accès, *etc.*).

Ces principes demeurent plus que jamais d'actualité afin de se prémunir de toute utilisation abusive des données à caractère personnel dans le cadre d'une campagne électorale. L'évolution de la réglementation applicable en matière de protection des données à caractère personnel conduit également à faire application des nouvelles dispositions de la réglementation, en particulier s'agissant des droits des personnes dont les données sont traitées.

La diversité des informations pouvant conduire à considérer que l'on se trouve en présence d'opinions politiques implique que les données collectées soient traitées de manière transparente. Une information suffisante et facilement accessible doit ainsi être délivrée aux personnes concernées.

L'apparition de nouveaux droits (droit à la limitation du traitement, à la portabilité, *etc.*) devra également être prise en compte dans le cadre de pratiques telles que la prospection politique afin de garantir leur effectivité. De la même manière, une réflexion plus globale devrait être menée sur les conditions dans lesquelles une telle prospection pourrait être réalisée notamment lorsqu'elle repose sur des fichiers constitués initialement dans un autre but (tels que les fichiers commerciaux).

L'entrée en application du RGPD entraînant la disparition de la plupart des formalités préalables tout en renforçant la protection accordée à chaque citoyen au travers notamment de la création de nouveaux droits et obligations pour les acteurs de la vie politique, **la CNIL a entamé une analyse approfondie qui la conduira à adapter prochainement ses recommandations et à formuler des bonnes pratiques en la matière.**

Dans le même temps, la CNIL entend poursuivre ses travaux s'agissant des nouveaux outils et usages mobilisés à des fins de communication politique dans le but d'affiner et d'asseoir sa doctrine en la matière dans une période marquée par l'organisation d'élections tant au niveau européen qu'au niveau national. En particulier, il s'agit, à partir des travaux entamés en matière de logiciels de prospection électorale, de préciser notamment les conditions dans lesquelles les données issues des réseaux sociaux peuvent être utilisées ainsi que le rôle de chacun des acteurs intervenant dans le cadre d'une campagne électorale.

Campagne électorale et utilisation des données personnelles : grands principes et point de vigilance

La CNIL a rédigé un article pour la revue AJCT (Actualité Juridique Collectivités territoriales) à paraître au mois de février 2019 au sein d'un dossier dédié « Internet, réseaux sociaux et campagne électorale ».

Données personnelles, réseaux sociaux et démocratie : au programme 2019 des autorités francophones

Le 19 octobre 2018, la CNIL a accueilli la réunion annuelle de l'Association francophone des autorités de protection des données personnelles (AFAPDP). Les autorités francophones ont été invitées à une matinée d'échanges autour de la thématique « Données personnelles, réseaux sociaux et démocratie ». Le sujet a naturellement émergé suite aux révélations de l'affaire « Cambridge Analytica » mais s'inscrit plus largement dans une réflexion menée par l'AFAPDP sur les questions électorales depuis plusieurs années. L'association a notamment participé à l'élaboration d'un Guide pratique pour la consolidation de l'état civil, des listes électorales et la protection des données personnelles[4], publiée par l'Organisation internationale de la Francophonie (OIF) en 2014.

Pour cette séance, l'AFAPDP a souhaité privilégier une approche transversale, qui déborde du simple cadre de la protection des données personnelles. À cette fin, l'AFAPDP a fait appel aux expertises complémentaires du Réseau des compétences électorales francophones (RECEF), du Réseau francophone des régulateurs médias (REFRAM) et de Reporters sans frontières (RSF). Tous s'interrogent sur leurs rôles respectifs avec l'émergence, dans les différentes étapes du processus électoral, de nouveaux outils digitaux, médias et réseaux sociaux.

Si des principes juridiques pertinents existent déjà, ils échappent totalement ou en partie aux réseaux sociaux et, plus largement, à l'espace numérique. Cette prise juridique, que l'on pourrait qualifier de partielle, pourrait être renforcée par de nouvelles dispositions législatives. Une approche multi-régulatrice pourrait également venir consolider la fiabilité et la sincérité des processus électoraux à l'heure du numérique et c'est dans cette optique qu'un groupe de travail multi réseaux est en train d'être mis en place entre l'AFAPDP, le RECEF et le REFRAM, avec le soutien de l'OIF.

4 https://www.francophonie.org/IMG/pdf/oif_guide-pratique_etatcivil-27-11-14.pdf

La réutilisation de données accessibles « en ligne » par le monde de la recherche : enjeux et perspectives

Des révélations ou affaires récentes ont illustré les dérives possibles liées à l'exploitation de données librement accessibles sur internet à des fins de recherche : détournements de finalité ou diffusion non contrôlée des résultats portant atteinte à la protection des données des personnes concernées. Plus généralement, face au constat de l'intérêt d'utiliser les données accessibles « en ligne » à des fins de recherche, la CNIL a décidé d'initier une réflexion s'agissant des conditions dans lesquelles ces opérations pouvaient être menées.

Recherche et utilisation de données à caractère personnel : des liens inextricables

Les gisements de données nés de l'utilisation d'internet et des réseaux sociaux attirent de nombreux acteurs qui souhaitent les exploiter et en tirer une valeur ajoutée pour leurs activités. L'utilisation de ces données présente des enjeux et risques significatifs pour la protection des données. L'affaire « Dinsinfo Lab » a ainsi illustré la sensibilité des enjeux liés à la réutilisation, par la recherche, des données accessibles en « ligne », les révélations sur l'affaire Cambridge Analytica ont illustré les détournements qui pouvaient être réalisés à partir des données initialement collectées pour des finalités de recherche et utilisées à d'autres fins.

Les chercheurs font partie des acteurs qui utilisent cet important volume de données. Dans ce contexte, la CNIL est ponctuellement saisie de projets de recherche effectués à partir de ces données pour s'assurer que ces projets s'inscrivent dans le respect de la réglementation applicable en matière de protection des données à caractère personnel.

L'articulation de certains principes résultant de cette réglementation avec les objectifs de la recherche peut sembler peu aisée. Dans le cadre des saisines de la CNIL, il avait ainsi pu être relevé que certains acteurs estimaient soit que la réglementation Informatique et Libertés ne concernaient pas leurs travaux, soit que les principes juridiques correspondant interdisaient ou contrevenaient à la plupart de ceux-ci. La réalisation de travaux de recherche nécessite en effet le plus souvent la collecte d'un volume important de données pour lesquelles il peut être difficile de définir précisément – et *a priori* - une durée de conservation. À ce titre, la constitution de jeux de données utiles pour d'autres études, l'accès à ces derniers afin d'assurer la reproductibilité de la recherche constituent autant d'enjeux qui doivent être conciliés avec les impératifs liés au respect de la réglementation Informatique et Libertés.

C'est dans ce contexte que la CNIL a souhaité entamé une réflexion sur les conditions juridiques dans lesquelles il est possible, à des fins de recherche, de réutiliser des données accessibles en ligne. Cette réflexion doit également permettre de clarifier la réglementation applicable en la matière dans un contexte politique et social marqué par plusieurs « affaires » relatives à la réutilisation de données accessibles « en ligne » par des chercheurs. Il apparaît en effet primordial que des réflexes en matière de protection des données personnelles soient intégrés aux projets de recherche dès leur conception, au risque que ceux-ci soient menés sans en tenir compte.

« La réalisation de travaux de recherche nécessite la collecte d'un volume important de données pour lesquelles il peut être difficile de définir précisément *a priori* une durée de conservation. »

Une réglementation Informatique et Libertés au bénéfice du secteur de la recherche

À l'heure du renforcement de la réglementation applicable en matière de protection des données à caractère personnel, la CNIL rappelle que de nombreuses dispositions peuvent être mobilisées au bénéfice des traitements de données mis en œuvre pour des finalités de recherche. Le RGPD prévoit par exemple, dans certaines conditions, des exceptions à l'interdiction de traiter des données sensibles, à l'obligation d'informer les personnes dont les données sont collectées, ainsi qu'à l'exercice des droits à l'effacement et d'opposition.

Le RGPD distingue la recherche scientifique, la recherche historique et la recherche à des fins statistiques. Il indique que la recherche scientifique devrait être interprétée au sens large et couvrir « par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé », mais aussi « les études menées dans l'intérêt public dans le domaine de la santé publique » (considérant 159 du RGPD).

Il est de ce fait apparu nécessaire que la CNIL entame, en amont comme en aval de l'entrée en application du RGPD, des travaux pour présenter et définir plus finement le cadre juridique applicable. Ces travaux doivent ainsi permettre d'accompagner la mise en conformité des acteurs – tant publics et privés – du monde de la recherche. En particulier, il s'agit notamment d'expliciter les conditions dans lesquelles les traitements projetés peuvent être mis en œuvre en rappelant que le consentement ne constitue que l'une des bases légales mobilisables avec par exemple l'exécution d'une mission d'intérêt public ou encore l'intérêt légitime du responsable de traitement, de s'interroger sur la loyauté de la collecte de données réalisée ainsi que sur l'information des personnes concernées qui doit être délivrée.

Sur la question de l'information en particulier, l'une des difficultés soulevées par l'application des dispositions du RGPD réside dans le bon équilibre à trouver entre la nécessité de délivrer des informations suffisantes et celui de favoriser la participation à une étude, à une recherche.

De la même manière, ces travaux devront permettre de clarifier les rapports susceptibles d'exister entre les différents champs de la recherche (recherche publique, recherche privée) ainsi que les éventuelles distinctions à opérer selon que l'on se trouve dans l'un ou l'autre de ces champs. Il importe en effet que chacun des acteurs concernés soit en mesure de comprendre ce qu'il peut faire ou non à partir des données collectées et ce, en fonction du contexte dans lequel il s'inscrit. Cette clarification semble d'autant plus importante que certains chercheurs sont par exemple susceptibles de passer de l'une à l'autre de ces sphères au cours de leur carrière.

Ces travaux, qui seront menés en lien avec les acteurs de la recherche, devront également permettre de déterminer les garanties appropriées à mettre en place pour encadrer la collecte, l'utilisation ainsi que la réutilisation des données accessibles « en ligne » par le monde de la recherche. En particulier, il s'agira de déterminer dans quelles conditions les chercheurs peuvent avoir accès aux données en ligne sur les plateformes de réseaux sociaux afin, par exemple, d'éviter les situations dans lesquelles seuls quelques chercheurs pourraient accéder à ces données ou que seules les recherches servant les plateformes en termes de marketing ou d'efficacité commerciale puissent reposer sur un accès aux données détenues.

La démarche initiée par la CNIL vise ainsi à :

- **assurer une meilleure sécurité juridique** aux acteurs de la recherche en clarifiant le cadre juridique applicable aux projets de recherche basés sur le traitement de données accessibles en ligne et en dotant ces acteur d'outils simples de compréhension du RGPD appliqués à leurs projets ;
- **émettre des recommandations en phase avec les besoins et contraintes des organismes de recherche,** afin de leur permettre de mener à bien leurs projets tout en s'assurant de leur conformité avec le cadre juridique applicable. Ces recommandations pourraient s'appuyer sur une consultation des acteurs du monde de la recherche en particulier sur les points suivants : l'accès aux données déposées sur les plateformes, la mise en œuvre des droits des personnes concernées, la définition des durées de conservation à appliquer, la mise à disposition de la communauté de recherche des jeux de données à caractère personnel ou encore les mesures de sécurité à mettre en œuvre.

Quelle protection pour les données des enfants ?

En 2018, 83 % des 12-17 ans possédaient un ordiphone (smartphone). 91% d'entre eux se connectaient tous les jours sur Internet pour y passer en moyenne 27 heures par semaine. 37 % de cette tranche d'âge effectuaient des achats en ligne (source : le baromètre 2018 du numérique réalisé par le Crédoc).

Si les mineurs sont devenus des acteurs du numérique à part entière, c'est d'abord du fait de leur utilisation, massive, **des médias sociaux** (messageries instantanées, réseaux sociaux, réseaux de partage de photos ou de vidéos) pour diffuser des informations sur eux-mêmes ou sur d'autres mineurs. Et quand ce ne sont pas les enfants qui le font, ce sont leurs parents qui publient sur Internet des photos et vidéos de leurs enfants.

On assiste aussi à la multiplication des **objets connectés dans le monde de l'enfance** - montres, bracelets, jouets connectés, jusqu'aux doudous (*cloudpets*) - et dans la vie familiale - enceintes « intelligentes », domotique, « maisons communicantes », *etc.*

Enfin, le numérique a largement pénétré le domaine scolaire et en particulier les pratiques pédagogiques, qu'il s'agisse des outils de gestion de la vie scolaire, des espaces numériques de travail, des services éducatifs en ligne, ou encore du développement du *learning analytics*.

Ces pratiques et usages numériques se traduisent par autant de traitements de données, d'analyses de traces, qui en disent énormément sur les enfants, leurs centres d'intérêt, leurs comportements, leurs déplacements, leur potentiel intellectuel, leur profil de personnalité et qui sont, de ce fait, fortement convoités. Comment protéger ces données, particulièrement sensibles s'agissant d'enfants ?

Parallèlement, nos sociétés favorisent le développement de l'autonomie et de la responsabilisation de la personne, quel que soit son âge. Il s'agit, selon l'expression de Michel Foucault, de faire de chaque individu un « entrepreneur de lui-même » et donc de privilégier chez l'enfant l'accompagnement de la découverte de son identité et de son originalité personnelles.

Une reconnaissance croissante des droits des enfants

La **Convention internationale des droits de l'enfant** de 1989 a consacré cette conception en reconnaissant à tout enfant non seulement un droit à la protection, pour compenser sa vulnérabilité, mais aussi le droit à un ensemble de prestations sociales, pour accompagner son développement, et des droits « libertés » qui doivent préparer l'enfant à sa future vie d'adulte. La Convention pose le principe de « l'intérêt supérieur de l'enfant », un concept dynamique dont la portée ne peut être évaluée qu'*in concreto*, de façon individuelle.

En France, la mutation sociétale qui est en cours s'est déjà traduite dans le droit.

De nombreuses dispositions légales autorisent les mineurs non émancipés à prendre des initiatives. Leur incapacité juridique de principe ne signifie pas l'absence de tout droit individuel.

Dans le domaine de la justice, la règle générale veut qu'un enfant puisse exercer seul ses droits, sans condition d'âge, depuis l'entrée en vigueur, en 2007, de la Convention européenne sur l'exercice des droits des enfants du 25 janvier 1996 qui vise à « promouvoir, dans l'intérêt supérieur des enfants, leurs droits, à leur accorder des droits procéduraux et à en faciliter l'exercice ». Un enfant peut ainsi porter plainte, témoigner, être entendu par le juge dans une procédure civile ou pénale, demander à bénéficier de l'aide juridictionnelle ou saisir le Défenseur des droits. Aucune condition d'âge ne peut non plus restreindre le droit d'un mineur de solliciter l'asile politique, de demander à accoucher sous X ou d'adhérer à une association.

À partir de 13 ans, un mineur peut demander une carte de donneur d'organes. Il doit donner son consentement à son adoption plénière ou à la modification de son nom.

Parfois, l'autonomisation du jeune nécessite une intervention préalable des parents. C'est ainsi qu'un jeune peut, après 16 ans, signer seul un contrat de travail ou ouvrir un compte bancaire assorti d'une carte bancaire, mais après avoir obtenu l'accord de ses parents.

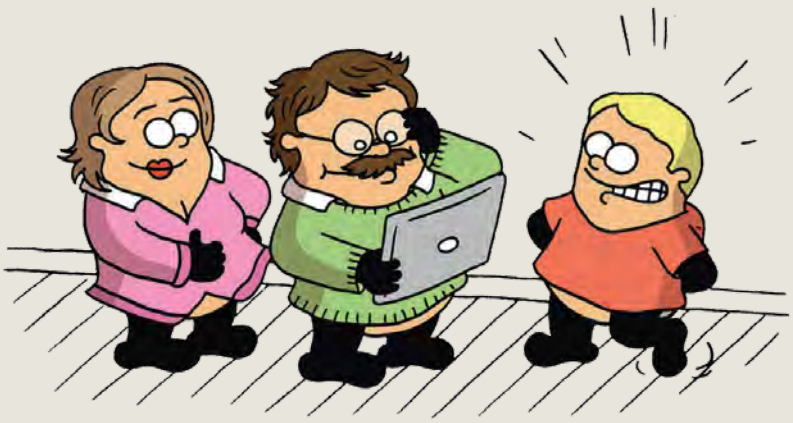
Dans d'autres circonstances, l'avis de l'enfant doit, en dernier ressort, toujours prévaloir. Lorsqu'un mineur a reçu des soins médicaux à l'insu de ses parents, il a le droit de s'opposer à ce qu'ils en soient informés. Il appartient au médecin de jouer un rôle de conciliateur en cas de conflit familial, étant entendu que la décision définitive appartient toujours à l'enfant mineur.

C'est aussi le cas lorsqu'une recherche médicale est envisagée sur un mineur. L'autorisation d'y participer doit être recueillie auprès des personnes qui exercent l'autorité parentale. Néanmoins, le participant mineur doit être consulté, dans la mesure où son état le permet, au vu d'une information qui doit être adaptée à sa capacité de compréhension. Son adhésion personnelle à la recherche doit être recherchée. S'il ne souhaite pas - ou plus - y participer, sa décision doit, en toute hypothèse, être respectée.

Garantir un droit effectif à la protection des données des enfants

C'est en matière de recherche médicale, que le droit de la protection des données personnelles des enfants a connu, en France, une première évolution législative significative. La loi pour la république numérique d'octobre 2016 a prévu qu'un mineur de quinze ans peut s'opposer à ce que ses parents aient accès aux données le concernant qui ont été recueillies à cette fin. Il peut également s'opposer à ce que ses parents soient informés d'une action de prévention, d'un dépistage ou d'un diagnostic. Le mineur est alors le seul à recevoir l'information et à pouvoir exercer ses droits.

Pour sa part, la CNIL, prenant en compte le fait que le droit français distinguait déjà selon l'âge des mineurs pour leur permettre d'accomplir seuls certains actes, s'est demandé, dès le début des années 2000, s'il ne convenait pas de permettre aux mineurs, au-delà d'un certain âge de maturité, d' accomplir certains « actes de la vie courante » sur Internet, ne serait-ce que la création d'une boîte aux lettres électronique ou l'inscription sur un site pour enfant.



Les conseils qu'elle prodigue sur son site, sur le site educnum ou via les actions de sensibilisation qu'elle mène auprès des jeunes, témoignent de sa volonté de renforcer les droits des enfants sur leurs données personnelles tout en leur assurant une protection renforcée.
Ces réflexions doivent intégrer le nouveau cadre juridique issu du **RGPD**. Celui-ci a introduit pour la première fois dans le droit de la protection des données personnelles des dispositions propres aux mineurs, considérant qu'il s'agit de personnes **particulièrement vulnérables** qui doivent bénéficier d'une protection spécifique en raison de leur moindre conscience des risques encourus en cas de traitement de leurs données personnelles, par exemple sur les réseaux sociaux. Ceci est vrai en matière de marketing et de profilage. Le RGPD prévoit ainsi que pour les services en ligne destinés aux mineurs de 16 ans et qui nécessitent le recueil du consentement, celui des parents est requis. Toutefois, les États membres peuvent prévoir dans leur droit national un âge minimal moindre, qui ne peut être inférieur à 13 ans ; en France cet âge est de 15 ans.

À cet effet, le RGPD promeut l'adoption de codes de conduite spécifiques sur la protection des données des enfants et incite les autorités de protection des données à porter une attention particulière aux activités destinées spécifiquement aux enfants.

Mais le RGPD ne se contente pas de définir un cadre protecteur pour le traitement de données relatives aux enfants. Il leur reconnaît **également des droits individuels spécifiques :**

- Leur consentement peut, à partir d'un âge fixé au niveau de chaque État (quinze ans en France), constituer le fondement légal des traitements de données liés à des offres directes de services par Internet, nonobstant l'exception de minorité.
- Le respect du principe de transparence implique que les informations destinées à des enfants soient rédigées dans des termes qui leur soient aisément compréhensibles.
- Les droits de rectification et à l'oubli sont jugés particulièrement importants lorsque le consentement au traitement des informations a été donné par un mineur.

Dans ce contexte, à l'aune du RGPD, il est important de **lancer une réflexion d'ensemble sur les droits des mineurs sur leurs données personnelles**, ainsi que sur les conditions dans lesquelles il convient de les encourager à les exercer.

C'est pour l'ensemble de ces raisons que la CNIL a décidé d'engager durant l'année une réflexion sur ces questions en concertation avec les acteurs concernés, tant les parents, les jeunes et la communauté éducative que les professionnels du numérique. Parallèlement, le groupe de travail international en éducation numérique, créé par la conférence mondiale des commissaires à la protection des données et piloté par la CNIL, a également engagé un travail sur les bonnes pratiques en matière d'information des enfants sur leurs droits.

« Le RGPD reconnaît des droits individuels aux mineurs ».

Plusieurs questions se posent au sujet de l'interprétation et de l'application du RGPD. Mais, au-delà du règlement général, il convient de s'interroger, à l'instar des travaux menés par d'autres autorités de protection des données européennes, sur les conditions dans lesquelles les enfants devront pouvoir exercer leurs droits :

- Quels dispositifs opérationnels faut-il promouvoir pour s'assurer de l'âge des enfants ?
- Dans quelles circonstances le consentement préalable des titulaires de l'autorité parentale doit-il être recueilli ?
- Comment organiser ce recueil ?
- Comment s'assurer qu'un enfant a bien été autorisé par ses parents à donner son consentement ?
- Comment adapter l'information destinée aux mineurs pour qu'elle leur soit facilement compréhensible ?
- Comment faciliter l'exercice des droits de rectification et à l'oubli spécialement ouverts aux mineurs ?
- De façon plus générale, dans quelles conditions peut-on leur reconnaitre la possibilité d'exercer directement leurs droits (d'accès, de suppression, *etc.*) et avec quelles garanties, s'agissant notamment de l'utilisation de leurs données à des fins commerciales ?

Les Ressources

LES RESSOURCES HUMAINES

Le plafond d'emploi de la CNIL est passé de 198 emplois en 2017 à 199 emplois en 2018. Il s'agit de l'effet 2018 des deux créations d'emplois décidées par la loi de finances pour 2018, dont le déploiement se poursuivra en 2019. Ces deux emplois sont spécifiquement dédiés à la préparation de l'entrée en application du RGPD et au développement d'expertises pointues en technologies de l'information. Ces deux emplois à compétences transversales ont permis d'apporter un appui technique et méthodologique aux services en vue de répondre à l'accroissement des activités. La CNIL a été en mesure de répondre à l'augmentation massive des plaintes et aux sollicitations du public en mobilisant les ressources humaines existantes, dont la charge de travail s'est accrue de manière conséquente, et en les orientant vers les activités prioritaires.

La CNIL s'est donc attachée à redéployer les compétences des équipes en charge de l'enregistrement des formalités préalables et l'accompagnement des déclarants, notamment vers les activités de développement des outils de conformité d'une part, et de traitement des demandes des usagers d'autre part.

En dépit de ces efforts, force est de constater qu'à six mois de l'entrée en application du RGPD, les besoins en ressources humaines de la CNIL restent importants au regard des enjeux soulevés par cette nouvelle régulation et les attentes des citoyens et des opérateurs publics et privés.

À cet égard, il convient de souligner les efforts d'augmentation des effectifs de nos homologues européens compte tenu du nouveau cadre réglementaire européen.

L'année 2018 a également été marquée par le transfert de deux emplois vers la Direction des services administratifs et financiers des services du Premier ministre dans le cadre des mutualisations de certaines fonctions supports.

DONNÉES SOCIALES

199 emplois fin 2018

63% de femmes

37% d'hommes

40 ans Âge moyen

8 ans l'ancienneté moyenne à la CNIL

77% des agents occupent un poste de catégorie A

44% des postes occupés par des juristes

25% des postes occupés par des assistants

18% des postes occupés par des ingénieurs / auditeurs des systèmes d'information

53% des agents travaillant à la CNIL sont arrivés entre 2013 et 2018

LES RESSOURCES FINANCIÈRES

En 2018, le budget alloué à la CNIL s'élève à **17 658 988 €** en autorisation d'engagement et en crédits de paiement, répartis comme suit : **14 474 800 €** pour le budget de personnel (titre 2) et **3 184 188 €** en autorisation d'engagement et en crédits de paiement pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6).

Le budget consacré à la masse salariale (titre 2), qui comprend la rémunération (charges incluses) des agents de la Commission et des indemnités versées aux commissaires, a été exécuté à hauteur de 96 %.

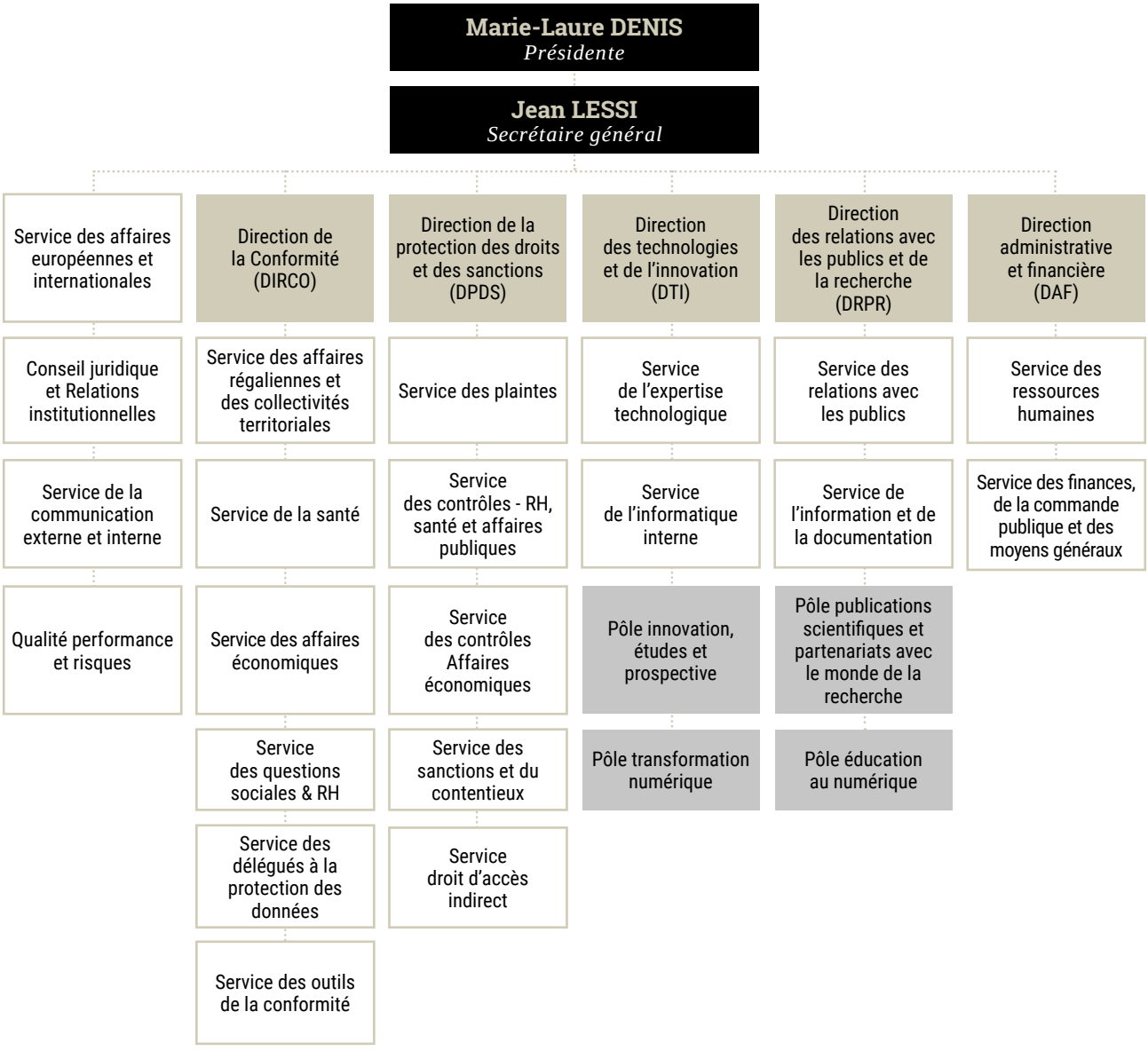
Concernant le budget hors titre 2, la consommation de cet exercice, en AE (autorisations d'engagement) et en CP (crédits de paiement), a été conforme aux prévisions annoncées dans les documents budgétaires antérieurs, avec un taux de 98,5 %.

Avec la mise en œuvre effective du nouveau cadre juridique de la protection des données personnelles, issu du Règlement général sur la protection des données (RGPD), la CNIL a dû adapter son système d'information, développer ses téléservices et les missions de contrôle, ainsi que renforcer les formations au Règlement européen et en anglais. La CNIL a également modernisé ses actions d'information et de communication en réalisant une formation en ligne ouverte à tous (MOOC) dédiée à la protection des données personnelles, mise en ligne en mars 2019.

Enfin, les dépenses de fonctionnement sur l'exercice 2018 sont impactées par la refacturation des prestations mutualisées (dont la participation au financement du Centre de documentation), aux bénéfices de la direction des services administratifs et financiers des services du Premier Ministre dans le cadre du programme Fontenoy-Ségur, à hauteur de **192 600 €** en AE et en CP.

CRÉDITS 2018	Autorisations d'engagement	Crédits de paiement
Budget LFI	**17 658 988**	**17 658 988**
Titre 2	14 474 800	14 474 800
Hors Titre 2	3 184 188	3 184 188
Budget disponible	**16 838 254**	**16 961 001**
Titre 2	14 402 426	14 402 426
Hors Titre 2	3 003 136	3 125 883
Budget consommé	**16 726 510**	**16 850 000**
Titre 2	13 762 634	13 762 634
Hors Titre 2	2 963 876	3 087 366

Organigramme des Directions et Services



Commission Nationale de l'Informatique et des Libertés
3, Place de Fontenoy - TSA 80715 - 75 334 PARIS CEDEX 07 / www.cnil.fr / Tél. 01 53 73 22 22 / Fax 01 53 73 22 00

Conception & réalisation graphique : LINÉAL 03 20 41 40 76 / www.lineal.fr

Impression et diffusion : Direction de l'information légale et administrative
Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr

Crédit photos : CNIL, Getty Image, Martin Vidberg
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 : 978-2-11-145976-2
DF : 5HC45550
Prix : 15 €

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles