2019

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

2019

Rapport d'activité

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

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

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, Xavier Gorce
Illustration de couverture : Geoffrey Dorne

Date de publication : juin 2020

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 2019

CONSEILLER & RÉGLEMENTER

33 AUDITIONS PARLEMENTAIRES

362 AUTORISATIONS DE RECHERCHE SANTÉ

160 DÉLIBÉRATIONS DONT : **117** AVIS SUR DES PROJETS DE TEXTE

ACCOMPAGNER LA CONFORMITÉ

64 900 ORGANISMES ONT DÉSIGNÉ UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

21 000 DPO DÉSIGNÉS

+ 31 % PAR RAPPORT À 2018

62 000 COMPTES CRÉÉS SUR LE MOOC* ATELIER RGPD**

2 287 NOTIFICATIONS DE VIOLATIONS DE DONNÉES

PROTÉGER

14 137 PLAINTES

+ 27 % PAR RAPPORT À 2018

4 517 DEMANDES DE DROIT D'ACCÈS INDIRECT

+ 6 % PAR RAPPORT À 2018

3 573 VÉRIFICATIONS EFFECTUÉES

*MOOC : Massive Open Online Course Description, est un outil de formation à distance
**RGPD : Règlement général sur la protection des données

INFORMER

145 913 APPELS REÇUS

17 302 REQUÊTES REÇUES PAR VOIE ÉLECTRONIQUE

8 millions DE VISITES SUR CNIL.FR

115 700 *FOLLOWERS* SUR TWITTER

35 000 FANS SUR FACEBOOK

115 000 ABONNÉS SUR LINKEDIN

CONTRÔLER & SANCTIONNER

300 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT :

53 CONTRÔLES EN LIGNE

45 CONTRÔLES SUR PIÈCES

42 MISES EN DEMEURE DONT :

2 PUBLIQUES

2 RAPPELS À L'ORDRE

2 AVERTISSEMENTS

8 SANCTIONS DONT :

7 AMENDES D'UN MONTANT TOTAL DE 51 370 000 EUROS

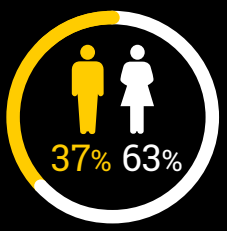
5 INJONCTIONS SOUS ASTREINTE

2 NON-LIEUX

RESSOURCES HUMAINES

BUDGET : **18,5 MILLIONS D'EUROS**

215 emplois



39 ans Âge moyen

48% DES POSTES OCCUPÉS PAR DES JURISTES

22% PAR DES ASSISTANTS

19% PAR DES INGÉNIEURS / AUDITEURS DES SYSTÈMES D'INFORMATION

80% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A

58% DES AGENTS TRAVAILLANT À LA CNIL SONT ARRIVÉS ENTRE 2014 ET 2019

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 2019

Janvier

18/01 > Publication du **6e cahier Innovation & Prospective** du laboratoire d'innovation numérique de la CNIL

21/01 > La formation restreinte de **la CNIL prononce une sanction** de 50 millions d'euros à l'encontre de la société Google LLC

22-23/01 > **La CNIL présente au 11e Forum international de la cybersécurité** (FIC)

23/01 > **Travailleurs sociaux :** La CNIL publie un kit d'information pour protéger les données de vos publics

31/01 > **La CNIL et la DGCCRF** font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et de leurs données personnelles

31/01 > **La CNIL et INRIA** décernent le prix « protection de la vie privée » 2018

Février

02/02 > Marie-Laure DENIS est nommée Présidente de la CNIL par décret du Président de la République pour un mandat de cinq ans

21/02 > **Ouverture des données publiques :** la CNIL et la CADA proposent une consultation en ligne sur leur projet de guide pratique

Mars

11/03 > La CNIL lance **sa formation en ligne** sur le RGPD ouverte à tous

28/03 > La CNIL publie un règlement type sur la **biométrie sur les lieux de travail**

Avril

11/04 > **Gestion des ressources humaines et des alertes professionnelles :** la CNIL lance une consultation publique sur deux futurs référentiels

Mai

13/05 > **Élections européennes :** pour une campagne électorale respectueuse des données personnelles

13/05 > **Développeurs :** la CNIL met en ligne un kit de bonnes pratiques

23/05 > **1 an de RGPD :** une prise de conscience inédite

27/05 > **Contrôle du blocage administratif des sites :** la personnalité qualifiée présente son 4e rapport d'activité

Juin

03/06 > Entrée en vigueur de la nouvelle **loi Informatique et Libertés et de son nouveau décret d'application**

06/06 > **Sergic :** sanction de 400 000 euros pour atteinte à la sécurité des données et non-respect des durées de conservation

14/06 > **Le conseil national des barreaux et la CNIL** renouvellent leur convention de partenariat pour 3 ans

18/06 > **Uniontrad Company :** 20 000 euros d'amende pour vidéosurveillance excessive des salariés

28/06 > **Le cadre juridique relatif au consentement a évolué,** le site web de la CNIL aussi

28/06 > **Ciblage publicitaire en ligne :** quel plan d'action de la CNIL ?

Juillet

01/07 > La CNIL lance une consultation sur le **référentiel d'agrément de l'organisme de contrôle du code de conduite**

03/07 > **Données & Design :** une nouvelle plateforme pour la communauté des designers autour du RGPD

08/07 > Sept régulateurs publient le fruit de leur approche commune sur **« la régulation par la donnée ».**

10/07 > **Sécurité des systèmes de vote par internet :** la CNIL actualise sa recommandation de 2010

12/07 > **Certification des compétences du DPO :** la CNIL délivre son premier agrément

15/07 > La CNIL lance une consultation publique auprès des **chercheurs sur les traitements de données à des fins de recherche scientifique**

18/07 > **Cookies et autres traceurs :** la CNIL publie de nouvelles lignes directrices

18/07 > **Gestion des vigilances sanitaires :** publication du référentiel pour les traitements de données personnelles

25/07 > **Active assurances :** sanction de 180 000 euros pour atteinte à la sécurité des données des clients

25/07 > La CNIL publie un nouveau modèle de registre simplifié

Septembre

02/09 > Lancement de la 4e édition du **prix CNIL-INRIA**

04/09 > **Projet de loi relatif à la bioéthique :** audition de Marie-Laure Denis devant la commission spéciale de l'Assemblée nationale

20-22/09 > **Les journées Educnum à Poitiers**

18/09 > **Collectivités territoriales :** la CNIL publie un guide de sensibilisation au RGPD

24/09 > **Droit au déréférencement :** la CJUE a rendu ses arrêts

30/09 > **Projet de loi de finances 2020 :** publication de l'avis de la CNIL sur l'expérimentation permettant la collecte de données sur les plateformes en ligne

Octobre

17/10 > **Open data :** la CNIL et la CADA publient un guide pratique de la publication en ligne et de la réutilisation des données publiques

29/10 > **Expérimentation de la reconnaissance faciale dans deux lycées :** la CNIL précise sa position

Novembre

04/11 > La CNIL lance une consultation publique sur le référentiel relatif à la **désignation des conducteurs ayant commis une infraction**

06/11 > **L'Association des maires de France et des présidents d'intercommunalité et la CNIL** signent une convention de partenariat pour la période 2019 - 2022

15/11 > **Reconnaissance faciale :** pour un débat à la hauteur des enjeux

26/11 > **Futura Internationale :** sanction de 500 000 euros pour démarchage téléphonique illégal

27/11 > **Communication politique :** la CNIL présente un plan d'action à l'occasion des élections municipales 2020

Décembre

02/12 > **La CNIL publie son registre RGPD**

04/12 > **Radars-tronçons :** mise en demeure du ministère de l'intérieur

10/12 > **Vidéosurveillance excessive de salariés au moyen de caméras connectées :** mise en demeure de la société boutique.aéro

10/12 > **La CNIL publie son avis sur le projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique**

10/12 > **Dispositifs d'alertes professionnelles :** publication du référentiel pour les traitements de données personnelles

10/12 > **Évènement :** les *civic tech* bouleversent-elles vraiment la démocratie ?

11/12 > ***Civic tech*, données et demos :** une exploration des interactions entre démocratie et technologies

12/12 > La CNIL participe au **forum de l'emploi tech de l'État**

18/12 > Mises en demeure de plusieurs **établissements scolaires pour vidéosurveillance excessive**

31/12 > **Droit au déréférencement et informations sensibles :** les éclairages du Conseil d'État

LES MEMBRES DE LA CNIL

LE BUREAU

PRÉSIDENTE

Marie-Laure DENIS,

Conseillère d'État.

Présidente de la CNIL
depuis le 2 février 2019.

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.

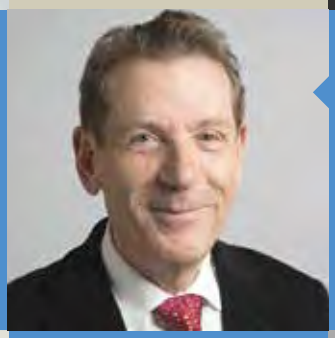
VICE-PRÉSIDENT

Éric PÉRÈS

Membre du Conseil économique,
social et environnemental.

Secteur : Environnement,
transports et énergie.
Éric PÉRÈS est membre de la CNIL
depuis décembre 2010,
puis vice-président depuis février 2014.

LES MEMBRES (COMMISSAIRES)



Alexandre LINDEN

Conseiller honoraire à la Cour de cassation,
Président de la formation restreinte
de la CNIL.

Secteur : Travail et ressources humaines
(formation professionnelle, recrutement,
cybersurveillance, etc.)

LES MEMBRES ÉLUS DE LA FORMATION RESTREINTE

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

Philippe-Pierre CABOURDIN

Conseiller maître à la Cour des comptes,
vice-président de la formation restreinte
de la CNIL.

Secteur : Banque, assurance et fiscalité

Dominique CASTERA

Membre du Conseil économique,
social et environnemental.

Secteur : Vie politique et citoyenne

Marc DANDELOT

Conseiller d'État honoraire,
Président de la CADA (Commission
d'accès aux documents administratifs)

Anne DEBET

Professeur des universités

Secteur : Données publiques
et recherche / Délégués à la protection
des données et nouveaux outils
de conformité

Bertrand du MARAIS
Conseiller d'État

Secteur : Communications électroniques et Technologies innovantes / Plateformes en ligne / Europe et international

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

Loïc HERVÉ
Sénateur de la Haute-Savoie

Secteur : Travail et ressources humaines (formation professionnelle, recrutement, cybersurveillance, etc.)

Christian KERT
Président du conseil d'orientation pour la prévention des risques naturels majeurs

Secteur : Sport, médias et culture

Sylvie LEMMET
Conseillère maître à la Cour des comptes

Secteur : Défense / Administration numérique

Christine MAUGÜE
Conseiller d'État

Secteur : Justice

François PELLEGRINI
Professeur des universités à l'université de Bordeaux

Secteur : Commerce et publicité / Cybersécurité / Europe et international

Valérie PEUGEOT
Chercheuse au sein d'Orange Labs et Présidente de l'association Vecam

Secteur : Santé et assurance maladie

Sylvie ROBERT
Sénatrice d'Ille-et-Vilaine

Secteur : Éducation et enseignement supérieur

COMMISSAIRE DU GOUVERNEMENT
• Nacima BELKACEM • Adjointe : Ève JULLIEN

AVANT-PROPOS DE LA PRÉSIDENTE

Marie-Laure DENIS
Présidente de la CNIL

2019 : UNE RÉGULATION DES DONNÉES EN PLEINE EXPANSION

Pour la deuxième année consécutive, la CNIL constate des chiffres inédits, témoignant de la très forte mobilisation autour du RGPD (règlement général sur la protection des données) de la part de tous les publics : des indicateurs qui montrent que la CNIL est un service public de premier plan.

2019, UNE ANNÉE RICHE DE MISE EN PRATIQUE OPÉRATIONNELLE

Le constat est indéniable : un an après l'entrée en application du RGPD, l'année 2019 démontre que le RGPD est au cœur des préoccupations des Français et des Européens. Cette année a été marquée par un nombre toujours plus élevé de plaintes adressées à la CNIL et par la coopération avec ses homologues européens devenue une réalité quotidienne. L'année 2019 en chiffres, c'est notamment plus de 14 000 plaintes, soit plus de 27 % d'augmentation par rapport à l'année précédente, dont 20 % de plaintes transfrontalières, 145 000 appels, 8 millions de

visites sur notre site web et 17 300 requêtes électroniques sur Besoin d'aide, soit 12 % d'augmentation sur la même période. En parallèle, près de 65 000 organismes ont désormais déclaré un délégué à la protection des données (DPO).

La CNIL s'est pleinement emparée du nouveau cadre juridique. Elle a activé les nouveaux seuils de sanction prévus par le RGPD, à l'image de la sanction Google de janvier 2019, qui reste encore, **à ce jour, la sanction la plus importante en Europe** décidée par les autorités de protection de données. D'autres sanctions à l'encontre d'entreprises de tailles variables, dans différents secteurs et sur différents sujets, ont été prises, pour un montant total de 51 370 000 euros.

De nombreux outils d'accompagnement à la conformité RGPD ont été développés, parmi lesquels nos premiers outils de droit souple, notre cours en ligne ouvert à tous (MOOC) qui compte aujourd'hui plus de 62 000 créations de compte, le guide pratique à destination des collectivités territoriales, le guide *open data* en collaboration avec la CADA ou le site design.cnil.fr.

Même au niveau mondial, nous constatons que le RGPD reste présent dans l'actualité politique et médiatique, trois ans après son adoption et un an demi après son application effective. C'est assez rare, voire inédit, pour un texte européen. Il est donc de notre responsabilité d'assurer le succès de cette nouvelle règlementation, en tant qu'outil de protection des citoyens, de confiance dans l'univers numérique et enfin de souveraineté. C'est pourquoi la CNIL prend une part active au débat sur la gouvernance mondiale des données et la promotion du modèle européen. Elle est très investie sur tous les grands dossiers actuels : *Cloud Act, Privacy Shield,* adéquation du Japon et bientôt de la Corée du Sud, pour ne citer que quelques exemples.

2020, UNE ANNÉE POUR CONSTRUIRE DES SOLUTIONS

Outre les garanties nécessaires à la libre circulation des données, ainsi que la nécessité capitale de maintenir un internet ouvert, des questions telles que l'accès, la surveillance et la localisation par les pouvoirs publics sont devenues des préoccupations croissantes.

Que ce soit au niveau des personnes, des professionnels ou du collectif européen, **la CNIL a pour objectif de construire des solutions durables,** respectueuses des textes et appliquées par tous, pour poser un cadre de confiance sécurisant pour les entreprises et les consommateurs. Cela se traduira par cinq axes stratégiques devant guider notre action d'ici 2021.

1. Donner la priorité aux enjeux numériques de la vie quotidienne des Français.

La CNIL sera l'alliée de confiance du quotidien numérique des citoyens. Nous enrichirons l'offre éditoriale du site internet pour les particuliers, notamment des jeunes, au cœur de notre action. Nous renforcerons également la lisibilité et la simplicité de la parole de la CNIL pour fournir, plus encore que par le passé, des réponses clés en main, des recommandations pratiques et des outils numériques pour protéger efficacement sa vie privée. Nous axerons enfin l'ensemble de nos missions sur le quotidien numérique des Français, afin d'améliorer, dans les faits, leur degré de contrôle sur leurs données.

« La CNIL : une alliée du quotidien numérique. »

« Le fil rouge de 2020 sera l'appropriation par tous et la concrétisation pour tous des promesses et potentialités du RGPD. »

2. Assumer une régulation équilibrée de la protection des données entre répression et accompagnement.

La CNIL doit s'assurer que la protection des données entre définitivement dans les mœurs et la culture quotidienne des organismes publics et privés, conditions impérative du succès du RGPD. Son action d'accompagnement sera plus hiérarchisée, adaptée et priorisée sur les collectifs, professionnels ou de la société civile, ainsi que sur les types de traitements de données présentant le plus fort impact, par leur nature ou leur ampleur, sur les personnes et le monde de demain. Pour faire écho à cette responsabilité accrue donnée aux organismes dans la gestion de leurs traitements de données, la CNIL s'investira pleinement dans les actions répressives, qui ont pris une nouvelle ampleur avec le RGPD.

3. Prendre une part active, dans la mesure de nos moyens, à la géopolitique internationale de la donnée, en lien avec la diplomatie française.

La voix de la CNIL sera portée à l'international, au sein du collectif européen, où l'approche coopérative doit faire émerger une culture commune et une efficacité visible pour tous, et dans les arènes d'influence mondiale, où se joueront dans les années à venir les grands équilibres géopolitiques en matière de protection des données. Assise sur sa longue expérience d'autorité administrative indépendante, la CNIL doit continuer à contribuer au succès du nouveau modèle de gouvernance de la donnée, qui est la clé d'une véritable souveraineté numérique européenne en la matière.

4. Offrir une expertise publique de pointe sur le numérique et la cybersécurité.

La cybersécurité est devenue un enjeu majeur pour les entreprises et les organismes publics. La CNIL dispose d'une expertise technique de premier plan dans le paysage de cette régulation qu'elle doit approfondir, notamment en matière de cybersécurité. Pour apporter aux défis qu'elle rencontre une réponse plus complète, et donner à l'État dans son ensemble une capacité globale de réponse efficace, elle doit promouvoir et participer à la mise en réseau des expertises et outils avec les autres régulateurs et composantes de l'État numérique. Elle poursuivra également son investissement dans d'autres approches, en particulier économiques et éthiques, au service d'une vision toujours plus moderne de la régulation du numérique.

5. Incarner un service public innovant et rassemblé autour de ses valeurs.

Enfin, la CNIL se doit d'être exemplaire dans l'exercice de ses missions comme vis-à-vis de ses agents. La régulation des données personnelles dans le monde numérique ne peut se faire en chambre ; elle impose au contraire une dynamique continue de confrontation au réel, de vérification du bien-fondé des actions et décisions au regard de leurs effets dans le temps. Cet impératif se déclinera sur plusieurs niveaux. Au niveau du recrutement tout d'abord, la CNIL se fera un devoir de refléter ces valeurs humanistes qui la portent à l'heure où le numérique bouleverse les rapports sociaux et professionnels. Ensuite, la CNIL approfondira les atouts offerts par le numérique dans ses outils pour répondre davantage aux attentes de ses publics.

De grandes étapes ont été franchies en 2019, du chemin reste néanmoins à parcourir pour achever la transformation et parvenir à une culture Informatique et Libertés pleinement partagée et diffusée dans le pays.

MOT DU SECRÉTAIRE GÉNÉRAL

Louis DUTHEILLET DE LAMOTHE
Secrétaire général

POUR QUE L'INFORMATIQUE SOIT TOUJOURS AU SERVICE DE CHAQUE CITOYEN

Chaque rapport d'activité de la CNIL est l'occasion d'un constat semblable. Ce constat, c'est celui d'une année de mobilisation pleine et entière des équipes de la CNIL dans l'accomplissement de leur mission de service public, face à une charge croissante. Les chiffres, détaillés tout au long du présent rapport, les témoignages des agents et la description de leurs actions, illustrent l'engagement de chacun pour répondre à une activité accrue liée aux sollicitations et aux enjeux auxquels la CNIL doit faire face. Je souhaite en particulier commencer ces quelques mots en saluant l'action, en 2019 et pendant tout le temps où il a été en poste, du précédent secrétaire général, Jean Lessi, qui a quitté ses fonctions le 10 avril 2020.

DES OUTILS ADAPTÉS À DE NOUVEAUX BESOINS

Les causes de cette charge sont multiples. Il s'agit, bien sûr, d'assumer les nouvelles missions confiées à la CNIL par le législateur européen et français (certification, outils de droit souple, accompagnement des délégués à la protection des données, réponse aux analyses d'impact relatives à la protection des données – ou AIPD –, gestion des notifications de violations, instruction des codes de conduite, etc.). Il s'agit aussi de mettre en œuvre de nouvelles méthodes de travail, et notamment la coopération avec nos homologues, objectivement chronophages, mais si précieuses pour répondre tant à l'attente de cohérence et de sécurité juridique des entreprises qu'au besoin de protection renforcée des citoyens à l'échelle géographique pertinente : l'Europe. Il s'agit, également, de s'adresser plus encore que par le passé à certains publics dont les besoins spécifiques appellent une réponse et des outils adaptés, notamment les plus petites structures publiques (petites communes et petits établissements publics) et privées (TPE-PME). Il s'agit, surtout, toutes missions, toutes méthodes et tous publics confondus, individus comme professionnels, de faire face à des exigences de protection et de conseil plus fortes que jamais, portant sur les nouveautés du RGPD, mais

« Les besoins spécifiques de certains publics appellent une réponse et des outils adaptés. »

comportant aussi une importante part de rattrapage des droits et obligations existant depuis 1978.

Ce qui est frappant, au-delà des chiffres ou même de l'activité non chiffrable, c'est de constater que par tous ces capteurs se manifestent, non seulement une soif de maîtrise des personnes sur leurs données, non seulement une appropriation (en progrès) par les opérateurs de leur responsabilité, mais aussi des transformations majeures de notre société, déjà bien connues, mais dont la protection des données est un prisme assez saisissant.

DES SUJETS DE RÉFLEXION MULTIPLES

Ces enjeux cruciaux transparaissent à travers plusieurs thématiques dont la CNIL a eu à connaître en 2019 : le lancement du débat – auquel elle avait appelé – sur la reconnaissance faciale et les nouveaux usages de la vidéo, qui renvoie entre autres à la question si fondamentale de l'anonymat dans l'espace public et des formes de surveillance légitimes ; le chantier en cours sur l'identité numérique, porteur de tant d'opportunités mais interrogeant la possibilité – mise en défi par le numérique depuis l'origine – de compartimenter notre vie citoyenne, commerciale, professionnelle en ligne, et invitant ainsi à la construction de solutions équilibrées ; la montée en puissance des assistants vocaux et des agents conversationnels, et les questions qu'elle soulève, au-delà de l'usage des données et de l'intimité, sur les rapports homme-machine.

La CNIL a également fait face à la diffusion d'une délinquance numérique, dont les cyberattaques et les multiples atteintes aux personnes en ligne, qui se nourrit de mésusage de nos données personnelles, qui frappe les petits comme les gros opérateurs et, par ricochet, les personnes ; la démultiplication de la puissance de traçage des individus en ligne par des acteurs transnationaux, notamment privés, toujours plus importants ; le risque de fracture numérique aux dépens d'une partie de la population, se doublant d'une capacité trop inégale à protéger ses données, et la nécessité de penser l'éducation et l'accompagnement numériques sous un jour nouveau.

Ces différents sujets, individuellement ou mis bout à bout, ont quelque chose de vertigineux. Ils confirment chaque jour l'actualité de l'article 1er de la loi Informatique et Libertés et de son appel à la vigilance, pour que l'informatique soit toujours « au service de chaque citoyen » et que son développement se fasse dans le respect de « l'identité humaine » et de nos libertés fondamentales. Plus que jamais, réguler l'usage des données personnelles, c'est gérer une tâche quotidienne – le volume des saisines, pour faire simple – tout en gardant à l'esprit cette tectonique des plaques.

VERS UNE COOPÉRATION ENTRE TOUS LES ACTEURS

La CNIL y contribue, avec des moyens qui devront poursuivre leur progression pour saisir les opportunités et lutter réellement contre les menaces du moment. L'objectif n'est évidemment pas qu'une institution, aussi centrale soit-elle dans le sujet, soit capable de tout faire toute seule. Au contraire, l'ordre public nécessaire dans l'espace numérique ne peut être assuré que par une conjonction des régulations et des interventions publiques, y compris juridictionnelles, dont la force doit globalement être renforcée. De même, une priorité est que, par un effort partagé (par de nombreux acteurs publics, privés, de la société civile) et partenarial d'éducation au numérique, les personnes soient mieux armées pour maîtriser leurs données, leurs usages, et pour avoir une force autonome d'action dans ce nouveau contexte. Une autre priorité est que les entreprises et plus largement tous les innovateurs inventent de nouveaux modèles vertueux de produits, de services et de services publics, dessinant un écosystème numérique respectueux des personnes, inclusif, durable, social.

C'est dans ce sens que la CNIL restera engagée en 2020 au service de la cause si bien décrite par l'article 1er de notre loi, modernisée et relayée au niveau européen par le RGPD il y a deux ans.

Analyses

Retour sur le plan d'action de la CNIL sur les cookies

Depuis plus de 20 ans, les cookies sont au cœur des solutions publicitaires sur internet. Ils permettent d'enregistrer les données personnelles des utilisateurs et d'analyser leur comportement. Faisant application du cadre juridique français et européen (RGPD, directive ePrivacy, loi Informatique et Libertés), la CNIL répond aux préoccupations des internautes, d'une part, et accompagne les acteurs du marketing numérique dans leur mise en conformité, d'autre part.

La CNIL et les cookies : une histoire pas si récente...

1994

Lou Montulli et **John Giannandrea** proposent une solution permettant de stocker un état dans un nouvel objet qu'ils décident d'appeler *« **Persistent Client State HTTP Cookies** »* ou « **cookie** ».

Première bannière publicitaire sur le site HotWired

1996

La société DoubleClick (rachetée en 2007 par Google) est créée pour exploiter ces cookies tiers pour la publicité, et invente l'une des méthodes de publicité en ligne les plus populaire : **le reciblage *(retargeting)*.**

1998

Oingo propose une méthode de publicité contextuelle : **un algorithme analyse le contenu des pages pour proposer des publicités relatives aux contenus visités.**

2002

Adoption de la **directive vie privée et communications électroniques** (ePrivacy) qui oriente les professionnels sur les bonnes pratiques en termes de traitement de données personnelles et de prospection commerciale en ligne.

2003

Google rachète Oingo et renomme le système **AdSense**

DÉFINITIONS

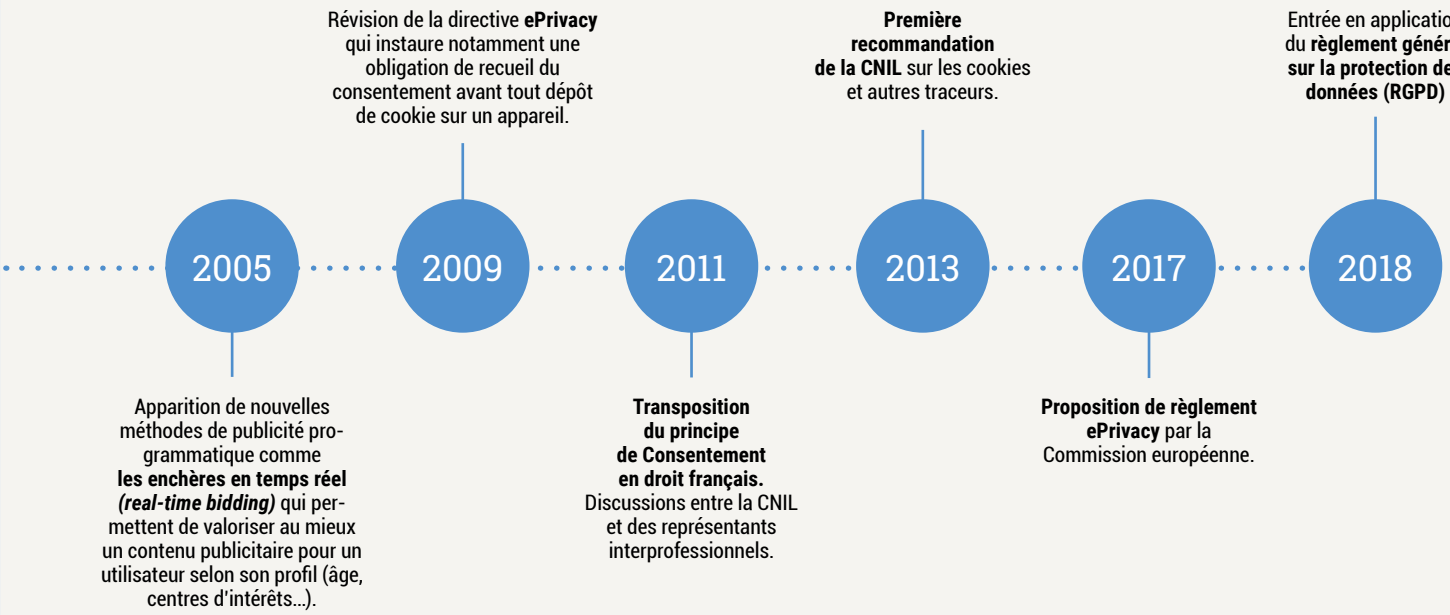
Un cookie (ou témoin de connexion) est un petit fichier envoyé par les sites web visités à un utilisateur et stocké sur le terminal utilisé pour la navigation (par exemple un ordinateur personnel, un téléphone). Il permet de conserver un état, c'est-à-dire une mémoire des évènements antérieurs comme une authentification à un site ou la constitution d'un panier d'achat. Les cookies peuvent contenir des données personnelles. Il résulte de l'article 82 de la loi Informatique et Libertés que l'utilisateur doit consentir avant toute opération d'écriture ou de lecture d'un cookie sur un terminal, à l'exception des cas dans lesquels le cookie est strictement nécessaire au fonctionnement du service en ligne auquel l'utilisateur veut accéder.

Les **cookies « nécessaires »**, internes, permettent d'enregistrer des informations entre deux consultations d'un même site web sur un même appareil. Ils permettent d'enregistrer un panier d'achat, des identifiants de connexion ou encore des éléments de personnalisation de l'interface. Ils ne requièrent pas de consentement de la part de l'utilisateur.

Les **cookies « statistiques »** permettent à un site de suivre les actions d'un internaute sur un site web. Lorsque les statistiques sont anonymes (c'est-à-dire ne permettent pas de retrouver une personne), le consentement de l'utilisateur n'est pas nécessaire.

Les **cookies « non nécessaires »** au fonctionnement du service demandé par l'utilisateur supposent un consentement de la part de celui-ci :

- Les **cookies « internes »** ou ***« first-party »*** sont déposés par le site consulté. Ils peuvent être déposés en plus des cookies nécessaires et peuvent être utilisés pour collecter des données personnelles, suivre le comportement de l'utilisateur et servir à des finalités publicitaires.
- Les **cookies dits « tiers »**, **« tierce partie »** ou ***« third party »*** sont des cookies déposés par (ou pour) un site B (souvent une régie publicitaire) sur un site A : cela permet au site B de voir quelles pages ont été visitées sur le site A par un utilisateur et de collecter des informations sur lui.



DE LA DIRECTIVE AU RÈGLEMENT EPRIVACY EN EUROPE

La nécessité d'encadrer la technologie potentiellement très intrusive des cookies s'est traduite par l'adoption de la directive ePrivacy en 2002. Cette directive complète et précise le cadre général applicable au traitement des données personnelles (directive 95/46 du Parlement européen et du Conseil puis RGPD) dans le domaine des communications électroniques. Elle spécifie notamment des règles relatives aux pratiques de prospection commerciale en ligne, aux opérations de suivi de navigation, aux traitements de données réalisés par des opérateurs de télécommunications, etc.

La révision de cette directive en 2009 a conduit à renforcer la protection de l'intégrité des appareils connectés en instaurant, à son article 5.3, une obligation de recueil du consentement préalable avant toute opération consistant à inscrire ou à accéder à des informations stockées dans ces terminaux (en particulier le dépôt ou la lecture de cookies ou autres traceurs sur les appareils connectés). L'article 5.3 de cette directive a été transposé en droit français à l'article 82 de la loi Informatique et Libertés.

Afin d'assurer une bonne articulation entre le RGPD et la directive ePrivacy, la Commission européenne a publié une proposition de règlement ePrivacy le 10 janvier 2017 : le projet de texte conserve l'idée d'une protection renforcée des communications électroniques, en ce que celles-ci peuvent révéler des données « très sensibles et personnelles »[1]. Ainsi, le consentement des personnes demeure la clé de voûte permettant de préserver la confidentialité de leurs communications électroniques, de protéger leurs terminaux ou encore de leur épargner des formes de prospection commerciale jugées trop envahissantes.

Les discussions, qui ont pris du retard, sont toujours en cours aujourd'hui au niveau européen, pour déterminer les contours de ce futur texte d'application directe dans l'ensemble des États membres. Dans l'attente de son adoption, la directive ePrivacy révisée en 2009 reste applicable.

INFOSPLUS

Quelle est la différence entre RGPD et directive ePrivacy ?

Le RGPD et la directive ePrivacy sont complémentaires :

Le RGPD, qui se fonde sur l'article 8 de la Charte des droits fondamentaux de l'Union européenne, vise à encadrer le traitement des données personnelles.

La directive ePrivacy se base, quant à elle, sur l'article 7 de cette Charte et s'attache à encadrer les communications électroniques et, plus particulièrement, l'usage des cookies.

COMMENT LA CNIL FAIT-ELLE APPLIQUER CES RÈGLES EN FRANCE ?

Début 2017, l'annonce de la révision de la directive ePrivacy, sous forme de règlement d'application directe, a conduit la CNIL à suspendre ses actions sur la question des cookies. L'objectif de la Commission européenne était, en effet, d'aboutir à une adoption du règlement en mai 2018, parallèlement à l'entrée en application du RGPD. Toutefois, les discussions se sont poursuivies au-delà de cette date et les délais des négociations en cours sur ce texte sont encore difficiles à prédire.

Pour tenir compte des incertitudes liées au délai d'adoption de ce nouveau texte et de la nécessité de clarifier certaines pratiques non respectueuses des droits des personnes, la CNIL a choisi en 2019 de faire du ciblage publicitaire une priorité pour plusieurs raisons :

- Cette pratique soulève des enjeux de protection des données très forts pour les personnes de par son caractère massif et parfois très intrusif. La CNIL observe une forte prise de conscience citoyenne s'agissant du traçage en ligne, en particulier depuis l'entrée en vigueur du RGPD, qui a fait naître des inquiétudes mais également des attentes en matière de protection des données en ligne.
- En droit, le RGPD, entré en application le 25 mai 2018, soit depuis près de deux ans, a renforcé les exigences en ce qui concerne les modalités de recueil du consentement, qui doit désormais être libre, éclairé, explicite et univoque. Ces nouvelles exigences sont applicables dans le champ de la directive ePrivacy (qui renvoie au RGPD sur ce point).

1 Considérants 2 et 9 de la proposition de règlement « vie privée et communications électroniques » du 10 janvier 2017.

« 11 % des internautes expliquent que ce sont les « spams, sollicitations commerciales, vente de listes contacts par les entreprises » qui les ont rendus sensibles à la question de la protection des données. »

Ainsi, la simple poursuite de la navigation sur un site, qui était une modalité valable d'expression du consentement avant mai 2018, ne peut plus, désormais, traduire un consentement valide de l'utilisateur au dépôt de cookies.

- Le ciblage publicitaire au moyen de cookies est au cœur de nombreuses plaintes, qui mettent notamment en avant que le consentement de l'utilisateur n'est pas valablement recueilli. La CNIL est dans l'obligation de traiter dans un délai raisonnable les plaintes dont elle est saisie.

- Les professionnels du secteur du marketing en ligne ont eux-mêmes exprimé leur souhait de mieux comprendre leurs obligations issues du RGPD et de la directive ePrivacy.

- Enfin, d'autres autorités de protection des données se sont saisies de ce sujet (Royaume-Uni, Belgique, Grèce, Pays-Bas, etc.) pour tirer, concernant les cookies et autres traceurs, toutes les conséquences des nouvelles exigences du RGPD concernant le consentement.

La CNIL a donc décidé de mettre en œuvre un plan d'action en plusieurs étapes :

- **juillet 2019 :** publication de lignes directrices sur les cookies et autres traceurs, rappelant l'état du droit issu du RGPD ;

- **septembre-novembre 2019** : concertation avec des organisations représentatives des professionnels et de la société civile ;

- **décembre 2019 :** projet de recommandation sur les cookies et autres traceurs, visant à préciser les modalités opérationnelles de mise en œuvre des nouvelles exigences applicables au recueil du consentement des utilisateurs ;

- **janvier 2020 :** lancement d'une consultation publique sur ce projet de recommandation ;

- **à venir :** publication de la recommandation finalisée.

La CNIL a ainsi choisi de laisser aux opérateurs une période de 6 mois d'adaptation à la nouvelle recommandation (à compter de la publication définitive de celle-ci), avant de démarrer ses investigations pour vérifier le respect des nouvelles obligations issues du RGPD en matière de recueil du consentement. Le Conseil d'État a, dans une décision du 16 octobre 2019, validé cette approche progressive.

Répondre aux préoccupations des citoyens

Au cours des deux dernières années, les plaintes portant sur les mécanismes de traçage en ligne aux fins de ciblage publicitaire se sont multipliées. Ainsi, l'équipe à l'origine du navigateur Brave ainsi que l'association Open Rights Group ont déposé des plaintes, en 2018, contre Google et contre d'autres sociétés du secteur de *« l'ad tech »* recourant à des mécanismes d'enchères en temps réel (désignés sous l'acronyme *RTB* pour *real-time bidding*), auprès des autorités de contrôle irlandaise et britannique.

De même, l'association britannique Privacy International a attaqué sept acteurs internationaux du marché publicitaire, qui procèdent à la collecte à grande échelle de données personnelles. Parallèlement, les associations None of your business et Panoptykon Foundation ont également saisi plusieurs autorités de contrôle sur ces thématiques en ciblant plusieurs acteurs majeurs du numérique, influents dans le monde de la publicité en ligne.

Ces plaintes ont souvent été déposées dans plusieurs États membres à la fois, activant un mécanisme de coopération entre les régulateurs des différents pays européens. Elles traduisent une inquiétude croissante des citoyens quant à la réalité du traçage et de la collecte de leurs données personnelles en ligne ainsi qu'un sentiment général de défiance palpable à différents titres. Ainsi, un sondage IFOP pour la CNIL réalisé en octobre 2019[2] fait ressortir que 11 % des internautes expliquent que ce sont les « spams, sollicitations commerciales, vente de listes contacts par les entreprises » qui les ont rendus sensibles à la question de la protection des données, derrière le « piratage et vol de données » (27 %) juste devant le rapport aux GAFA (8 %). Plus généralement, 54 % se disent également plus inquiets qu'il y a quelques années quant à la présence de publicité ciblée sur des sites web.

La CNIL a également publié quatre baromètres depuis 2014, autour des pratiques numériques des internautes (2015[3], 2016[4], 2018[5], 2019[6]). Le taux d'internautes français ayant utilisé un bloqueur de publicités sur leur ordinateur est passé de 36 % à 54 % de 2015 à 2019. Si la principale raison est de ne plus voir les publicités

2 « Les Français et la protection des données personnelles », octobre 2019, sondage IFOP pour la CNIL réalisé auprès d'un échantillon de 1 004 personnes représentatif de la population française âgée de 18 ans et plus

3 « Pratiques numériques et vie privée : l'âge de la maturité pour les internautes français ? », 2016, linc.cnil.fr

4 « Pratiques numériques et vie privée en 2016 : des internautes pragmatiques », 2016, linc.cnil.fr

5 « Baromètre LINC : des utilisateurs plus passifs vis-à-vis des assistants vocaux que des smartphones ou navigateurs », 2018, linc.cnil.fr

6 « [Baromètre LINC 2019] - Les pratiques de protection des données progressent », 2019, linc.cnil.fr

« 65 % de ces personnes estiment que les demandes d'autorisation de dépôt de cookies actuelles sont inefficaces. »

intrusives, les personnes interrogées soulignent également à 33 % qu'il s'agit de protéger leurs données personnelles. Ces chiffres recoupent ceux obtenus à l'issue d'un sondage IFOP commandé par la CNIL en décembre 2019 sur les « Français et la réglementation en matière de cookies ». Ainsi, 70 % des personnes interrogées estimaient indispensable d'obtenir à chaque fois leur accord, même si cela prend un peu plus de temps dans la navigation sur les sites concernés, avant tout dépôt de traceurs. Pour autant, 65 % de ces personnes estiment que les demandes d'autorisation de dépôt de cookies actuelles sont inefficaces. De même une écrasante majorité de ces personnes (90 %) estime nécessaire de connaître l'identité des entreprises susceptibles de suivre leur navigation sur le web.

Ces sondages dénotent clairement une prise de conscience massive ainsi qu'une aspiration collective à plus de transparence et de maîtrise des pratiques de traçage en ligne.

CookieViz et les outils de la CNIL

Une des missions de la CNIL est de favoriser la sensibilisation du public et sa compréhension des enjeux de la protection de leurs données. Cette mission est particulièrement importante sur le sujet du suivi du comportement des utilisateurs de sites web ou d'applications mobiles, de nombreuses pratiques s'étant développées sans que les utilisateurs ne le sachent.

Cette asymétrie est particulièrement présente dans l'usage des cookies qui sont longtemps restés un concept obscur pour le plus grand nombre. Si leur existence est désormais connue du grand public, la prise de conscience de l'ampleur de leur utilisation reste nécessaire pour permettre un débat factuel sur la question, et une meilleure compréhension de la législation.

Dans ce cadre, la CNIL avait développé en 2013 l'outil CookieViz, un outil de visualisation pour mesurer l'impact des cookies et autres traceurs lors de votre propre navigation. Cet outil a récemment été mis à jour afin d'en faciliter l'utilisation et de lui apporter de nouvelles fonctionnalités. Premier logiciel à destination du grand public développé en interne par la CNIL, CookieViz est en outre un logiciel libre (licence GPLv3) qui peut être repris par tout un chacun. Cet outil analyse en direct les interactions de votre navigateur avec les différents serveurs sollicités lors du chargement d'une page web, afin d'identifier les cookies utilisés, présentant ainsi une visualisation dynamique du traçage auquel l'utilisateur est soumis.

Plus globalement, la CNIL cherche également à faciliter la mise en conformité avec la réglementation des entreprises et organismes publics. Elle travaille ainsi activement à fournir une palette d'outils facilitant le travail des responsables de traitement. L'outil PIA, qui permet de faciliter la réalisation des analyses d'impact relatives à la protection des données et le guide RGPD du développeur sont deux exemples récents d'outils visant à accompagner la mise en conformité des responsables de traitement.

Par ailleurs, dans le cadre de la publication de la recommandation « cookies et autres traceurs », la CNIL travaille à rendre disponibles des outils de mise en conformité, que ce soit en limitant au maximum l'usage de traceurs ou, lorsqu'ils sont incontournables, en proposant des outils permettant un recueil du consentement respectueux des bonnes pratiques proposées par la CNIL.

La politique répressive de la CNIL

Les actions menées par la CNIL au titre de ses pouvoirs de contrôle à posteriori se dérouleront en deux temps.

Tout d'abord, sur la base de plaintes qu'elle a reçues, la CNIL a initié dès 2019 des investigations qui se prolongent au 1er trimestre 2020. Le périmètre de cette première série de contrôles porte principalement sur le respect des principes en vigueur depuis la révision de la directive ePrivacy intervenue en 2009, inchangés avec le RGPD, notamment le caractère préalable du consentement au dépôt de traceurs, l'information adéquate de l'utilisateur, ou encore la possibilité pour celui-ci de retirer effectivement son consentement. Lorsque des manquements sont mis en évidence, ils feront le cas échéant, en fonction de leur nature et de leur gravité, l'objet de mesures correctrices. Il s'agit, pour la CNIL, de mettre un terme à des manquements pour lesquels les obligations sont claires depuis plusieurs années.

Dans un deuxième temps, une fois la période d'adaptation écoulée, six mois après la publication de sa nouvelle recommandation, la CNIL conduira de nouvelles missions de contrôle. Elle vérifiera alors le respect plein et entier des obligations de la loi Informatique et Libertés, y compris des nouveautés résultant de l'entrée en application du RGPD, en matière de traceurs et cookies, telles qu'éclairées par cette recommandation.

GROS OU PETITS ACTEURS, LES MÊMES RÈGLES POUR TOUS

Il est parfois avancé que l'application de la directive ePrivacy favoriserait les géants du numérique, en particulier les « GAFA », ceux-ci pouvant alors utiliser leurs univers authentifiés (ou « loggués ») pour obtenir plus facilement le consentement des utilisateurs.

Le fait que l'utilisateur soit authentifié ne dispense aucunement de recueillir son consentement, dès lors que des traceurs non exemptés de consentement sont utilisés. L'existence d'une relation antérieure avec l'utilisateur via un compte n'a pas d'impact sur la nécessité de recueillir un consentement valable pour ces traceurs. En conséquence, tous les acteurs sont soumis aux mêmes règles si eux ou leurs utilisateurs sont situés en Europe.

Par ailleurs, le fait d'utiliser un seul traceur pour de multiples finalités n'exonère pas non plus de recueillir le consentement pour les finalités qui le nécessitent.

Par exemple, si un cookie d'authentification est également utilisé à des fins de ciblage publicitaire, le consentement de l'internaute devra être recueilli pour cette dernière finalité ; le consentement devra être recueilli de la même manière lorsque l'utilisateur n'est pas identifié, de façon complètement indépendante d'une éventuelle acceptation de conditions générales d'utilisation du service.

Cela signifie donc que les environnements authentifiés seront contrôlés de la même manière que les autres sites web ou applications mobiles, et subiront les mêmes conséquences en cas de non-conformité à la réglementation.

Ainsi, s'il existe des différences objectives de choix de modèles économiques, de masses de données traitées dans ces environnements authentifiés, ou de notoriété auprès des consommateurs, les règles sont les mêmes pour tous, et s'appliquent de la même manière. Si la réglementation en matière de protection de la vie privée n'a pas pour objet de résoudre d'éventuelles situations de concurrence déloyale, elle n'en crée pas non plus.

LA POSITION DES AUTRES ÉTATS DE L'UNION EUROPÉENNE

La CNIL n'est pas la seule autorité européenne à s'être emparée du sujet de la publicité ciblée. À titre d'exemple, **l'autorité néerlandaise** a énoncé, courant 2019, que les *« cookies walls »* (pratique consistant à priver d'accès à un site ou service les personnes ne consentant pas au dépôt de traceurs) ne sont pas conformes à la réglementation. **L'autorité belge** de protection des données (APD), qui partage cette position dans sa recommandation sur le marketing direct[7], préconise de permettre à l'utilisateur de consentir finalité par finalité, plutôt que de recourir à un mécanisme de consentement global. **L'autorité bavaroise** a, quant à elle, annoncé qu'elle avait lancé une enquête généralisée sur les pratiques de 40 sites web, en précisant qu'aucune d'entre elles n'est conforme à la réglementation, et en laissant entrevoir la possibilité de sanctions. Son analyse se fonde notamment sur la transparence, le consentement qui n'est pas collecté avant le dépôt du cookie, et le fait que le consentement ne fait pas l'objet d'un acte positif. De même, **l'autorité hellénique** de protection des données a adressé des courriers de rappel à la loi à plusieurs acteurs (notamment à des éditeurs) avant de publier, sur son site, une recommandation relative à l'usage des cookies et technologies similaires[8].

Par ailleurs, **l'autorité fédérale allemande** de protection des données et l'autorité britannique ont publié des lignes directrices sur les cookies respectivement en mars et en juillet 2019. Enfin, plusieurs autorités ont été approchées par des fédérations et associations afin d'envisager l'élaboration de codes de conduite liés à la publicité en ligne.

Dans ce contexte, la CNIL échange régulièrement avec ses homologues européens afin de favoriser une harmonisation des positions européennes sur le sujet. Cette démarche s'étend également aux guides et recommandations émises dans ce domaine par chaque autorité de protection.

À la différence du RGPD qui est d'application directe dans les États membres et qui bénéficie d'un cadre de coopération renforcé, la directive ePrivacy a été transposée de manière variable dans chaque pays et son application a pu être confiée à des autorités de nature différentes (par exemple, l'équivalent des ARCEP, de la DGCCRF ou encore des CNIL locales). Ces disparités complexifient l'harmonisation, qui ne pourra réellement être renforcée qu'une fois la directive ePrivacy remplacée par un règlement d'application directe.

> « Les règles sont les mêmes pour tous, et s'appliquent de la même manière. »

7 « Marketing direct : l'Autorité de protection des données clarifie les règles du jeu », 10 février 2020, autoriteprotectiondonnees.be

8 « Recommandations pour la conformité des contrôleurs de données avec la législation spécifique sur les communications électroniques » (en grec), 25 février 2020, dpa.gr

Reconnaissance faciale : pour un débat à la hauteur des enjeux

La reconnaissance faciale est de plus en plus présente dans le débat public aux niveaux national, européen et mondial. Cette technologie soulève en effet des questions inédites touchant à des choix de société. C'est pourquoi la CNIL a appelé, en 2018[9], à un débat démocratique sur ce sujet, ainsi que plus largement sur les nouveaux usages de la vidéo. En novembre 2019[10], elle a contribué au débat en présentant les éléments techniques, juridiques et éthiques qui doivent, selon elle, être pris en compte dans l'approche de cette question complexe.

Face à la puissance de la reconnaissance faciale, des choix politiques sont nécessaires sur le rôle dévolu à la technologie, sur ses effets sur les libertés fondamentales des individus, sur la place de l'humain à l'ère numérique. Ces choix dessineront certains contours du monde de demain. Le débat ne doit donc pas se résumer à un examen technique des usages possibles et de l'efficacité de cette technologie, ou sur comment la « rendre acceptable » par les citoyens.

Le sujet est complexe et mérite un débat lucide et approfondi. Il est donc nécessaire de déterminer dans quels cas la reconnaissance faciale est nécessaire dans notre société démocratique, et ceux dans lesquels elle ne l'est pas.

Le débat sur cette technologie doit donc être proactif et prospectif, afin de garder la main sur le modèle de société que nous souhaitons. L'objectif est d'éviter de découvrir après coup, que, par l'accumulation progressive de nouveaux cas d'utilisation de cette technologie, par sa diffusion à bas bruit dans la vie quotidienne des citoyens, la société aurait changé sans que ce changement ait fait au préalable l'objet d'un débat d'ensemble et d'un choix politique délibéré.

DÉFINITION

La reconnaissance faciale est une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier.
La reconnaissance faciale appartient à la catégorie plus large des techniques biométriques.

> « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo. »

C'est pourquoi la CNIL, forte de son expertise en matière de reconnaissance faciale et garante du pacte républicain sur le numérique posé par la loi Informatique et Libertés et le RGPD, a apporté une première contribution, de méthode, à ce débat. **Cette contribution, publiée le 15 novembre 2019, poursuit quatre objectifs :**

1 - Présenter, techniquement, la reconnaissance faciale
Afin que l'objet du débat soit clair pour tous. Cette technique biométrique de reconnaissance automatisée d'une personne, à partir des caractéristiques de son visage, ne doit en effet pas être confondue avec d'autres techniques de traitement des images (par exemple, avec des dispositifs de « vidéo intelligente » qui permettent de détecter des évènements ou des émotions sans reconnaître, pour autant, les individus), avec lesquelles elle peut, parfois, se combiner. Surtout, derrière « la » reconnaissance faciale, il existe une grande diversité d'usages possibles, allant du déverrouillage d'ordiphone à la reconnaissance d'une personne recherchée par les forces de police dans une foule, en passant par l'ouverture de comptes bancaires. Ces utilisations ne soulèvent pas toutes les mêmes enjeux, notamment en termes de contrôle des personnes sur leurs données.

Cet état des lieux nuancé s'impose afin d'éviter tout amalgame et tout jugement d'ensemble sur cette technologie. Il faut raisonner au contraire cas d'usage par cas d'usage.

2 - Mettre en lumière les risques
Ces risques, qui peuvent être technologiques, éthiques ou sociétaux, sont liés à la nature biométrique de la reconnaissance faciale : les données extraites des visages touchent au corps, à l'intimité des personnes. Toute violation de données, tout mésusage ferait peser des risques importants (blocage d'accès à un service, usurpation d'identité, etc.). La reconnaissance faciale repose en outre sur une probabilité, et non une certitude absolue, de correspondance entre les visages comparés et le « gabarit » de référence. Les variations de performance peuvent donc avoir des conséquences très importantes pour les personnes mal reconnues.

Un autre enjeu est que cette technologie permet le traitement de données à distance, sans contact, voire à l'insu des personnes. Dans l'environnement numérique actuel, où les visages des personnes sont disponibles dans de multiples bases de données et captées par de nombreuses caméras, la reconnaissance faciale peut devenir un outil particulièrement omniprésent et intrusif. Le renforcement de la surveillance permis par cette technologie peut enfin réduire l'anonymat dont disposent les citoyens dans l'espace public.

Cette évaluation des risques est nécessaire pour déterminer ceux qui ne sont pas acceptables dans une société démocratique et ceux qui peuvent être assumés moyennant des garanties appropriées.

9 « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19 septembre 2018, cnil.fr

10 « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 15 novembre 2019, cnil.fr

3 - Rappeler le cadre s'imposant à ces dispositifs

Les législateurs européen (RGPD, directive « Police-Justice ») et national (modifications de la loi Informatique et Libertés en 2018) ont très récemment encadré, plus strictement qu'auparavant, les dispositifs biométriques dans le but d'adapter le niveau de protection des données aux nouveaux usages du numérique. Tout usage, y compris expérimental, de la reconnaissance faciale devra donc respecter ce cadre juridique modernisé.

Conformément à ces règles, la nécessité de tels dispositifs devra, au cas par cas, être établie : la reconnaissance faciale ne peut être utilisée sans impératif particulier de forte fiabilité de vérification de l'identité des personnes. Ces textes exigent également de s'assurer de la proportionnalité des moyens déployés et de veiller à la protection particulière dont doivent bénéficier les enfants. Ils imposent de placer le respect des personnes au cœur des dispositifs, par exemple en recueillant leur consentement ou en leur garantissant le contrôle de leurs données. C'est en appliquant ces principes, récemment réaffirmés au niveau européen, que la CNIL a déjà eu l'occasion d'admettre dans leur principe certains usages tout en encadrant leurs modalités pratiques (contrôles aux frontières dans les aéroports), et d'en refuser d'autres (contrôle d'accès d'élèves dans des établissements scolaires).

Ces exigences supérieures s'imposeront à tout encadrement, même expérimental, des systèmes de reconnaissance faciale.

INFOSPLUS

À quoi sert la reconnaissance faciale ?

La reconnaissance faciale peut remplir deux fonctions distinctes :

l'authentification d'une personne,
qui vise à **vérifier qu'une personne est bien celle qu'elle prétend être**. Dans ce cas, le système va comparer un gabarit biométrique préenregistré (par exemple, stocké dans une carte à puce) avec un seul visage, par exemple celui d'une personne qui se présente à un point de contrôle, afin de vérifier si cette personne est la même. Cette fonctionnalité repose donc sur la comparaison de deux gabarits.

l'identification d'une personne,
qui vise à retrouver **une personne au sein d'un groupe d'individus**, dans un lieu, une image ou une base de données. Dans ce cas, le système doit effectuer un test sur chaque visage capté pour générer un gabarit biométrique et vérifier si celui-ci correspond à une personne connue du système. Cette fonctionnalité repose ainsi sur la comparaison d'un gabarit avec une base de données de gabarits. Par exemple, elle permet de lier un « état civil » (nom, prénom) à un visage, si la comparaison est faite avec une base de photographies associées à un nom et un prénom. Elle peut aussi consister à **suivre la trajectoire d'une personne dans une foule,** sans nécessairement faire le lien avec l'état civil de la personne.

« Il faut raisonner cas d'usage par cas d'usage. »

4- Préciser le rôle de la CNIL

La CNIL n'est ni décideur ni prescripteur en cette matière : le choix d'un tel encadrement, de sa nature et de sa portée, appartient au Gouvernement et au Parlement.

La CNIL est en revanche dotée par le droit, européen et national, de missions de conseil, notamment aux pouvoirs publics, et de contrôle. Elle entend jouer pleinement son rôle à l'égard de cette technologie, en particulier en fournissant un conseil indépendant dans le cadrage juridique et méthodologique d'une démarche expérimentale. Elle pourra également conseiller les porteurs de projets sur les expérimentations envisagées et contribuer, dans sa sphère de compétence, à l'évaluation de ces dispositifs. La CNIL exercera, au besoin, ses pouvoirs d'enquête sur ces dispositifs en prenant toute mesure correctrice nécessaire pour protéger les personnes. Dans l'exercice de l'ensemble de ses missions, la CNIL conservera sa totale indépendance.

FOCUS

Quelles sont les exigences de la CNIL ?

Trois exigences essentielles doivent guider les réflexions sur toute expérimentation en matière de reconnaissance faciale :

Première exigence : tracer des lignes rouges, avant même toute expérimentation
La reconnaissance faciale, qu'elle soit expérimentale ou non, doit respecter le cadre européen, RGPD et directive « Police-Justice ». Dans ce cadre, tout n'est pas et ne sera pas permis en matière de reconnaissance faciale. Le but des expérimentations est, sans doute, de dessiner les frontières qui circonscrivent le champ du souhaitable (politiquement, socialement, etc.), comme celui du possible (technologiquement, financièrement, etc.). **Pour autant, des frontières préexistent à l'exercice.**

Deuxième exigence : placer le respect des personnes au cœur de la démarche
Ainsi, leur **consentement** devra être recueilli pour chaque dispositif le permettant, tout particulièrement dans le cadre d'expérimentations. **Le contrôle des données**, par des supports possédés par les individus et leur en assurant la maîtrise, doit être privilégié. **La transparence** à l'égard des personnes devra être assurée en toute circonstance, par la fourniture d'informations claires, compréhensibles et aisément accessibles. Leurs **droits de retrait du dispositif**, d'accès aux informations qui les concernent et de recours à une intervention humaine en cas de contrôle automatique devront être garantis. **La sécurité de leurs données** biométriques, relatives à l'intimité des personnes et dont toute compromission peut avoir des conséquences graves sur leur vie quotidienne, doit constituer une condition impérieuse de leur traitement.

Troisième exigence: adopter une démarche sincèrement expérimentale
Mettre en place un cadre expérimental implique notamment une **limitation dans le temps et dans l'espace** de dispositifs de reconnaissance faciale, une **identification exacte des objectifs poursuivis** par ces expérimentations et de leurs critères de réussite. La définition précise de leurs modalités d'évaluation, qui doit être rigoureuse, contradictoire, pluridisciplinaire et menée dans des délais raisonnables, ainsi que la détermination des autorités chargées de celle-ci, constituent des dimensions essentielles. La comparaison avec d'autres dispositifs techniques pouvant répondre aux mêmes besoins permettra en outre une meilleure évaluation des systèmes de reconnaissance faciale.

Le cadre juridique doit ainsi garantir la sincérité des expérimentations conduites, dont l'issue ne saurait être préjugée. Il doit pour cela consacrer une méthode expérimentale rigoureuse, inspirée du cadre juridique plus général en la matière et du « guide méthodologique » récemment élaboré par le Conseil d'État[11], afin de tirer tout le parti possible d'une telle démarche tout en faisant montre de la prudence nécessaire face aux risques posés par la reconnaissance faciale.

11 « Améliorer et développer les expérimentations pour des politiques publiques plus efficaces et innovantes », 3 octobre 2019, conseil-etat.fr

Diplomatie de la donnée

Le CNIL s'investit pleinement dans la coopération européenne. Il s'agit d'une nécessité à la fois juridique et politique : le succès du nouveau modèle européen de gouvernance de la donnée est la clé d'une véritable souveraineté européenne. Au-delà de ce cercle européen, la CNIL prend également une part active à la géopolitique internationale de la donnée.

LA VISION EUROPÉENNE SUR LA PROTECTION DES DONNÉES

Le Comité européen de la protection des données (CEPD), nouvel organe de l'Union européenne mis en place par le RGPD et qui rassemble les autorités de l'UE, poursuit ses activités en matière de coopération et de cohérence européennes. La CNIL continue de contribuer activement à la réussite du collectif européen en portant sa vision propre, grâce à une longue expérience de son métier de régulateur.

Le RGPD a mis en place un système inédit de coopération au niveau européen, fondé sur des piliers décentralisés (les autorités nationales de protection des données) qui convergent au sein du CEPD afin d'assurer une instruction et un traitement cohérents des cas transfrontaliers. Ce nouveau mécanisme implique un dialogue permanent entre autorités et des échanges formalisés entre « autorité chef de file » et « autorité(s) concernée(s) » pour aboutir à des décisions collectives applicables pour toute l'UE.

Le CEPD élabore également une véritable doctrine européenne en matière de protection des données personnelles. Dès 2016, un travail important d'interprétation et d'explicitation des dispositions du RGPD a été mené par les autorités de protection européennes, avec l'adoption d'une série de lignes directrices. Certains sujets, comme le champ d'application territorial du RGPD, qui peut concerner des entreprises en dehors de l'UE, font l'objet d'une attention particulière et de réactions de nombreux acteurs internationaux.

LA PRÉSENCE EUROPÉENNE DE LA CNIL

La CNIL est présente aux réunions des groupes d'experts chaque semaine à Bruxelles, ainsi qu'à la réunion plénière du CEPD qui se tient désormais tous les mois. En France, elle s'implique quotidiennement dans le suivi des travaux au niveau européen et l'instruction des cas transfrontaliers. La CNIL et ses homologues de l'UE constatent la même évolution : le RGPD a transformé une activité nationale de protection des données en une activité européenne. L'effectivité de cette coopération européenne constitue une priorité pour la CNIL, qui se traduit notamment par son rôle de rapporteur sur de nombreux dossiers ou encore de coordinateur pour plusieurs groupes d'experts thématiques du CEPD.

L'échelon européen est le premier et principal champ d'action pour la CNIL en matière de diplomatie de la donnée. Le dialogue et la coopération entre autorités européennes, dont l'action repose sur des cadres nationaux et des traditions juridiques qui peuvent varier, sont le fondement d'un modèle de régulation inédit au niveau européen.

FOCUS

Les réseaux d'autorités comme vecteurs d'influence

Le CEPD, établi par le RGPD en tant qu'organe de l'Union européenne, constitue le réseau d'autorités le plus intégré, doté de la personnalité juridique et de pouvoirs propres. D'autres réseaux, tels que l'Association francophone des autorités de protection des données personnelles (AFAPDP), existent par ailleurs et représentent un réel vecteur d'influence pour la promotion de la protection des données au niveau international. Les CNIL des États qui font partie de la Convention du Conseil de l'Europe sur la protection des données se rassemblent également tous les ans au sein de la « Conférence de printemps », accueillie chaque année par une autorité membre.

La CNIL entretient par ailleurs des relations étroites avec d'autres réseaux linguistiques et régionaux à travers le monde, comme le réseau ibéro-américain, celui des autorités de la région Asie-Pacifique ou encore le réseau africain. Toutes les autorités sont rassemblées depuis près de 40 ans au sein de la Conférence internationale des commissaires à la protection des données qui est devenue, en 2019, l'Assemblée mondiale de la vie privée (AMVP).

DE NOUVEAUX ENJEUX INTERNATIONAUX

Un levier de développement

Lors de la réunion du G20 d'Osaka de juin 2019, les chefs d'États et de gouvernements ont adopté une déclaration qui reconnaît notamment que « la circulation transfrontalière des données, des informations, des idées et des connaissances génère une productivité accrue, une plus grande innovation et un meilleur développement durable, tout en soulevant des défis liés à la vie privée, à la protection des données, aux droits de propriété intellectuelle et à la sécurité ». Les leaders du G20 considèrent qu'il « est nécessaire que les cadres juridiques, tant nationaux qu'internationaux, soient respectés ».

La CNIL, comme les autres autorités européennes, estime que l'UE doit se montrer ambitieuse et qu'elle doit défendre et promouvoir son modèle de régulation ainsi que ses standards en parallèle des discussions internationales en matière commerciale. Certains pays tiers sont reconnus par l'UE comme étant adéquats et offrant un niveau de protection substantiellement équivalent à celui de l'Union. La CNIL participe ainsi chaque année aux travaux du CEPD destinés à évaluer la mise en œuvre et la conformité du *Privacy Shield*, instrument sur lequel s'appuie la Commission européenne pour reconnaître ce pays comme adéquat. La récente décision d'adéquation pour le Japon prévoit aussi un mécanisme de revue périodique qui implique les autorités de protection des données de l'Union.

Alors que les développements mondiaux en matière d'économie numérique ou de commerce international appellent à une libre circulation des données, d'autres pays imposent, à l'inverse, des obligations en matière de localisation des données. La Chine et la Russie, en particulier, imposent aux opérateurs sur leur marché intérieur d'héberger leurs données sur leur territoire national, contrainte qui soulève également de nouvelles problématiques relatives à la vie privée et à l'accès aux données par les autorités de ces pays. De même, les acteurs majeurs de l'économie numérique mondiale étant américains, une grande partie des données personnelles sont, en pratique, hébergées aux États-Unis ou soumises, à certains égards, aux lois de ce pays.

À SUIVRE

Les standards mondiaux seront-ils compatibles ?

Différentes traditions juridiques se côtoient, certains modèles se confrontent alors que les grands acteurs de l'économie numérique appellent à garantir une libre circulation des données au niveau mondial.

Ces enjeux sont au cœur des discussions internationales et font partie des échanges en cours au sein du réseau international des autorités de protection des données. La CNIL s'implique en particulier dans les travaux qu'elle pilote, au sein de cette enceinte, ayant pour objectif d'identifier les principes communs existants et standards à développer au niveau international.

« Le RGPD a transformé une activité nationale de protection des données en une activité européenne. »

La coopération avec les autorités judiciaires à l'international

La question de l'accès transfrontalier aux données dans le cadre d'enquêtes de police ou procédures judiciaires se fait ainsi de plus en plus pressante aux niveaux européen et international, compte tenu notamment des nouveaux usages numériques et des défis posés aux autorités lorsque suspects, victimes et éléments de preuve se trouvent dans des juridictions différentes. Il est évidemment essentiel d'apporter une réponse concrète à cette problématique pour permettre l'efficacité des enquêtes, mais cela ne doit pas se faire aux dépens du droit des personnes.

Les problématiques soulevées par des lois comme le *Cloud Act* américain ne sont pas anecdotiques. Les usages numériques ont pour conséquence l'émergence de problématiques nouvelles en matière de coopération policière ou judiciaire, qui placent la donnée au cœur des enjeux de sécurité, d'efficacité mais aussi de souveraineté. Les débats en cours ne sont donc pas uniquement juridiques, mais bel bien aussi diplomatiques et géopolitiques.

Il est dès lors essentiel, au niveau mondial, d'affirmer les garanties relatives aux conditions matérielles et procédurales pour l'accès aux données protégées par le droit de l'UE. Pour les autorités européennes, cette question doit également être considérée dans le cadre d'autres négociations internationales en cours sur l'accès transfrontalier aux données personnelles – ou preuves électroniques – avec en particulier les discussions sur la proposition de règlement européen à ce sujet, mais aussi le projet de protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité ou encore le projet d'accord entre l'UE et les États-Unis sur l'accès aux données et preuves électroniques.

FOCUS

Impact du *Cloud Act* américain sur le cadre européen en matière de protection des données

En juillet 2019, les autorités de l'UE ont pris position sur l'impact du *Cloud Act* américain (loi fédérale adoptée en 2018) sur le cadre juridique européen en matière de protection des données. Cette loi permet aux autorités américaines, dans le cadre d'une procédure judiciaire, d'adresser directement des demandes d'accès aux entreprises du numérique soumises au droit américain, y compris lorsque ces données sont stockées en-dehors des États-Unis.

En réaffirmant l'application du RGPD, la CNIL et les autorités européennes ont considéré que de telles demandes des autorités américaines, lorsqu'elles sont émises en dehors de tout accord international ou traité d'entraide judiciaire, ne sauraient être considérées comme licites.

UNE ACCÉLÉRATION MONDIALE SUR LES ENJEUX DE LA PROTECTION DES DONNÉES

Depuis son entrée en application en 2018, le phénomène RGPD se poursuit, et la législation européenne devient même un sujet de discussions dans de nombreux pays en dehors de l'UE.
En effet, sans pour autant être perçu comme un standard directement applicable au niveau mondial, le RGPD a été perçu comme un signal fort de l'UE concernant la défense et le respect de son cadre juridique en matière de protection des données. Cette conception exigeante a notamment inspiré des développements législatifs dans plusieurs régions du monde.

Des évolutions nationales

Certains pays ont procédé à une mise à jour de leur cadre national en matière de protection des données afin de se rapprocher des standards et dispositions du RGPD. C'est le cas notamment du Japon, de la Corée du Sud, du Bénin ou encore de l'Australie. Un processus législatif en ce sens est également en cours en Suisse, en Tunisie et au Burkina Faso par exemple.

D'autres États ont, pour la première fois, adopté un cadre juridique général encadrant les traitements de données personnelles, et dont les principales dispositions peuvent se rapprocher de celles du RGPD. C'est le cas en particulier de l'État de Californie avec le *California Consumer Privacy Act* (CCPA) adopté en octobre 2018 et entré en application au 1er janvier 2020, mais aussi du Brésil avec la *Lei Geral* de *Proteçao de Dados (LGPD)* adoptée en 2019. Aux États-Unis, les débats et initiatives pour l'adoption d'une loi fédérale en matière de vie privée se font aussi de plus en plus nombreux. En Inde, où la Cour suprême a consacré en 2017 le droit à la vie privée comme droit fondamental, un projet de loi est actuellement en discussion au Parlement.

Une dynamique internationale

Au-delà des développements nationaux, la dynamique est prolongée par les initiatives d'organisations régionales ou internationales. L'OCDE est actuellement engagée dans un processus de revue de ses lignes directrices sur la vie privée et la Convention 108 du Conseil de l'Europe relative à la protection des données personnelles a fait l'objet de travaux de modernisation qui se sont achevés en mai 2018 par l'adoption d'un Protocole instaurant une Convention modernisée, désignée comme la « Convention 108+ ». Ouverte à signature en octobre 2018, la Convention 108+ compte désormais

35 États signataires, dont la France, et 3 ratifications ; elle nécessite cependant d'être ratifiée par 38 parties afin d'entrer en vigueur. La CNIL participe, aux côtés des autorités françaises, aux réunions du comité du Conseil de l'Europe sur la protection des données (T-PD), chargé d'accompagner l'interprétation et la mise en œuvre de ce traité.

Elle constitue un outil unique en son genre pour la convergence mondiale des standards de protection des données car il s'agit du seul instrument contraignant (c'est-à-dire qui a un caractère obligatoire) à vocation universelle fournissant un ensemble complet de principes partagés.

Enfin, le développement de normes techniques au niveau international reflète également une prise en compte accrue de nouvelles exigences en matière de protection des données, de respect de la vie privée ou encore de sécurisation des données. C'est le cas de la norme ISO 27701, publiée en août 2019, qui vient compléter deux normes bien connues de la sécurité des systèmes d'information. La CNIL a activement œuvré à son élaboration, avec le soutien de l'Association française de normalisation (AFNOR) et du CEPD.

Si le RGPD a véritablement eu rayonnement mondial, et s'il est parfois une source d'inspiration, d'autres approches sont toutefois à l'œuvre et une certaine concurrence des modèles est perceptible à l'échelle mondiale. La géopolitique de l'écosystème numérique mondial est également en constante évolution, avec notamment l'émergence de nouveaux acteurs majeurs, en particulier en Asie. La CNIL s'engage donc au niveau international dans une véritable diplomatie de la donnée, en participant à de nombreux forums internationaux, afin de promouvoir l'acquis européen et diffuser sa conception du droit dans ce domaine.

FOCUS

Travaux de l'OCDE sur la vie privée et l'économie numérique

En novembre 2019 s'est tenue la première réunion du groupe de travail de l'OCDE sur la gouvernance des données et la vie privée dans l'économie numérique, nouvellement établi au sein du Comité de la politique de l'économie numérique (CPEN) de l'organisation. La CNIL représente la France au sein de ce nouveau groupe de travail qui a pour mandat l'examen de nombreux sujets connexes entre protection des données personnelles et économie numérique ainsi que l'évaluation des lignes directrices existante de l'OCDE sur la vie privée. L'organisation joue un rôle important pour la définition commune entre les gouvernements de l'OCDE de grands principes en matière de vie privée, en particulier dans le contexte des flux de données internationaux.

La CNIL co-préside également depuis 2019 le groupe d'expert de l'OCDE sur la vie privée et la protection des données, chargé de conseiller l'organisation et de présenter des contributions dans le cadre de l'examen de la mise en œuvre de ses lignes directrices sur la protection de la vie privée.

Traitements à finalité de recherche scientifique : retour sur la consultation publique

Dans la continuité des travaux entamés en matière de recherche scientifique (hors santé), la CNIL a publié une consultation publique à destination des acteurs de la recherche sur son site web du 15 juillet au 30 septembre 2019. Cette consultation, qui a réuni 268 contributions, a pour objectif de permettre une meilleure compréhension des traitements de données personnelles à finalité de recherche scientifique et clarifier le cadre juridique applicable.

Une volonté d'accompagnement des acteurs de la recherche

Avec cette consultation publique, la CNIL a souhaité avoir une meilleure connaissance des pratiques des chercheurs en vue de leur proposer un accompagnement qui corresponde autant aux besoins qu'aux contraintes exprimés. Les traitements qui poursuivent une finalité de recherche scientifique et historique sont soumis aux au RGPD ainsi qu'à la loi Informatique et Libertés. Ces textes prévoient des dérogations et des aménagements afin de concilier les spécificités de la recherche avec l'impératif de protection des données personnelles.

Les questions posées lors de la consultation avaient trait :

- aux caractéristiques des traitements mis en œuvre par les chercheurs (nature de l'organisme dans lequel la recherche est effectuée, provenance des données traitées et outils de collecte utilisés) ;
- aux possibilités de demander le consentement des personnes concernées et aux éventuelles difficultés rencontrées pour le recueillir ;
- aux moyens utilisés et obstacles identifiés pour déterminer la durée de conservation des données traitées ;
- aux conditions dans lesquelles des données sensibles sont traitées dans le cadre de recherches ;
- aux manières d'informer les personnes concernées et aux cas dans lesquels cette information s'avère impossible, demande des efforts disproportionnés ou compromet la réalisation des objectifs de la recherche ;
- aux modalités d'exercice des droits par les personnes concernées ;
- aux garanties de sécurité mises en place ou susceptibles de l'être, comme par exemple la pseudonymisation.

FOCUS

Le traitement des données sensibles dans le cadre de la recherche publique (hors santé)

La loi Informatique et Libertés, modifiée à la suite de l'entrée en application du RGPD, a supprimé de nombreuses formalités préalables, y compris certaines applicables alors aux traitements de recherche. Pour exploiter des données sensibles, dont l'utilisation est en principe prohibée, les traitements à finalité de recherche peuvent notamment mobiliser les exceptions suivantes :

le consentement de la personne concernée ;

le fait que les données ont été manifestement rendues publiques par la personne concernée ;

la consultation préalable de la CNIL pour les traitements nécessaires à la recherche publique, sous réserve que des motifs d'intérêt public important les rendent nécessaires. En 2019, la CNIL a été saisie de trois demandes d'avis en ce sens.

En dehors de cette procédure et de toute disposition spécifique, les traitements de données sensibles justifiés par l'intérêt public doivent désormais être autorisés par un décret en Conseil d'État après avis motivé et publié de la CNIL.
À toutes fins utiles, pour de tels traitements, le responsable du traitement veillera à réaliser, si nécessaire, une analyse d'impact relative à la protection des données et le cas échéant, à la transmettre à la CNIL.

Des retours variés

Plusieurs centaines de contributions ont été reçues par la CNIL. La plupart des contributions émanaient du secteur public (universités, établissements publics, organismes parapublics, etc.), de chercheurs ou de délégués à la protection des données. Une quinzaine de contributions ont été reçues du secteur privé : structures privées à but non lucratif, entreprises privées, associations chargées d'une mission de service public, organismes réalisant des études de marché, travaux avec des partenariats privés. Par ailleurs, les contributions étaient relatives à des domaines de recherche très divers (par exemple sociologie, psychologie, histoire, sociojuridique, droit, sciences politiques, philosophie, économie et gestion, sciences du langage, philologie, sciences de l'information et de la communication, agronomie, sciences cognitives, neurosciences cognitives, recherche clinique, statistiques, radioastronomie, développement de technologies, bio-informatique, génie civil), même si une majorité des contributions relevait des sciences humaines et sociales.

Les contributions ont fait apparaître un certain nombre de questions vis-à-vis de la réglementation applicable en matière de protection des données. Au-delà des observations relatives à la technicité des termes employés et à la difficulté d'accès au contenu pour des non spécialistes de la protection des données personnelles, les principales difficultés rencontrées dans l'application des textes sont :

- l'obligation d'information au moment où les données sont obtenues, en cas de collecte directe ;
- la difficulté de fixer une durée de conservation pour les données collectées au regard de la possibilité de conserver les données « pour des durées plus longues » ;
- l'obligation pour la recherche publique de recueillir l'avis préalable de la CNIL pour traiter de données sensibles.

Les suites de la consultation

Les contributions à la consultation publique permettront de nourrir la réflexion en vue d'élaborer des contenus dédiés sur le site web de la CNIL en 2020. Une attention particulière sera portée à la lisibilité de ces contenus et des efforts seront menés pour les rendre accessibles au plus grand nombre. La CNIL s'emploiera à apporter les éclairages nécessaires aux acteurs de la recherche pour les accompagner au mieux dans le respect de leurs obligations, car il ressort des réponses un souhait important de formation sur cette matière.

À SUIVRE

Les travaux à l'échelle européenne

Bien que le RGPD ait prévu des dérogations propres aux traitements mis en œuvre pour une finalité de recherche scientifique ou historique, cette matière continue de susciter des interrogations, y compris au niveau européen.

Dans son avis préliminaire du 6 janvier 2020 sur la protection des données et la recherche scientifique, le Contrôleur européen à la protection des données appelle à mener des analyses approfondies et à un débat entre la communauté de la recherche et les spécialistes de la protection des données personnelles notamment sur la distinction entre les notions de consentement au sens du RGPD et au sens de l'éthique scientifique. Il soulève également la question de l'incompatibilité des protocoles de recherche déceptifs ou visant à dissimuler l'objet réel de la recherche avec l'article 13 du RGPD prévoyant un droit à l'information des personnes concernées auquel il ne peut être dérogé.

Par ailleurs, le Contrôleur recommande, entre autres, l'adoption au niveau européen de codes de conduite sur des thèmes tels que le régime applicable aux catégories particulières de données ou encore l'exercice des droits des personnes concernées dans les cas où ceux-ci peuvent faire l'objet de limitations.

Le Contrôleur se propose en outre de faciliter le débat entre les organismes de défense des libertés publiques, la communauté de la recherche et les grandes sociétés technologiques en vue de l'élaboration d'un cadre visant à permettre aux chercheurs d'accéder aux données conservées par les principales entreprises privées pour des recherches d'intérêt public.

Les bonnes pratiques en matière de projets de recherche ont, pour leur part, été inscrites parmi les sujets possibles dans le programme de travail 2019-2020 du Comité européen de la protection des données.

« La CNIL s'emploiera à apporter les éclairages nécessaires aux acteurs de la recherche pour les accompagner au mieux dans le respect de leurs obligations [...]. »

Santé : un accompagnement intensifié

Compte tenu de la sensibilité et des enjeux considérables des données de santé, la CNIL a particulièrement renforcé son dispositif d'accompagnement des organismes concernés. Une consultation, publiée auprès de professionnels de la recherche scientifique, ainsi que les décisions délivrées par la CNIL, lui ont ainsi permis de renforcer sa doctrine.

LES TRAITEMENTS À FINALITÉ DE RECHERCHE, D'ÉTUDE OU D'ÉVALUATION DANS LE DOMAINE DE LA SANTÉ

Les décisions délivrées par la CNIL durant l'année 2019 lui ont permis de consolider sa doctrine en matière de traitements de données de santé afin d'accompagner au mieux les acteurs de la recherche. Le fruit de ces réflexions sera d'ailleurs, à partir de 2020, mis à la disposition du plus grand nombre grâce à la publication de fiches thématiques sur le site web de la CNIL et la mise en ligne d'un MOOC consacré à la santé.

La distinction entre les entrepôts de données et les projets de recherche

La loi Informatique et Libertés implique de distinguer, parmi les traitements de données de santé, ceux qui ont pour finalité la constitution d'un entrepôt de données, d'une part, et ceux qui ont pour finalité la réalisation d'un projet de recherche dans le domaine de la santé, d'autre part. Ces deux types de traitements sont en effet soumis à des régimes juridiques partiellement différents, s'agissant notamment des formalités préalables à accomplir avant leur mise en œuvre (figurant respectivement aux sous-sections 1 - articles 65 et suivants - et 2 - articles 72 et suivants - de la section de la loi consacrée aux données de santé). Par ailleurs, les enjeux de protection des données et de la vie privée (minimisation des données, gestion des accès, mesures de sécurité, etc.) se posent en des termes différents. Or, la distinction entre ces deux types de traitements, entrepôts et projets de recherche, est parfois délicate. La CNIL a donc publié, le 28 novembre 2019, une fiche pratique sur son site web[12] à destination des acteurs de la recherche.

Lorsqu'un responsable de traitement envisage la création d'une base de données comportant des données de santé, il doit déterminer si elle permettra la réalisation ultérieure de plusieurs traitements (« entrepôt ») ou s'il s'agit d'une recherche, étude ou évaluation ponctuelle.

Les **entrepôts de données** sont principalement créés pour collecter et disposer de données massives (données relatives à la prise en charge médicale du patient, données issues de précédentes recherches, etc.). Ces bases de données sont notamment constituées pour une longue durée, de plus de dix ans en général. Elles peuvent être alimentées par de multiples sources (professionnels de santé, patients, pharmacies, établissements de santé, etc.).

Une **recherche**, étude ou évaluation dans le domaine de la santé est, quant à elle, un traitement de données qui poursuit une finalité de recherche précise et répond à une question spécifique et ponctuelle. La durée de la recherche est limitée et connue. Les données sont le plus souvent collectées ou extraites spécifiquement pour les besoins de la recherche.

Dans le cas d'un entrepôt constitué à des fins de recherche, chaque traitement fait l'objet d'un régime juridique distinct, qu'il s'agisse par exemple de la création de l'entrepôt de données, qui est un traitement de données en tant que tel, ou

FOCUS

Les demandes d'autorisation de traitements de santé (recherche, étude, évaluation)

La CNIL a poursuivi son processus de simplification des démarches grâce à la délivrance d'une dizaine de décisions uniques en 2019, autorisant ainsi par ce biais, selon les estimations fournies par les responsables de traitement concernés, près de 4 000 traitements. Elle a également pu dresser un état des lieux des recours au mécanisme de la décision unique, qui se justifie en pratique dans trois hypothèses :

un volume important de traitements réalisés (de quelques dizaines à plusieurs centaines par an) ;

un besoin de mise en œuvre rapide de traitements ne pouvant être anticipés (liés à l'actualité législative, réglementaire ou sectorielle, par exemple) ;

la mise en œuvre récurrente d'un seul traitement de données.

Malgré ces mesures de simplification, la CNIL a reçu 486 demandes d'autorisation en 2019.

12 « Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ? » sur www.cnil.fr

encore des projets de recherches, études ou évaluations réalisés à partir des données conservées dans l'entrepôt par le même responsable de traitement ou d'autres organismes.

Dans tous les cas, une analyse d'impact sur la protection des données (AIPD) doit être réalisée par le responsable de traitement. Cette analyse doit être transmise avec le dossier de demande d'autorisation adressé à la CNIL, le cas échéant.

Chaque projet de recherche mis en œuvre à partir des données de l'entrepôt devra être mené en conformité avec les dispositions relatives aux recherches et faire l'objet d'un engagement de conformité à une méthodologie de référence (procédure simplifiée) ou, à défaut de conformité avec l'un de ces référentiels, d'une demande d'autorisation recherche auprès de la CNIL.

LA TRANSPARENCE DANS LE CADRE DES RECHERCHES DANS LE DOMAINE DE LA SANTÉ

Véritable socle d'une relation de confiance entre la personne concernée par le traitement de données et le responsable de traitement, le principe de transparence a été renforcé avec l'entrée en application du RGPD. Ce principe de transparence passe en premier lieu par l'information des personnes concernées.

L'information des personnes concernées par un projet de recherche dans le domaine de la santé

Les personnes concernées doivent être individuellement informées lorsqu'un traitement de leurs données personnelles a pour finalité un projet de recherche, d'étude ou d'évaluation dans le domaine de la santé, au regard de la loi Informatique et Libertés et du RGPD.

Si les données ont déjà été collectées, le RGPD prévoit trois hypothèses dans lesquelles le responsable de traitement n'est pas tenu de faire une information individuelle :

- lorsqu'il est impossible d'informer les personnes ;
- lorsque le fait d'informer rend impossible ou peut compromettre la réalisation des objectifs du traitement ;
- lorsque l'information ne peut être réalisée qu'au moyen d'efforts disproportionnés.

FOCUS

Le cas de l'« effort disproportionné »

L'effort disproportionné constitue l'argument le plus fréquemment invoqué par les responsables de traitement.

Selon les lignes directrices du CEPD sur la transparence[13], dans cette hypothèse, le responsable de traitement « devrait mettre en balance les efforts qui lui sont demandés pour communiquer les informations à la personne concernée et l'incidence et les effets sur la personne concernée dans le cas où celle-ci ne recevrait pas ces informations ».

Les justifications apportées par le responsable de traitement qui invoque le critère des efforts disproportionnés pour bénéficier d'une exception à l'information individuelle des personnes (évaluation de la difficulté matérielle pour ré-identifier les personnes concernées, de la charge de travail humaine, du coût financier, de l'ancienneté des données, du nombre de personnes, etc.) font l'objet d'une évaluation au cas par cas, notamment en fonction des moyens dont dispose le responsable de traitement.

13 « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 », adoptées le 29 novembre 2017, Groupe de travail « Article 29 »

LA TRANSPARENCE DES ÉTUDES ET DE LEURS RÉSULTATS, UN ÉLÉMENT D'APPRÉCIATION DE L'INTÉRÊT PUBLIC

Les traitements de données personnelles dans le domaine de la santé ne peuvent par ailleurs être mis en œuvre qu'en considération « de la finalité d'intérêt public qu'ils présentent ». Lorsque le traitement envisagé n'est pas conforme à un référentiel, c'est à la CNIL, lors de l'instruction de la demande d'autorisation, d'évaluer l'intérêt public de la finalité du traitement envisagé.

Concernant les traitements réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, l'intérêt public de la finalité est également évalué par le comité éthique et scientifique pour les recherches, les études et les évaluations. Ce comité peut se saisir ou être saisi pour avis, par la CNIL ou le ministère chargé de la Santé, sur le caractère d'intérêt public que présentent ces traitements au regard de la loi.

Parmi les critères permettant d'évaluer l'intérêt public d'une recherche figure, notamment, la transparence et la publication des résultats. Ainsi, comme l'a souligné l'Institut national des données de santé (devenu la Plateforme des données de santé) dans sa publication relative aux Principes d'appréciation de l'intérêt public[14], les efforts supplémentaires mis en œuvre par le responsable de traitement afin d'assurer la diffusion la plus large possible des résultats et des moyens permettant d'évaluer la validité de la recherche constituent un critère d'appréciation de l'intérêt public de l'étude.

La CNIL se montre particulièrement attentive et exigeante quant à la publication des résultats des études, qui permet une transparence en aval de la mise en œuvre des traitements.

FOCUS

La transparence dès la conception

Au-delà de la diffusion des seuls résultats de l'étude et de la méthodologie utilisée, l'instauration d'une transparence dès la conception, avant le début de l'étude, doit être encouragée. Il pourrait s'agir, par exemple, de la mise en place, d'un portail de transparence sur lequel figurerait la liste des traitements mis en œuvre par un responsable de traitement, ainsi que les références vers les publications réalisées.

« La CNIL se montre particulièrement attentive et exigeante quant à la publication des résultats des études, qui permet une transparence en aval de la mise en œuvre des traitements. »

14 « Principes d'appréciation de l'intérêt public », 2019, Indsanté

Le RGPD, un instrument au service de la cybersécurité

La CNIL accompagne les administrations et les entreprises dans la prise en compte de la sécurité informatique depuis 1978. L'obligation de sécurité, inscrite dans la loi depuis plus de 40 ans, a été renforcée par le RGPD et complétée de nouveaux outils comme la notification des violations, l'analyse d'impact sur la protection des données ou les codes de conduite. La CNIL va continuer à jouer pleinement son rôle au service de la cybersécurité en déployant son action autour de quatre axes : la sensibilisation du grand public, l'accompagnement des PME et des collectivités locales, la poursuite de son action répressive et l'accompagnement de l'écosystème cyber.

LA SÉCURITÉ, UNE OBLIGATION PRÉSENTE DÈS 1978... ET UN CADRE RENFORCÉ AVEC LE RGPD

Le principe de sécurité fait partie des principes fondamentaux de la loi Informatique et Libertés. En effet, l'absence de sécurité d'un traitement de données personnelles ferait notamment courir le risque que les données soient récupérées par un tiers malveillant et utilisées contre les personnes concernées.

Le RGPD a rehaussé, à plusieurs égards, les exigences en matière de sécurisation des données personnelles et, ainsi, renforcé la vocation des autorités de protection des données à accompagner l'ensemble des entreprises et les administrations en matière de cybersécurité. Le nouveau règlement a repris l'exigence fondamentale de sécurité et y a créé trois nouvelles obligations :

- la tenue d'un registre recensant toutes les violations de données personnelles.
- La notification de ces violations à l'autorité de contrôle, dès lors qu'elles engendrent un risque pour les droits et libertés des personnes concernées. Cette nouvelle obligation est similaire à une obligation déjà existante avant le RGPD mais qui s'imposait aux seuls opérateurs de communications électroniques.
- L'information des personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

Le RGPD introduit aussi de nouveaux instruments à disposition des entreprises et administrations, notamment l'analyse d'impact relative à la protection des données (AIPD), rendue obligatoire avant la mise en œuvre de tout traitement de données présentant un risque élevé, et qui doit comporter un volet dédié à la sécurité.

Le non-respect de l'obligation de sécurité, en tant que telle, est susceptible d'amendes administratives pouvant s'élever jusqu'à 10 000 000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Le nouveau régime de sanctions conduit les autorités de protection à relever le niveau des amendes infligées aux responsables de traitement qui ne respectent pas les obligations de sécurité. En 2019, cinq amendes importantes ont été prises ou proposées au niveau européen pour des défauts de sécurité, l'absence de notification de violation de données ou de communication aux personnes concernées.

Enfin, la mise en conformité avec les règles de protection des données constitue souvent la première étape dans la mise en place d'une politique de cybersécurité. C'est pourquoi la CNIL publie régulièrement des guides pour accompagner les responsables de traitement et leurs sous-traitants, comme par exemple :

- une recommandation sur les mots de passe adoptée en 2017[15];
- un guide sur la sécurité des données personnelles[16];
- les guides sur les analyses d'impact sur la protection des données et le logiciel PIA[17];
- une check-list sécurité[18];
- début 2020, un guide aidant les développeurs à sécuriser leurs développements, publié sur la plateforme GitHub[19].

UN CONTRÔLE SYSTÉMATIQUE ET DES SANCTIONS RÉGULIÈRES

Les manquements à l'obligation de sécurité figurent également parmi les manquements les plus couramment constatés par la CNIL : 2/3 des sanctions depuis 2017 incluent un manquement à la sécurité, et plus de 40 % des sanctions sont prises sur ce seul fondement. À ce jour, les montants des sanctions sur le seul fondement d'un défaut de sécurité oscillent entre 15 000 et 400 000 euros et elles concernent notamment les manquements suivants :

- des données librement accessibles par modification d'URL (défaut d'authentification, URL prédictible), par exemple quand il suffit de modifier un nombre dans la barre d'adresse pour accéder à des documents d'autres personnes ;
- une politique de mot de passe non conforme, c'est-à-dire ne respectant pas la recommandation mot de passe de la CNIL[20];
- la transmission de mot de passe en clair, par exemple quand, à la création d'un compte sur un site, le mot de passe choisi est envoyé en clair dans un email et est donc interceptable ;

15 « Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers », 27 janvier 2017, cnil.fr
16 « Guide de la sécurité des données personnelles », 2018, cnil.fr
17 « Les guides AIPD (analyse d'impact relative à la protection des données) », 2018, cnil.fr
18 « Évaluer le niveau de sécurité des données personnelles de votre organisme », PDF, 2 octobre 2017, cnil.fr
19 « Guide RGPD du développeur », janvier 2020, github.com
20 « Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers », 2017, cnil.fr

- la transmission de données par une connexion non chiffrée (HTTP), par exemple dans le cas d'un formulaire sur un site web par lequel l'utilisateur envoie des données personnelles ;
- l'absence de verrouillage automatique des sessions des postes de travail, permettant ainsi à un tiers d'accéder à un système d'information contenant des données personnelles ;
- un défaut de protocole de test afin de garantir l'absence de vulnérabilité avant la mise en production d'un nouveau développement : c'est le cas quand un organisme développe un nouvel outil (application, site web, formulaire) traitant des données personnelles, sans prévoir de phase de test destinée à identifier les éventuelles vulnérabilités de l'outil.

> « La protection des données constitue souvent la première étape dans la mise en place d'une politique de cybersécurité. »

Par ailleurs, la sécurité est vérifiée de manière systématique dans les 300 procédures formelles de contrôle que la CNIL mène chaque année, d'abord par la vérification du respect des principes de base (mots de passe, sécurisation bases de données et réseau, etc.), mais aussi par la vérification de l'existence d'un registre des violations, nouvelle obligation issue du RGPD.

LA CNIL, UN ACTEUR DE LA CYBERSÉCURITÉ

En 2020, l'objectif principal de la CNIL en matière de cybersécurité sera d'améliorer le niveau minimal des entreprises traitant des données personnelles.

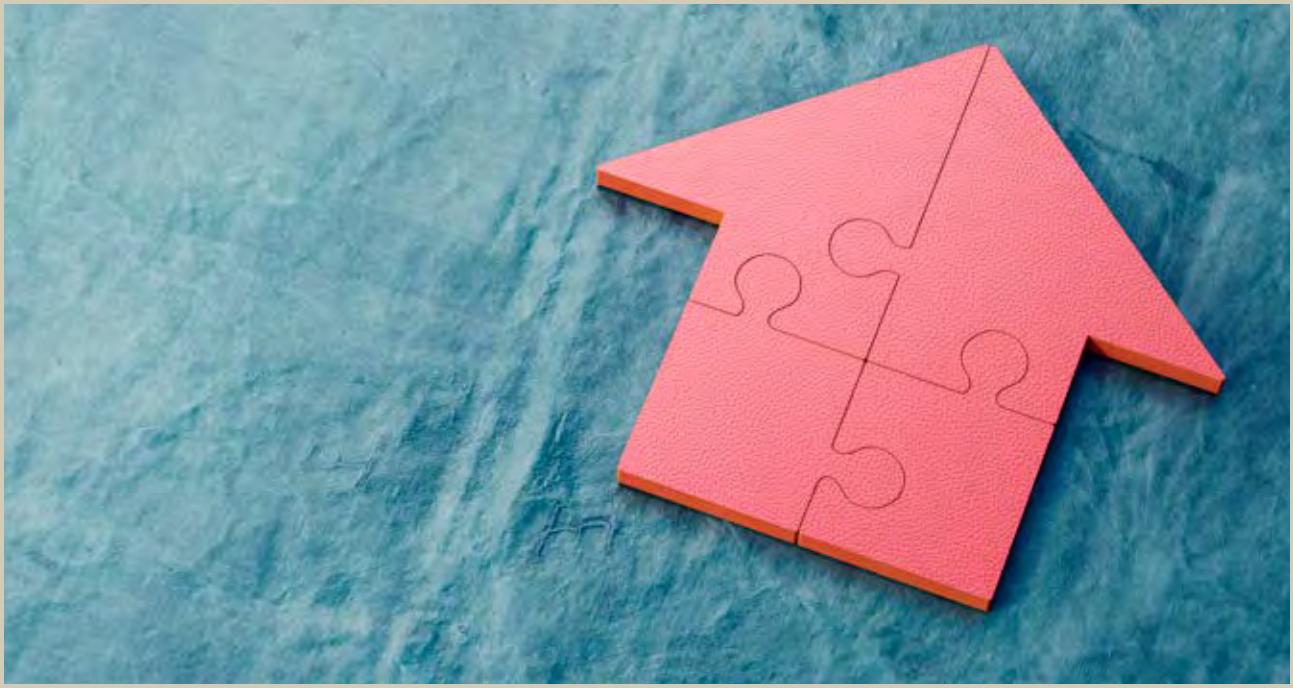
Son action, tournée vers les PME et la grande majorité des entreprises françaises, sera donc complémentaire de celle des autres acteurs publics de la cyber, notamment l'ANSSI et la section cybercriminalité du parquet de Paris qui prennent déjà en charge le traitement des incidents graves touchant des acteurs publics ou présentant une importance particulière (CHU de Rouen, TV5 Monde, etc.).

La CNIL participe également à de nombreux travaux internationaux autour de la cybersécurité, au sein du Comité européen de protection des données évidemment, en particulier pour accompagner les entreprises dans la mise en place de codes de conduite destinés à intégrer les questions de protection de données dans les référentiels des acteurs. La CNIL participe aussi aux enceintes de normalisation, notamment à l'ISO, où elle a contribué aux normes de la série 27000 et, récemment, à l'adoption de la norme 27701 sur la protection des données.

Afin de poursuivre son engagement sur la cybersécurité, quatre volets d'action seront renforcés et lancés dans les prochains mois par la CNIL.

DÉFINITION

La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires.
En pratique, un processus de pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) par des données indirectement identifiantes (alias, numéro dans un classement, etc.) afin d'en réduire leur sensibilité. Cela peut être réalisé par hachage cryptographique des données des individus, telles que son adresse IP, son identifiant utilisateur, son adresse e-mail.
Les informations supplémentaires permettant l'identification doivent être conservées séparément et être soumises à des mesures techniques et organisationnelles. Contrairement à l'anonymisation, la pseudonymisation est un processus réversible. Les données résultant d'une pseudonymisation sont considérées comme des données personnelles et restent donc soumises aux obligations du RGPD.
Le règlement européen encourage l'utilisation de la pseudonymisation dans le cadre du traitement des données personnelles. Par ailleurs le RGPD considère que la pseudonymisation permet de réduire les risques pour les personnes concernées et contribue à la mise en conformité au règlement.



1ER AXE : Poursuivre la sensibilisation du grand public aux enjeux de sécurisation des données personnelles dans les usages du quotidien

Dans la continuité des guides et contenus déjà publiés, la CNIL renforcera l'information du grand public sur la cybersécurité (mots de passe, principes de base, etc.) en produisant des ressources utilisables par le plus grand nombre, en publiant un guide « Comment protéger mes données ? » et en mettant en place des partenariats avec des relais au sein de la société civile et des entreprises, notamment via le collectif Educnum.

2E AXE : Accentuer l'accompagnement des entreprises, notamment des PME, en tirant les enseignements des violations de données personnelles reçues

Un effort particulier sera conduit pour sensibiliser les PME, les collectivités locales et les délégués à la protection des données sur les attaques les plus courantes et les nouvelles tendances ; il s'agira aussi d'accompagner les entreprises et les administrations dans l'utilisation des nouveaux outils du RGPD pour préciser les exigences en matière de sécurité.

La CNIL s'adressera aux différentes fonctions de ces organismes pour les sensibiliser aux questions de protection des données, afin que ces questions fassent réellement partie du quotidien opérationnel dans les organismes : c'est le sens de la publication d'un guide général à destination des développeurs incluant notamment des actions en matière de sécurité applicative (janvier 2020).

Par ailleurs, la CNIL développera une approche pédagogique de la sécurité, par exemple en produisant des fiches, à partir des notifications de violations reçues et des constats réalisés en contrôle, pour présenter de manière simple les principales attaques et failles de sécurité observées. Des recommandations sur les actions pour s'en prémunir pourront également être proposées. Un guide en ligne listant les principales mesures de sécurité identifiées par la CNIL pour répondre aux risques couramment rencontrés par les responsables de traitement viendra compléter le guide sécurité, notamment dans le cas des analyses d'impact sur la protection des données. Enfin, la CNIL étudiera la possibilité de publier de nouvelles recommandations relatives à la sécurité, en complément de la recommandation mot de passe.

3E AXE : Accroître la visibilité et la lisibilité de la politique répressive en matière de sécurité

Alors que la sécurité est l'un des manquements les plus sanctionnés, la CNIL poursuivra son action répressive sur les atteintes les plus manifestes à l'obligation de sécurité afin de s'assurer que les responsables de traitement atteignent un niveau minimal de sécurité.

4E AXE : Renforcer les liens avec l'écosystème de la cybersécurité

La CNIL participe déjà à de nombreux groupes professionnels (club EBOIS, CLUSIF, CESIN, ISO) et est partenaire du Forum International pour la Cybersécurité.

Elle jouera pleinement son rôle vis-à-vis de l'écosystème cyber, dont les solutions reposent parfois elles-mêmes sur des traitements de données personnelles devant respecter les obligations du RGPD. Elle poursuivra ainsi son travail avec la communauté cyber pour analyser plus finement comment les obligations du RGPD doivent être prises en compte dans l'utilisation des outils de protection des systèmes informatiques.

FOCUS

Le *credential stuffing*, une attaque par force brute sur les identifiants et mots de passe

Le *credential stuffing* consiste à tester, sur une page de connexion à un service, un grand nombre de couples « identifiant et mot de passe » provenant d'autres violations de données, parfois très anciennes. En partant du principe que les utilisateurs utilisent toujours les mêmes mots de passe, il est souvent possible d'obtenir des concordances (et donc, finalement, un accès illégitime à un service).

Cette technique d'attaque est proche des attaques par force brute dont l'objet est de renseigner et de tester, de façon automatique, un grand nombre de combinaisons possibles de mots de passe ou clés pour un identifiant connu. La contre-mesure la plus classique est le blocage de compte après quelques tentatives infructueuses, à la manière du blocage d'une carte de paiement après une saisie erronée consécutive de 3 codes PIN.

En ayant constaté que l'identifiant d'un utilisateur est souvent son adresse courriel et que la plupart des utilisateurs utilisent un seul et même mot de passe pour différents comptes, les attaquants ont imaginé ce nouveau type d'attaque qui exploite des listes qualifiées contenant des centaines de millions de courriels associés à un mot de passe, disponibles sur le dark web.

Si le *credential stuffing* ne permet pas forcément et facilement de cibler un compte en particulier, il permet :

- de trouver un grand nombre de comptes valides, car même un faible pourcentage de plusieurs centaines de millions de comptes représente un volume de données intéressant pour les attaquants ;
- de déjouer les mesures de sécurité les plus simples mises en œuvres ;
- d'être plus difficilement détecté : l'utilisation d'une architecture distribuée utilisant des réseaux de machines zombies (*botnets*) couplée à du *credential stuffing* et associée à de la résolution automatique de CAPTCHA contourne la majorité des systèmes dont les mesures de sécurité sont basiques.

Cependant, il existe des mesures pour se protéger. En tant que responsable de traitement, il est envisageable de :

- proposer un mécanisme de double authentification à ses utilisateurs voire une authentification forte lorsque cela est réaliste ;
- ne pas utiliser l'adresse courriel comme identifiant ;
- mettre en œuvre des dispositifs de détection de flux anormaux, en respectant les dispositions du RGPD.

En tant qu'utilisateur :

- utiliser un gestionnaire de mot de passe protégé avec un mot de passe robuste, ce qui facilite l'utilisation de mots de passe robustes et différents pour chaque service en ligne ;
- en cas de violation, à la réception d'un courriel de la part du responsable de traitement ou à la lecture d'un article de presse, modifier son mot de passe sur le service concerné et sur tous les autres services sur lesquels le même mot de passe a été utilisé ;
- utiliser la double authentification lorsque le service le propose ;
- si le service est très sensible (courriel, réseaux sociaux, banque, données de santé), utiliser une adresse courriel dédiée et non utilisée en dehors de ce cadre ;
- vérifier, lorsque cela est possible, que son adresse courriel n'est pas présente dans un fichier ou une base de données publiée à la suite d'un piratage, par exemple en utilisant **https://haveibeenpwned.com/**

Renforcer les solutions d'identité numérique grâce au RGPD

Dans un contexte de dématérialisation croissante des démarches administratives et de multiplication des services en ligne, la notion d'identité vit des mutations profondes, à mesure qu'émerge l'identité numérique. La maîtrise de ses identités par l'utilisateur et la sécurité de celles-ci sont primordiales pour la protection de la vie privée des personnes et le développement de services numériques de confiance.

L'INTÉRÊT DE L'IDENTITÉ NUMÉRIQUE

Pour une même personne, il peut exister plusieurs identités en fonction du contexte (état civil, vie sociale et professionnelle, services, jeux en lignes, etc.) et du niveau de confiance associé.

Une identité numérique peut reposer sur différents supports : cela peut être un téléphone, une carte à puce ou bien des serveurs lorsqu'elle est totalement dématérialisée. Dans de nombreux pays, et bientôt en France, l'État fournit une carte nationale d'identité numérique qui permet d'étendre au monde numérique la possibilité de prouver des éléments de son état civil du monde physique.

FOCUS

La différence entre carte d'identité biométrique et carte d'identité numérique

La biométrie est un moyen d'authentification comme les mots de passe, la possession d'un smartphone dont le numéro a été enregistré, ou encore une carte bancaire et son code PIN. Elle permet de vérifier le lien entre une identité et son porteur. Elle peut également servir à identifier les personnes.

Un règlement européen voté en juin 2019 oblige les États membres à rendre biométrique leur carte nationale d'identité en intégrant, sur un support sécurisé, une photo et deux empreintes digitales du titulaire. Ainsi celle-ci pourra être utilisée, comme cela est aujourd'hui le cas pour les passeports, pour authentifier le porteur lors des passages aux frontières. Cependant cela ne les rend pas nécessairement « numériques » car elles ne peuvent être utilisées que dans le monde physique.

Une carte d'identité « numérique » est une carte d'identité qui contient une identité numérique et qui peut être utilisée pour prouver en ligne les attributs d'identité qu'elle contient. Par exemple, la carte nationale d'identité belge n'est pas (encore) biométrique mais elle est pourtant numérique depuis 2004. Elle permet ainsi à ses détenteurs de s'authentifier auprès du gouvernement belge et de signer numériquement des documents. Autre exemple, la carte nationale d'identité allemande ne contient des données biométriques qu'à la demande du porteur mais peut, dans tous les cas, être utilisée pour prouver en ligne ses attributs d'identité. Dans un objectif de protection de la vie privée, la carte allemande permet aussi à son détenteur de prouver qu'il est majeur sans indiquer son âge ou sa date de naissance.

LES GRANDS PRINCIPES DE LA CNIL EN MATIÈRE D'IDENTITÉ NUMÉRIQUE

La mise en œuvre d'une solution d'identité numérique comporte nécessairement un traitement de données personnelles. Dès lors, le RGPD est applicable. Compte tenu du développement des solutions d'identités numériques, voici les principaux points de vigilance en matière de protection des données, étant rappelé que ces dispositifs doivent le plus souvent faire l'objet, avant leur déploiement, d'une analyse d'impact sur la protection des données (AIPD) compte tenu des enjeux pour les personnes.

La pluralité des identités numériques

L'identité numérique étant multiple et contextuelle, il est important de permettre aux individus d'avoir plusieurs identités numériques. Ainsi, un individu devrait pouvoir utiliser différentes identités numériques dans différents contextes (par exemple : une identité numérique dite « régalienne », liée à l'état civil et garantie par l'État, pour s'inscrire sur les listes électorales et une identité numérique liée à un pseudonyme choisi par l'utilisateur pour un réseau social).

La proportionnalité de la solution d'identité numérique et l'importance des pseudonymes

L'identification et l'authentification devraient être graduées selon la confiance nécessaire à chaque service en ligne. En effet, il n'est pas nécessaire de sécuriser l'ensemble des cas d'usage de l'identité numérique et il peut être à

la fois plus simple pour les organismes, plus ergonomique pour les utilisateurs et plus protecteur en termes de traitement de données personnelles d'adapter le niveau de sécurité requis aux risques liés à l'usage d'une identité numérique.

En pratique, l'utilisation obligatoire d'une identité régalienne forte (c'est-à-dire l'identité garantie par l'État au plus haut niveau d'assurance) pourrait être limitée à un nombre de cas réduits tandis que les solutions déclaratives et l'utilisation d'un pseudonyme pourraient être privilégiées dès lors qu'il n'y a pas de besoin particulier de fiabilité, sans renoncer à l'impératif de bien sécuriser l'usage de toutes ces identités.

La minimisation des données

Un des principes clés du RGPD est le principe de minimisation des données. Il implique de s'assurer de ne traiter que les seules données « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

En conséquence, lors de l'utilisation d'une identité numérique pour l'accès à un service, seules les informations strictement nécessaires aux traitements prévus par ce service devraient lui être communiquées. En pratique, cela consiste à créer ou utiliser des solutions qui donnent accès aux seuls attributs nécessaires, par exemple seulement à un pseudonyme ou seulement au prénom et à l'année de naissance, en fonction de la nature du service utilisé. De nouvelles solutions techniques intégrant la protection de la vie privée dès la conception permettent non seulement de ne donner accès qu'aux attributs nécessaires, mais aussi de répondre à certaines questions en ne donnant que l'information strictement nécessaire (par exemple en répondant par oui ou non à la question « la personne est-elle mineure » plutôt qu'en envoyant tous les attributs de son état civil).

Il s'agit aussi de limiter l'information collectée par le fournisseur d'identité. Par exemple, il est possible de mettre en place des solutions décentralisées, qui ne permettent pas au fournisseur d'identité de savoir à quel service une personne s'est connectée.

En outre, il convient de privilégier les solutions intégrant la protection de la vie privée dès la conception et par défaut.

Soigner l'information délivrée aux personnes

Les traitements d'identité numérique peuvent avoir un impact important sur la vie quotidienne des individus. Dans ce contexte, une vigilance particulière devrait être portée à l'information des personnes concernées sur le traitement de leurs données, que ce soit à l'enrôlement ou au moment de partager certains attributs d'identité.

Le cas particulier de l'usage de la biométrie

Dans certains cas, la biométrie peut être utilisée pour confirmer le lien entre une identité état civil ou « régalienne » et un individu. Elle peut être utilisée lors de la création de l'identité numérique, ou lors de son utilisation. Elle est également utilisée dans certains pays pour compenser l'absence de registres d'état-civil correctement constitués.

Si le recours à la biométrie pour vérifier l'identité d'une personne ou permettre son authentification à un service en ligne peut sembler légitime, ce type de traitement est particulier car il fait intervenir des données sensibles qui bénéficient d'un niveau de protection renforcé. En effet, la donnée traitée est consubstantielle de la personne concernée et ne peut pas être remplacée en cas d'usurpation ou de compromission (un individu peut changer de mot de passe mais ne peut pas changer d'empreintes digitales). Il convient, dès lors, de porter une attention toute particulière aux conditions de licéité d'un tel traitement (art. 9 du RGPD). De manière générale, le stockage sur des supports individuels ou permettant à la personne de garder le contrôle sur leurs données sont plus protecteurs pour les personnes que les dispositifs reposant sur une base centrale de données biométriques.

LES IDENTITÉS NUMÉRIQUES RÉGALIENNES

Les identités numériques régaliennes sont depuis quelques années soumises au règlement européen n°910/2014 du 23 juillet 2014 dit eIDAS. Celui-ci a pour objectif d'accroître la confiance dans les transactions électroniques et l'interopérabilité des systèmes d'identité au sein du marché intérieur. Pour cela il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques à travers l'Europe.

Ce règlement formule notamment des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique pour les échanges entre les organismes du secteur public et les usagers au niveau européen. Il définit trois niveaux de solutions (bas, substantiel et élevé) en fonction du niveau de vérification de l'identité, permettant ainsi de disposer d'un spectre allant d'une vérification préalable succincte à une vérification en profondeur et pouvant faire intervenir des moyens d'authentifications variés (du mot de passe à la carte à puce).

Un niveau « bas » pourra suffire pour s'inscrire à des cours de natation sur le site de la mairie tandis qu'un niveau élevé pourrait être requis pour la déclaration de naissance d'un enfant. La bonne pratique est d'utiliser le niveau le plus faible qui garantisse un niveau de confiance suffisant pour un service donné.

FranceConnect

Aujourd'hui les solutions d'identité numériques eIDAS sont mises en œuvre grâce à France Connect, qui sert de pont entre des fournisseurs d'identité (les impôts, la Poste, Ameli, Alicem, etc.) et de nombreux services de l'administration en ligne (mairies, renouvellement de permis de conduire, etc.) ou des services

privés ayant un besoin réglementaire de vérifier des attributs d'identité.

S'il faut avoir à l'esprit que l'inaccessibilité de FranceConnect aurait un impact important sur l'accès à de nombreux services publics, cette architecture présente trois principaux avantages :

1 - Les fournisseurs d'identité n'ont pas connaissance des services utilisés par le détenteur de l'identité.

2 - France Connect peut sensibiliser les fournisseurs de service à l'importance d'identifier les attributs strictement nécessaires et suffisants à leur service, et ne leur transférer que ceux-ci.

3 - France Connect ne nécessite pas la mise en œuvre d'un registre de la population dédié à la gestion de l'identité numérique, même si France Connect effectue une vérification auprès du registre national d'identification des personnes physiques.

Il est à noter que FranceConnect centralise les traces techniques de connexion, et que l'utilisateur peut consulter ses traces et vérifier si des accès illégitimes ont eu lieu.

Le premier fournisseur d'identité visant un niveau élevé en France : Alicem

Alicem est une application mobile permettant aux personnes majeures titulaires d'un passeport biométrique ou d'un titre de séjour biométrique de créer une identité numérique pour accéder à des services en ligne tels que l'assurance maladie, la CAF, le site « impots.gouv.fr », etc.

Dans un premier temps, l'identité numérique Alicem ne pourra être utilisée que par l'intermédiaire de FranceConnect. C'est la première solution d'identité numérique développée par l'État qui vise à atteindre le niveau élevé au sens du règlement eIDAS. Une phase expérimentale a été lancée en 2019.

Sollicitée dans le cadre d'une demande d'avis, la CNIL a conseillé au gouvernement de ne pas rendre obligatoire l'utilisation de la reconnaissance faciale pour l'enrôlement. La CNIL a même suggéré d'utiliser des solutions alternatives à la reconnaissance faciale pour vérifier l'identité de la personne :

- Une vérification de l'identité en face à face : déplacement en préfecture, en mairie, auprès d'un service public accueillant du public.
- Une vérification manuelle de la vidéo et de la photographie sur le titre : envoi de la vidéo sur les serveurs de l'ANTS[21] et vérification opérée par un agent.
- Appel vidéo en direct avec un agent de l'ANTS.

À SUIVRE

2021 : année de la carte nationale d'identité numérique ?

En application du règlement européen relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union adopté en juin 2019, le gouvernement prévoit une carte d'identité numérique française pour 2021.
Cette carte serait à la fois une carte d'identité « classique » et le support d'une identité numérique forte portée par l'État.

Alors que les technologies ont beaucoup progressé ces dernières années, y compris pour proposer des systèmes plus protecteurs des données personnelles, la France pourrait être à la pointe de l'identité numérique respectueuse de la vie privée en choisissant une solution limitant au strict nécessaire ce que chaque entité participant à son utilisation obtient comme information, que ce soit à la création ou à l'utilisation d'une telle identité.

La CNIL devra être saisie pour avis des projets de textes qui viendront encadrer le futur dispositif. À ce stade, plusieurs éléments pourraient notamment être pris en compte :

- Certaines **architectures décentralisées** permettent d'éviter une interaction systématique avec le fournisseur d'identité au moment de l'utilisation du service. Comme pour la majorité des utilisations de la carte d'identité dans le monde physique, seul le fournisseur de service et l'utilisateur sont en mesure de savoir que l'identité est utilisée à un moment donné pour un service donné. En outre, lorsqu'une identification de plus haut niveau est requise, ou toutes les X utilisations de l'identité, une vérification que l'identité n'a pas été révoquée peut être mise en œuvre.
- Ces solutions pourraient intégrer, dès la conception, l'utilisation de différents identifiants, pour permettre par exemple **l'utilisation de plusieurs identifiants** sectoriels pour le secteur public.
- Afin de respecter le principe de minimisation des données, la solution choisie pourrait **permettre au fournisseur de service d'indiquer quels sont les attributs dont il a besoin** et assurer que seuls ceux-ci lui soient transmis.
- La solution choisie pourrait intégrer des **technologies de preuve de connaissance** qui permettent, par exemple, d'obtenir uniquement une preuve de majorité de la personne.

21 L'ANTS est l'agence nationale en charge de l'émission des titres d'identité : carte d'identité, passeport ou encore permis de conduire. Elle dépend du ministère de l'Intérieur.

Déréférencement, ciblage publicitaire et directive « Police-Justice » : retour sur l'actualité jurisprudentielle

Des décisions importantes en matière de déréférencement ont été rendues d'abord par la Cour de justice de l'Union européenne (CJUE) en septembre 2019, et par le Conseil d'État français en décembre 2019 puis en mars 2020. De plus, l'actualité jurisprudentielle, notamment l'arrêt du Conseil d'État concernant les « Américains accidentels » a permis de mieux comprendre l'articulation entre le RGPD et la directive « Police-Justice ».

DÉRÉFÉRENCEMENT : LES ÉCLAIRAGES DE LA CJUE ET DU CONSEIL D'ÉTAT

DÉFINITION

Le déréférencement permet de faire supprimer un ou plusieurs résultats fournis par un moteur de recherche à l'issue d'une requête effectuée à partir de l'identité (nom et prénom) d'une personne.
Cette suppression ne fait pas disparaître l'information sur le site web source : le contenu original reste inchangé et est toujours accessible en utilisant d'autres critères de recherche ou en allant directement sur le site à l'origine de la diffusion.

En 2016, la CNIL avait prononcé à l'encontre de la société Google une sanction publique de 100 000 €, en raison du refus de la société d'étendre ses mesures de déréférencement à l'ensemble des versions de son moteur de recherche. Google avait alors contesté cette sanction devant le Conseil d'État.

Dans le même temps, des personnes auxquelles Google avait refusé le déréférencement, ce qui avait par la suite été confirmé par la CNIL, ont contesté devant le Conseil d'État la décision de la CNIL.

Le Conseil d'État avait alors interrogé la CJUE afin d'obtenir des éclaircissements sur les modalités pratiques d'application du droit au déréférencement évoquées par cette même Cour en 2014 (arrêt « Google Spain »).

La CJUE a rendu deux arrêts le 24 septembre 2019, conduisant le Conseil d'État à se prononcer à son tour le 6 décembre 2019 à travers treize décisions.

La CJUE et le Conseil d'État ont d'abord rappelé que le traitement opéré par une société exploitant un moteur de recherche est spécifique, dans la mesure où elle n'est pas responsable de la diffusion de données, mais de leur seul référencement.

Les deux juridictions européenne et française ont apporté des éclairages sur des cas bien précis d'application du droit au déréférencement : d'une part, lorsque des données sensibles ou des infractions ou condamnations pénales sont concernées ; d'autre part, sur la portée territoriale du déréférencement.

Les plateaux de la balance du déréférencement

Les moteurs de recherche et les autorités de contrôles nationales disposent désormais d'un « guide du déréférencement », qui conduit à distinguer trois sortes de données :

- les données ordinaires (qui n'entrent pas dans les deux catégories suivantes) ;
- les données sensibles (au sens de l'article 9 du RGPD : religion, santé, etc.) ;
- les données faisant apparaître des infractions et condamnations pénales.

Les règles applicables à toute demande de déréférencement

Quelles que soient les données concernées, un moteur de recherche saisi d'une demande de déréférencement ou une autorité de contrôle nationale saisie d'une plainte pour refus de déréférencement doit se prononcer en prenant en compte :

- la nature des données en cause ;
- le contenu et son caractère plus ou moins objectif ;
- l'exactitude des données ;
- leur source ;
- les conditions et la date de leur mise en ligne ;
- les répercussions que leur référencement est susceptible d'avoir pour la personne concernée ;
- la notoriété de cette personne, son rôle dans la vie publique et sa fonction dans la société ;
- le rôle qu'elle a joué, le cas échant, dans la publicité conférée aux données la concernant.

Un moteur de recherche doit, à l'occasion d'une demande de déréférencement, faire la balance entre respect de la vie privée et protection des données, d'un côté, et droit à l'information des internautes, de l'autre.

Le fait de pouvoir accéder aux informations visées par la demande de déréférencement à partir d'une recherche effectuée sur d'autres mots clés que les prénoms et nom de la personne concernée (en accédant, par exemple, aux informations relatives à une conférence à laquelle la personne concernée avait participé en effectuant une recherche à partir de la date et du sujet de la conférence), constitue également un critère à prendre en compte en faveur du déréférencement.

Par exemple, le Conseil d'État a pris en compte la possibilité d'accéder à des informations relatives à un brevet d'invention à partir d'une recherche portant sur des mots clés ne mentionnant pas le nom du plaignant l'ayant déposé dans le passé.

Données sensibles et infractions ou condamnations pénales

Le déréférencement de résultats de recherche faisant apparaître des données sensibles

La CJUE rappelle que les données sensibles sont soumises à un régime de protection particulier (les « catégories particulières de données » au sens de l'article 9 du RGPD) et précise que celui-ci est aussi applicable aux moteurs de recherche.

Le traitement de données sensibles étant interdit, sauf exception (par exemple si la personne concernée a donné un consentement valide ou si elle a elle-même rendu publique ces données), la CJUE en déduit qu'une société exploitant un moteur de recherche doit, par principe, déréférencer un résultat de recherche faisant apparaître des données sensibles.

Toutefois, prenant en compte la nature spécifique du traitement opéré par un moteur de recherche, la CJUE n'interdit pas aux moteurs de recherche d'indexer des contenus comportant des données sensibles.

Les moteurs de recherche doivent donc seulement procéder à cette vérification à l'occasion d'une demande de déréférencement introduite par la personne concernée et sous le contrôle des autorités nationales compétentes.

Lors de l'examen de cette demande, le moteur de recherche doit vérifier « si l'inclusion de ce lien dans la liste de résultats, qui est affichée à la suite d'une recherche effectuée à partir du nom de cette personne, s'avère strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche ».

Au regard de la nature particulière des données sensibles, leur simple présence induit cependant une pondération particulière en faveur du déréférencement (sauf s'il s'agit de données manifestement rendues publiques par la personne concernée : on retombe alors dans le régime des données ordinaires).

Le déréférencement de résultats faisant apparaître des infractions ou condamnations pénales

Comme pour les données sensibles, les données d'infractions induisent une pondération particulière en faveur du déréférencement. La CJUE a ainsi considéré que la présence de données relatives à des infractions et condamnations pénales doit, en principe, conduire au déréférencement, sauf si les données en question apparaissent « strictement nécessaires » à l'information du public.

Elle a donc précisé les critères à prendre en compte pour traiter une demande de déréférencement portant sur ces données :

- la nature et la gravité de l'infraction ;
- le déroulement de la procédure, son

issue et l'étape de cette procédure à laquelle renvoie l'information ;
- le temps écoulé ;
- le rôle joué par la personne dans la vie publique et son comportement dans le passé ;
- l'intérêt du public au moment de la demande ;
- le contenu et la forme de la publication ainsi que les répercussions de celle-ci pour la personne.

Par ailleurs, le moteur de recherche est tenu d'aménager en permanence, et au moins lors de l'examen de la demande de déréférencement, la liste des résultats qu'il propose en vue d'assurer que le premier de ces résultats, au moins, mène à des informations à jour sur la situation judiciaire de la personne concernée.

La notoriété de la personne qui demande le déréférencement est un élément central à prendre en compte dans cette balance, d'après les décisions rendues par le Conseil d'État.

Portée territoriale du déréférencement

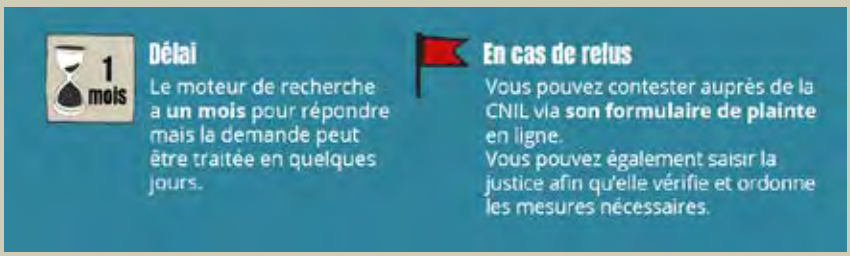
La CJUE a, dans l'un des arrêts du 24 septembre 2019, apporté d'importantes précisions sur la portée territoriale du déréférencement.

La portée exclusivement européenne, en principe, du droit au déréférencement

Lorsqu'il est appliqué, le déréférencement doit en principe être **effectif sur toutes les versions européennes du moteur de recherche.**

Concrètement, aucune recherche effectuée à partir du territoire européen sur la base de l'identité du demandeur ne doit pouvoir conduire au contenu déréférencé. Par exemple, les internautes italiens ne doivent pas pouvoir accéder à un contenu déréférencé en effectuant une recherche sur la base de l'identité d'un demandeur français, mais un internaute américain continuera, lui, à y avoir accès.

Comment s'assurer en pratique que le déréférencement d'un lien soit bien effectif sur l'ensemble des versions européennes du moteur de recherche, sans que ce cantonnement aux versions européennes soit aisément contournable, au moyen de certaines techniques, par un internaute situé en Europe ?
La Cour de justice de l'Union européenne renvoie aux juridictions nationales le soin d'apprécier, dans les affaires dont elles sont saisies, si le moteur de recherche a pris des mesures techniques suffisantes pour prévenir autant que possible ce risque de contournement.



FOCUS

Exemples de demandes

Le Conseil d'État a jugé comme strictement nécessaire à l'information du public le référencement de résultats de recherche renvoyant à des articles de presse relatifs à la condamnation, pourtant annulée par la Cour de Cassation, d'un maire pour apologie de crimes de guerre ou contre l'humanité.

Une personne demandait le déréférencement d'un lien renvoyant vers un site faisant état de son livre, indisponible à la vente, révélant son orientation sexuelle. Compte tenu du fait qu'il n'exerce plus d'activités littéraires et que le roman n'est plus édité, le Conseil d'État a jugé que le lien devait être déréférencé.
En revanche, d'autres liens renvoyant vers des informations relatives au roman, ne révélant pas son orientation sexuelle, peuvent être maintenus compte tenu de l'intérêt du public et du fait que les informations ont été manifestement rendues publiques par la personne.

C'est donc la présence de données sensibles qui fait la différence.

La question de l'institution d'un déréférencement de portée mondiale dans certaines hypothèses

La Cour de justice de l'Union européenne a également rappelé que les États membres peuvent instituer des standards de protection des droits fondamentaux plus élevés que ceux de l'Union européenne. Elle a souligné que le droit européen n'interdit pas à un État membre de prévoir un déréférencement de portée mondiale, c'est-à-dire l'impossibilité pour les internautes d'accéder à un lien déréférencé à partir de l'identité de la personne concernée, et ce peu importe leur lieu de recherche dans le monde.

Dans sa décision du 27 mars 2020 (CE, 27 mars 2020, *Google Inc.*, n° 39922) le Conseil d'État a estimé qu'une intervention du législateur est toutefois nécessaire pour autoriser la CNIL ou les juridictions françaises à ordonner un tel déréférencement mondial.

Par ailleurs, s'il était prévu par la loi, un tel déréférencement mondial ne serait pas systématique. La CNIL devrait, au cas par cas, mettre en balance entre, d'une part, l'atteinte particulièrement grave au droit de la personne concernée au respect de sa vie privée et à la protection de ses données personnelles et, d'autre part, le droit à la liberté d'information.

Prenons l'exemple d'un lien référencé aux nom et prénoms d'un plaignant français renvoyant vers un site japonais diffusant à son insu une vidéo pornographique le faisant apparaître. Un déréférencement mondial pourrait être justifié : en effet, d'une part, au vu de la nature du contenu et de l'absence de notoriété du plaignant, son déréférencement ne risque pas de porter atteinte à la liberté d'information du public international (un tel contenu n'ayant aucun intérêt à apparaître à la saisie des nom et prénom du plaignant sur un moteur de recherche) ; d'autre part, la gravité de l'atteinte portée aux droits et libertés du plaignant par un tel référencement et l'utilité d'une extension territoriale du déréférencement sont de nature à justifier un déréférencement mondial.

QUELLE ARTICULATION ENTRE LE RGPD ET LA DIRECTIVE « POLICE-JUSTICE » ?

Le RGPD et la directive dite « Police-Justice » **sont deux textes européens entrés en application en 2018 et qui présentent des champs d'application distincts et complémentaires.** Ils constituent le « paquet européen » de protection des données personnelles.

Les traitements mis en œuvre pour assurer la sûreté ou la défense de l'État sont exclus de ce cadre européen, puisqu'ils ne relèvent pas du champ d'application de l'Union européenne, et restent donc régis par les dispositions de la seule loi Informatique et Libertés (par exemple, un traitement qui aurait pour finalité le renseignement à des fins de sûreté de l'État).

On peut considérer, pour simplifier, que **le régime général est celui du RGP** : c'est le cas des traitements en matière civile ou commerciale, par exemple, mais aussi administrative. Cependant, lorsqu'un traitement est mis en œuvre « par les autorités compétentes 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, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces », alors ces traitements relèvent exclusivement de la directive « Police-Justice ». Il s'agit donc d'un **régime spécifique.**

La distinction entre l'objet d'un traitement et sa finalité

Pour déterminer si un traitement relève du champ du RGPD, du champ de la directive « Police-justice », voire de ces deux champs simultanément, il faut se fonder sur l'analyse des **finalités** du traitement, c'est-à-dire sur les objectifs poursuivis par le gestionnaire du fichier.

Dans sa décision dite « Association des Américains accidentels » du 19 juillet 2019, le Conseil d'État a toutefois introduit une distinction entre la **finalité** d'un traitement et son (ou ses) **objet**(s). La notion d'objet intervient pour déterminer s'il existe un **formalisme particulier**

FOCUS

Exemple de cette articulation : l'arrêt «Association des Américains accidentels» du Conseil d'État

Le Conseil d'État, dans sa décision dite « Association des Américains accidentels » du 19 juillet 2019, illustre l'articulation des champs juridiques prévus par le RGPD et la directive « Police-Justice ».
Il s'agissait de déterminer, notamment, si le traitement automatisé d'échange automatique des informations dénommé EAI, mis en œuvre par la direction générale des finances publiques (DGFiP) en vue de transférer des données personnelles sur des contribuables « Américains accidentels » aux autorités fiscales des États-Unis, relevait du RGPD ou de la directive « Police-Justice ».
Le Conseil d'État rappelle que le critère déterminant dans la détermination du champ juridique applicable est la finalité poursuivie par le traitement.
Ce faisant, **il distingue la notion de finalité et celle d'objet d'un traitement.**
En effet, la haute juridiction souligne que si le traitement en question a plusieurs objets dont celui de la prévention, la détection et la répression des infractions pénales, sa finalité est de permettre, en luttant contre la fraude et l'évasion fiscale, l'amélioration du respect de leurs obligations fiscales par les contribuables français et américains. Le traitement EAI n'a pas été mis en œuvre avec une finalité pénale, il relève donc du RGPD.

à respecter avant la mise en œuvre d'un traitement de données personnelles.

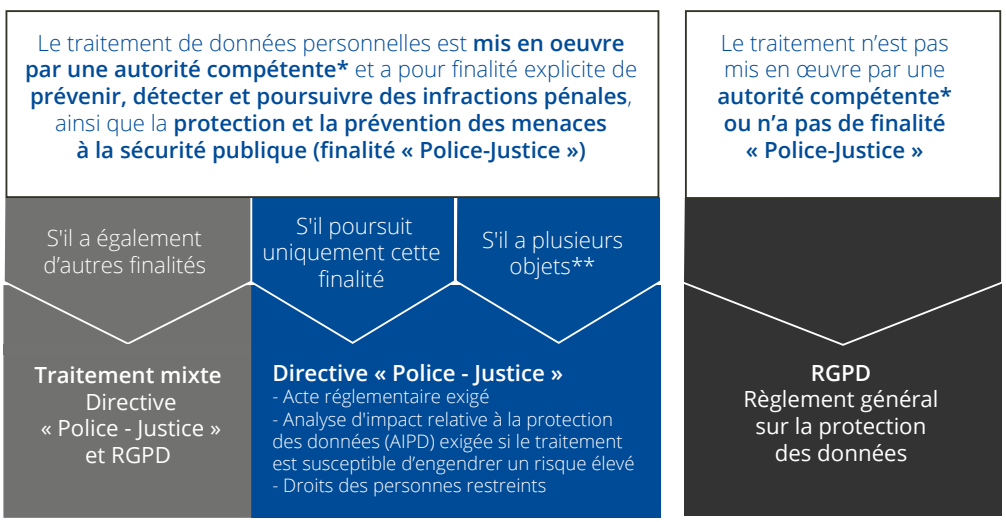
Si le RGPD a supprimé la plupart des formalités (déclarations, autorisations), la loi Informatique et Libertés prévoit en effet le maintien de certaines procédures préalables notamment pour les fichiers régaliens. L'article 31 de la loi prévoit ainsi que les traitements ayant pour « objet » la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté et mis en œuvre pour le compte par arrêté du ou des ministres compétents ou par décret en Conseil d'État (dans les deux cas pris après avis motivé et publié de la CNIL), en cas de traitement de données. Cet article s'applique, quel que soit le régime juridique applicable au traitement, qu'il relève du régime juridique du RGPD ou de la directive. Il est ainsi concevable qu'un fichier poursuive une finalité le conduisant à relever du RGPD, bien qu'il comporte, parmi ses objets (c'est-à-dire les utilisations qui sont faites de ses données), des usages relevant du champ pénal.

DÉFINITION

La finalité peut être comprise comme l'objectif justifiant l'utilisation de données personnelles.

Directive « Police-Justice » ou RGPD ?

Grille de lecture indicative pour les traitement relevant du paquet européen.



** Toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en matière pénale ou l'exécution de sanctions pénales (autorités judiciaires par ex.) ou tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de mettre en œuvre un traitement relevant de la directive (par ex. les services internes de sécurité de la SNCF).*
*** Pour comprendre la différence entre finalité et objet voir la décision dite « Américains accidentels » du 19 juillet 2019 (n°424216) du Conseil d'État.*

FOCUS

La décision du Conseil d'État du 16 octobre 2019 sur le plan d'action de la CNIL dans le domaine du ciblage publicitaire en ligne.

Le 16 octobre 2019, le Conseil d'État a rejeté le recours des associations La Quadrature du Net et Caliopen contre la décision de la CNIL de ménager une période d'adaptation en faveur des responsables de traitement en matière de dépôt de cookies et autres traceurs, explicitée dans deux communiqués les 28 juin[22] et 18 juillet[23] 2019 publiés sur son site web.

En effet :

- la CNIL avait annoncé, dans son communiqué de presse du 28 juin 2019, un plan d'action qui précisait les règles en matière de ciblage publicitaire ainsi que l'accompagnement des acteurs dans leur mise en conformité dans ce rapport d'activité, page 16.

- par une délibération du 4 juillet 2019, la CNIL a adopté des lignes directrices abrogeant sa recommandation du 5 décembre 2013 relatives aux cookies, qui considérait comme acceptable la poursuite de la navigation comme expression du consentement au dépôt de cookies et autres traceurs – pratique qui n'est plus acceptable depuis l'entrée en application du RGPD.

- un communiqué de presse du 18 juillet 2019 précisait qu'une nouvelle recommandation précisant les modalités pratiques de recueil du consentement au dépôt de cookies allait être adoptée dans le premier semestre 2020 et qu'une période d'adaptation de six mois suivant la publication de la future recommandation allait être laissée aux responsables de traitement pour respecter les nouvelles règles issues du RGPD.

Le Conseil d'État :

- a rejeté le recours des associations dirigé contre la période d'adaptation, au motif que la CNIL dispose d'un large pouvoir d'appréciation pour l'accomplissement de ses missions, en particulier pour ce qui concerne l'exercice de son pouvoir de sanction, que ce soit pour apprécier l'opportunité d'engager des poursuites de sa propre initiative ou pour décider des suites à donner aux plaintes qu'elle peut recevoir. Il a précisé que la CNIL peut élaborer un plan d'actions destiné à accompagner les acteurs concernés et rendre publique la position adoptée quant à l'usage de ses pouvoirs, notamment de sanction, sans méconnaître l'étendue de sa compétence.

- a considéré que la période d'adaptation, au cours de laquelle les opérateurs tolérant la poursuite de la navigation comme une modalité valable de recueil du consentement ne feront pas l'objet de sanctions de la part de la CNIL, a pour objet de permettre à l'ensemble des opérateurs de se mettre effectivement en conformité en définissant de nouvelles modalités pratiques de recueil du consentement. Il a également relevé que la CNIL continuera de contrôler le respect des autres obligations préexistantes depuis plusieurs années (existence d'un consentement préalable avant tout dépôt de cookies, possibilité de retirer son consentement de manière aisée, etc.).

- a jugé que la décision attaquée ne méconnaît pas le droit au respect de la vie privée et le droit à la protection des données personnelles prévus par l'article 7 de la Charte des droits fondamentaux de l'Union européenne et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, dès lors qu'elle contribue à remédier à des pratiques contraires au RGPD et à la loi Informatique et Libertés.

- a révélé, d'ailleurs, que le plan d'action global de la CNIL fixait pour l'ensemble des opérateurs, à une échéance raisonnable, une obligation de mise en conformité que l'exercice du pouvoir de sanction de la CNIL (appliqué de manière étalée dans le temps à des opérateurs particuliers) ne pourrait, en tout état de cause, pas faire respecter plus rapidement.

22 « Ciblage publicitaire en ligne : quel plan d'action de la CNIL ? », 28 juin 2019, cnil.fr
23 « Cookies et autres traceurs : la CNIL publie de nouvelles lignes directrices », 18 juillet 2019, cnil.fr

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 et sur les réseaux sociaux où elle met à disposition des outils pédagogiques et pratiques adaptés aux publics variés auxquels elle s'adresse.

Carole
Téléconseillère au service des relations avec les publics

En tant que téléconseillère juridique au service des relations avec les publics de la CNIL, j'ai pour mission d'informer, de conseiller et d'accompagner les usagers, particuliers comme professionnels.

Je traite à la fois des demandes écrites, courriers postaux, courriels, et demandes par formulaire en ligne, et j'assure la permanence téléphonique juridique.

Depuis l'entrée en application du RGPD, les sollicitations ont augmenté et ont changé. Face à cette nouvelle règlementation européenne, les professionnels nous demandent de les accompagner dans leurs démarches de conformité. Les particuliers, quant à eux, ont pris davantage conscience de leurs droits et entendent les exercer.

Ce métier est très enrichissant, j'apprends en continu. J'aime le contact avec les usagers et pouvoir leur apporter mon aide. Les questions posées sont variées et touchent tous les secteurs (travail, santé, commerce, énergie, banque, transport, réseaux sociaux, etc.).

Je suis également référente « commerce et marketing » ce qui me permet de travailler avec les autres services de la CNIL sur ces sujets, d'approfondir mes connaissances et ainsi d'accompagner encore mieux nos usagers.

8 005 443

visites sur cnil.fr en 2019

79

actualités et communiqués publiés en 2019

540

contributions aux consultations

6

consultations en ligne ont été publiées, avant l'adoption de référentiels ou d'un règlement type

DEUX ANS APRÈS LE RGPD, UNE PRISE DE CONSCIENCE INÉDITE

Le site de la CNIL

Deux ans après l'entrée en application du RGPD, **le nombre de visiteurs, qui reste stable par rapport à 2018 (8 098 232 visites)**, témoigne de l'intérêt constant du public pour les enjeux autour de la vie privée. La majorité des internautes visite les contenus relatifs au RGPD, qu'il s'agisse d'explications ou d'outils pratiques.

Afin de consolider ce qui a été accompli en 2018 pour le volet « Professionnel » du site web de la CNIL, de nouveaux outils, généraux ou spécifiques à des secteurs d'activité, sont régulièrement venus enrichir ceux existants. Par exemple, **un nouveau modèle de registre**, diffusé dans un format libre et ouvert (ODS) vient compléter les modèles déjà existants. **Plusieurs guides pratiques** ont également été conçus, notamment pour les collectivités territoriales, les développeurs ou les organismes publics souhaitant mettre en place de ***l'open data***.

La CNIL a également publié de nouveaux cadres de référence : un référentiel sur la gestion des vigilances sanitaires et un référentiel relatif aux dispositifs d'alertes professionnelles : ainsi, **la page « les cadres de référence »** a été revue et permet d'orienter au mieux les professionnels sur les changements introduits par le règlement, notamment la fin de la plupart des formalités. Le volet « Particulier » a bénéficié de nombreux contenus dédiés à la vie quotidienne numérique, grâce, notamment, à des fiches pratiques sur **les objets et jouets connectés**, sur les applications mobiles ou encore de nouvelles explications sur le droit au déréférencement. Les infographies et les vidéos, créées ou mises à jour, apportent un aspect pédagogique essentiel aux contenus éditoriaux.

Top 3 des actualités les plus consultées à destination des professionnels en 2019

- La CNIL lance sa formation en ligne sur le RGPD
  107 446 vues
- La CNIL publie un nouveau modèle de registre simplifié
  40 918 vues
- Développeurs : la CNIL met en ligne un kit de bonnes pratiques
  18 957 vues

Top 3 des communiqués les plus consultés publiés en 2019

- La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros contre Google LLC
  42 700 vues
- Cookies et autres traceurs : la CNIL publie de nouvelles lignes directrices
  23 246 vues
- SERGIC : sanction de 400 000 € pour atteinte à la sécurité des données et non-respect des durées de conservation
  22 154 vues

Top 3 des contenus pour les particuliers les plus consultés en 2019

- Faites régulièrement le ménage dans l'historique de navigation
  120 931 vues
- Les droits pour maîtriser vos données personnelles !
  115 396 vues
- Les courriers pour agir
  115 099 vues

Top 10 des contenus RGPD les plus consultés publiés en 2019

- RGPD - Par où commencer ? **234 744 vues**
- RGPD - Se préparer en 6 étapes **209 237 vues**
- Le registre des activités de traitement **160 426 vues**
- Le règlement général sur la protection des données - RGPD - **138 424 vues**
- Comprendre le RGPD - **135 648 vues**
- Les droits pour maîtriser vos données personnelles - **115 396 vues**
- RGPD : de quoi parle-t-on ? **90 526 vues**
- Conformité RGPD : comment informer les personnes et assurer la transparence ? **88 099 vues**
- Règlement européen sur la protection des données : ce qui change pour les professionnels - **85 810 vues**
- Outil PIA : téléchargez et installez le logiciel de la CNIL - **78 116 vues**

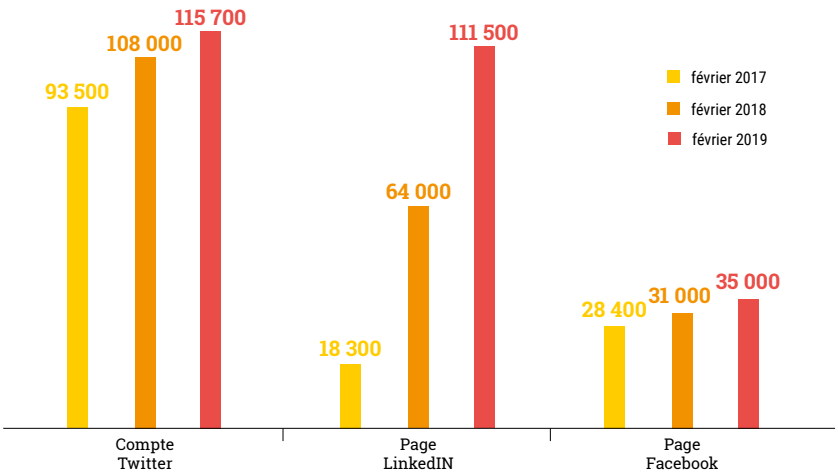
Les réseaux sociaux

La prise de conscience sur la protection des données est remarquable sur les réseaux sociaux : ainsi, plus de 262 000 comptes suivaient la CNIL fin 2019.

L'accompagnement de la CNIL auprès des professionnels a porté ses fruits, avec une **croissance de près de 50 % des *followers* sur LinkedIn en un an.** Si Twitter a connu une évolution plus modérée en 2019 que l'année précédente, Facebook a bénéficié d'une plus grande augmentation : de nombreux contenus à destination des particuliers ont été relayés sur ce réseau.

Les publications qui ont créé le plus d'engagement traitaient de l'actualité répressive de la CNIL ou des guides pratiques, bien que certains supports plus pédagogiques aient bénéficié d'un fort engagement de la part de la communauté, notamment la vidéo sur les jouets connectés. En images ou en *threads*, la tendance de 2019 était, pour les particuliers, aux conseils quotidiens de cybersécurité, par exemple sur l'e-réputation, les mots de passe ou encore les applications mobiles.

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



Nombre de fans sur Facebook au 3 février 2020

35 000
CNIL

4 700
Educnum

Nombre de *followers* sur Twitter au 3 février 2020

115 700
@CNIL

2 600
@Educnum

5 000
@LinCNIL

4 000
@CNIL_en

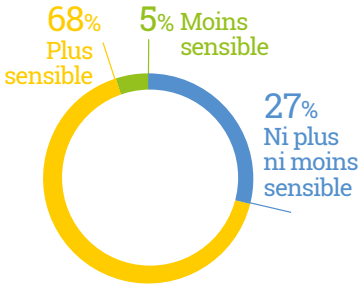
LES FRANÇAIS TOUJOURS PLUS SENSIBLES AUX ENJEUX DES DONNÉES PERSONNELLES

Selon un sondage IFOP réalisé en octobre 2019[1], **68 % des Français se disent plus sensibles à la question de la protection de leurs données personnelles.** Cette prise de conscience est dans la tendance de l'étude réalisée un an plus tôt, en octobre 2018 (66 %) et cristallise plusieurs inquiétudes : les piratages ou les vols de données, les spams et sollicitations commerciales ou encore l'utilisation faite des données par les réseaux sociaux.

45 % des personnes interrogées ont déjà constaté des abus dans l'utilisation faite de leurs données personnelles et, parmi eux, 20 % ont pris des mesures en réponse à ces abus, soit une augmentation de 4 % par rapport à 2018.

La progression du nombre de « comportements actifs » de la part des personnes ayant subi de tels abus traduit une certaine évolution de la prise de conscience sur les enjeux de la vie privée. Cela démontre la nécessité d'un accompagnement, de formation et de pédagogie concernant les outils existants, encore peu maîtrisés par les Français.

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 ?



1 Sondage réalisé en ligne, du 25 au 28 octobre 2019, auprès d'un échantillon de 1 004 personnes, représentatif de la population française âgée de 18 ans et plus.

Un guide de sensibilisation à destination des collectivités

Afin d'accompagner les collectivités territoriales dans leur mise en conformité au RGPD, la CNIL a élaboré un guide de sensibilisation disponible sur son site web et distribué directement aux 36 000 collectivités de France ainsi qu'au Salon des maires et des collectivités locales, auquel la CNIL était présente.

Ce guide s'adresse prioritairement aux communes de petite ou de moyenne taille, ainsi qu'à leurs groupements intercommunaux, ne disposant pas nécessairement en interne de ressources dédiées spécifiquement à la protection des données. Il propose des clés de compréhension des grands principes, des réflexes à acquérir, un plan d'action pour se mettre en conformité ainsi que des fiches pratiques. Il évoque les conditions de désignation du délégué à la protection des données afin que chaque collectivité puisse identifier la modalité la plus adaptée à sa situation.

Pour élaborer ce guide, la CNIL s'est rapprochée des principales associations regroupant les différents niveaux de collectivités et autres organismes intervenant auprès du secteur public local. Cet appui permet d'apporter des réponses concrètes et adaptées aux collectivités. Ce guide a été envoyé en version papier à toutes les mairies de Métropole et d'outre-mer.

En complément, des fiches techniques consacrées aux principaux sujets de préoccupation des collectivités ont été publiées sur le site web de la CNIL.

Ce guide a été réalisé par la CNIL avec le concours de l'Association des maires ruraux de France (AMRF), de l'Association des maires de France (AMF), de l'Association nationale des directeurs d'associations départementales de maires (ANDAM), de l'Assemblée des départements (ADF), des régions de France, de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP) et de la direction générale des collectivités locales (DGCL).

Des fiches pratiques en prévision des élections

En prévision des élections municipales de 2020, la CNIL a mis à jour plusieurs contenus destinés aux candidats et à leurs équipes électorales, dans une thématique « Vie politique et citoyenne » sur son site web.

Ces fiches pratiques regroupent des conseils pratiques généraux ou des explications plus approfondies sur certains sujets (communication par téléphone ou courrier électronique, les fichiers utilisables, les réseaux sociaux). La CNIL a également mis en place une plateforme de signalement sur son site web.

Cette action s'adresse également aux électeurs : en offrant une fiche récapitulant leurs différents droits et en proposant une plateforme de signalement pour ces élections.

LES RÉPONSES AUX PUBLICS

La CNIL informe et conseille les particuliers et les professionnels désireux d'obtenir un renseignement juridique ou une aide à la mise en conformité de leur traitement aux règles régissant la protection des données personnelles. Les usagers contactent la CNIL par téléphone lors des permanences juridiques tenues 4 jours par semaine, par téléservices en ligne, ou encore par courriel ou par courrier postal.

L'année 2019 a connu une augmentation sensible du nombre de requêtes écrites reçues (+ 5 %) avec 17 302 requêtes adressées principalement par les particuliers soucieux de connaître leurs droits ou désirant les exercer (droit d'accès pour l'essentiel). Le téléservice « Nous contacter » est la voie la plus utilisée par les usagers et est en constante progression (+ 6 % cette année).

La prise de conscience par les usagers de leurs droits est aussi confirmée par la forte augmentation de la consultation de la rubrique « Besoin d'aide » (+ 44 %), qui s'est enrichie à cet effet de 30 nouvelles réponses (soit un fond actualisé de 521 questions/réponses).

Les thématiques les plus consultées portent sur la CNIL (81 296 consultations), le casier judiciaire (28 530 consultations) et l'*opt-in/opt-out* (23 883 consultations).

Les professionnels privilégient le canal téléphonique pour les demandes de conseil en amont ou pour la mise en conformité de leurs traitements.

65 490 appels répondus ont été pris en charge par l'accueil téléphonique pour les questions simples (droit d'accès indirect, orientation vers autre administration ou mise en contact avec les services internes) et par les permanences juridiques, générales ou sectorielles (délégués à la protection des données, droit d'accès indirect, santé, plaintes et international).

145 913

appels reçus au 01 53 73 22 22

997 880

consultations de la rubrique questions/réponses (Besoin d'aide)

17 302

requêtes reçues par voie électronique

Rubrique Besoin d'aide (questions/réponses)

Les 5 thématiques les plus consultées en 2019 :
La CNIL c'est quoi ?
Extrait de casier judiciaire
Opt-in, Opt-out
Une donnée à caractère personnel c'est quoi ?
Faut-il déclarer un site web à la CNIL

Les particuliers plus attentifs à leurs droits

Les questions portant sur les droits des personnes (25 % des requêtes traitées) sont plus nombreuses que les questions relatives aux obligations des responsables de traitement (11 % des requêtes) ; elles portent principalement sur le déréférencement, la prospection, la vidéosurveillance au travail et dans les lieux d'habitation, et le droit d'accès indirect.

« Les demandes écrites de particuliers progressent et se concentrent sur 3 secteurs : internet-téléphonie (27 %), commerce/publicité (16 %) et banque/assurance/crédit (15 %)

SENSIBILISER AUX ENJEUX DU QUOTIDIEN NUMÉRIQUE

En 2019, la CNIL a participé à des sessions de formation destinées aux personnels de l'Éducation nationale. Elle a poursuivi ses actions auprès des publics jeunes, par des évènements et de nouvelles ressources pédagogiques.

Un dispositif renforcé de sensibilisation des professionnels de l'éducation

La CNIL a participé aux actions de sensibilisation et de formation des professionnels de l'éducation au RGPD, en présentiel et en ligne : plusieurs interventions ont été organisées à l'Institut des hautes études de l'éducation et de la formation de Poitiers.

La CNIL était une nouvelle fois présente au salon Educatec Educatice, avec un stand pour valoriser ses ressources pédagogiques, répondre aux nombreuses questions posées par les enseignants et autres acteurs de l'éducation. Elle a communiqué sur ses actions d'éducation au numérique en participant à des rencontres organisées dans le cadre du salon et notamment à une table-ronde de l'Association nationale des acteurs de l'École (An@é) sur le thème « Défis et enjeux d'une éducation numérique éthique et responsable ».

Participation de la CNIL à des actions de sensibilisation vers les jeunes publics

Tout au long de l'année, la CNIL a formé des jeunes en service civique de l'association e-Enfance et de la Défenseure des enfants au sujet de la protection des données personnelles et de la vie privée, en s'appuyant sur les pratiques numériques des jeunes. En 2019, ce dispositif a été étendu aux animateurs de l'association Génération Numérique. Les animateurs des clubs de football professionnels et des pôles Espoirs ont suivi, à la CNIL, un atelier interactif sur les réseaux sociaux, déployé ensuite auprès des jeunes joueurs.

La CNIL et le Défenseur des Droits ont participé à EducapCity, une course citoyenne pour sensibiliser les jeunes de 9 à 15 ans aux enjeux de la citoyenneté. Les enfants et adolescents ont testé leurs connaissances en répondant à des questions extraites du quiz *Les Incollables* « Ta vie privée, c'est secret ! ». Une nouvelle version des Incollables a été éditée.

La CNIL a mené différents travaux sur les droits des mineurs à l'ère numérique, en vue de publier sur son site des conseils pratiques destinés à tous les publics en 2020. Elle a participé à la réalisation d'une mallette pédagogique avec le Défenseur des droits, la Hadopi et le CSA, qui sera finalisée et diffusée en 2020.

Le numérique, une affaire de famille

Faisant le constat que les parents se sentent démunis face aux usages numériques de leurs enfants, la CNIL et le collectif Educnum ont organisé en septembre 2019 à Poitiers les **journées Educnum**, un évènement destiné aux familles et aux classes. La création d'un *escape game* sur des cas d'usage tirés du quotidien (objets connectés, réseaux sociaux et jeux vidéo, cyberharcèlement, *fake news*) a permis de sensibiliser parents et enfants aux enjeux soulevés par le numérique, sur un mode ludique et non anxiogène. Les participants sont repartis avec un livret explicitant les concepts du jeu, des ressources et des bonnes pratiques.

En 2020, l'*escape game* sera décliné en une application web pour permettre à chaque acteur de l'éducation et à chaque parent qui le souhaite de tester le jeu en ligne.

Une cohérence et convergence d'actions à l'international

La coopération internationale est restée active dans les domaines de l'éducation et des droits des enfants. La CNIL a poursuivi les échanges d'expériences et de bonnes pratiques entre les autorités au sein du Groupe de travail international qu'elle pilote concernant l'éducation au numérique (représentant soixante-six autorités de protection des données à travers le monde). Elle a relevé nombre d'évènements nationaux qui se sont tenus sous forme d'ateliers, *escape games*, parcours éducatifs, campagnes de sensibilisation et autres concours de classe. À cet effet, la création de nouvelles ressources pédagogiques nationales déclinées par tranches d'âge est venue soutenir les activités des élèves sur des thématiques issues du référentiel international de formation à la protection des données, visant l'acquisition de compétences pour savoir exercer de manière efficace leurs droits et devoirs dans l'univers numérique.

La CNIL a actualisé un état des lieux conduit en 2018 sur les cadres juridiques nationaux concernant l'exercice des droits des mineurs, et orienté plus spécifiquement son enquête internationale de 2019 sur les dispositifs d'information mis en place par les autorités de protection des données et l'existence de mécanismes de plaintes accessibles aux enfants. Un rapport consolidant les réponses fournies sera publié en 2020 et pourra conduire à l'élaboration de recommandations communes.

Par ailleurs, la CNIL a mené une veille active sur les initiatives engagées dans plusieurs pays visant l'élaboration de recommandations pratiques concernant la protection des données des enfants (Royaume-Uni, Irlande, États-Unis). Elle a participé auprès d'instances internationales (Conseil de l'Europe, OCDE) à certains travaux visant à renforcer les cadres de protection des données et le développement des compétences numériques des enfants face aux risques nouveaux dans l'environnement en ligne.

Sous l'égide de la présidence française du Comité des Ministres du Conseil de l'Europe (du 17 mai au 27 novembre 2019), la CNIL a participé à la publication d'un Manuel d'éducation à la citoyenneté numérique (version française provisoire)

Cet outil vient en appui à la Déclaration sur *l'éducation à la citoyenneté à l'ère du numérique* adoptée sous l'impulsion de la présidence française et à la recommandation CM/Rec(2019)10 du Comité des Ministres aux États membres visant à développer et à promouvoir l'éducation à la citoyenneté numérique.

CONSEILLER
les pouvoirs publics et le Parlement

L'année 2019 confirme les liens très intenses avec le Parlement : la CNIL a participé à plus de trente auditions et répondu aux questions techniques posées sous forme de questionnaires préparatoires. Elle a également donné son avis sur plusieurs projets de loi, notamment en matière de santé.

Manon
Juriste au service de la santé, pôle recherche

Notre service, composé de sept juristes, de deux assistantes et d'une chef de service, est chargé de l'accompagnement des acteurs dans le domaine de la santé (organismes publics, promoteurs industriels, établissements de soins, professionnels de santé, étudiants etc.). Il est organisé en deux pôles, « recherche » et « hors recherche ».

Pour rendre la réglementation applicable à ce secteur plus accessible, nous avons publié plusieurs fiches thématiques sur notre site web afin d'aider les professionnels à se mettre en conformité et à déterminer la formalité applicable à leurs traitements de données de santé. Pour des questions plus spécifiques, il est également possible de nous joindre lors de la permanence téléphonique organisée deux fois par semaine, de nous adresser une demande de conseil écrite ou de nous rencontrer lors d'interventions extérieures (colloques, actions de sensibilisation au RGPD, etc.).

L'accompagnement des professionnels se fait aussi lors de l'instruction des demandes d'autorisation « santé » et « recherche » au cours desquelles nous sommes souvent amenés à échanger avec les responsables de traitement. Nous sommes également sollicités dans le cadre de demandes d'avis sur des projets de loi ou des projets d'acte réglementaire.

J'ai participé durant l'année 2019 à l'instruction des demandes d'autorisation « recherche », qui demeurent nombreuses, malgré l'adoption de nouvelles méthodologies de référence en 2018. J'ai tout particulièrement œuvré à l'élaboration de la doctrine en matière de décisions uniques, qui constituent un mécanisme de simplification encore assez méconnu.

L'année 2020 sera l'occasion pour le service de la santé, d'une part, d'approfondir son accompagnement du grand public et des professionnels grâce à la publication de nouvelles fiches thématiques et d'un MOOC consacré à la santé et, d'autre part, de simplifier certaines démarches grâce à la publication de nouveaux référentiels.

LES ACTIVITÉS AU PARLEMENT

Concernant l'activité législative du Parlement, les projets de loi débattus au cours de l'année ont nécessité un recours à l'expertise de la CNIL dans des domaines déterminants pour l'avenir tels que les mobilités, la bioéthique, la création d'une taxe sur les services numériques ou encore la communication audiovisuelle et la souveraineté culturelle à l'ère numérique.

De même, le démarchage téléphonique, la création d'une carte vitale biométrique, ou encore la lutte contre les contenus haineux sur internet sont autant de thèmes majeurs abordés à l'occasion d'auditions devant les rapporteurs de ces propositions de loi.

Concernant la mission générale d'évaluation de la loi dévolue au Parlement, la CNIL a participé aux travaux d'évaluation de la loi relative à l'orientation et à la réussite des étudiants (ORE) au Sénat et, plus particulièrement, du dispositif Parcoursup.

La CNIL a également été entendue à l'Assemblée nationale, dans le cadre du programme de travail de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS), sur le sujet sensible du dossier médical partagé (DMP) et des données numériques de santé.

La CNIL a répondu, dans le cadre des pouvoirs de contrôle du Parlement, à la commission d'enquête du Sénat sur la souveraineté numérique, aux missions d'information de l'Assemblée nationale sur les menstruations, le régime des interdictions de stade et le supportérisme, les actions de groupe ou bien encore les plateformes numériques.

Enfin, les travaux conjoints des deux chambres menés au sein de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) ont conduit la CNIL à participer à une audition publique sur l'intelligence artificielle et la santé ainsi qu'à éclairer la réflexion sur la reconnaissance faciale.

À ces sollicitations viennent s'ajouter les demandes des parlementaires nommés en mission temporaire. En 2019, la CNIL a ainsi rencontré, dans ce cadre : la mission relative aux mesures de protection des entreprises françaises confrontées à des procédures extrajudiciaires ou administratives donnant effet à des législations de portée extraterritoriale ; la mission sur l'identification, l'orientation et le suivi des jeunes soumis à l'obligation de formation ; ou encore la mission sur la fraude aux prestations sociales.

Enfin, la CNIL a accueilli, au mois d'octobre 2019, un groupe de députés au laboratoire d'innovation numérique de la CNIL (LINC). Cette visite leur a permis de prendre connaissance des travaux menés par les experts pour l'accompagnement et le développement de solutions technologiques protectrices de la vie privée ainsi que des activités d'innovation et de prospective de la CNIL.

La préparation des auditions et réponses au Parlement mobilise très régulièrement les services de la CNIL, en raison de l'extrême variété des sujets abordés et des délais parfois assez courts pour tenir compte des contraintes de l'agenda des travaux législatifs.

L'AVIS DE LA CNIL SUR LE PROJET DE LOI BIOÉTHIQUE

Depuis les toutes premières lois de 1994, la CNIL n'avait plus eu l'occasion de se prononcer formellement sur un projet de loi bioéthique, ce qui marque une nouvelle étape dans ces débats situés aux confins du rapport entre l'identité humaine, le numérique et les nouvelles technologies. Sollicitée dans des délais extrêmement restreints au cours de l'été 2019, la CNIL a nourri les réflexions entourant la préparation de la révision de loi relative à la bioéthique dont elle a été saisie pour avis de plusieurs articles. Elle s'est attachée, pour l'essentiel, à vérifier les conditions de la bonne application du cadre juridique Informatique et Libertés aux mesures relatives aux conditions d'accès par les enfants nés de l'assistance médicale à la procréation à leurs origines, à l'usage du traitement algorithmique dans le cadre du soin des patients et à l'examen des caractéristiques génétiques à des fins de recherche scientifique.

S'il n'était bien évidemment pas du ressort de la CNIL de se prononcer sur des options politiques majeures telles que d'arbitrer en faveur d'un droit d'accès inconditionnel à l'identité du donneur ou au contraire en faveur d'un droit subordonné au consentement du donneur, il lui appartenait d'attirer l'attention des pouvoirs publics sur un certain nombre de points de vigilance essentiels.

Assurer les droits des personnes

Dans son avis du 11 juillet 2019[2], la CNIL a fait des observations sur l'information des personnes rappelant qu'il découlait des principes généraux de transparence et de loyauté de la loi Informatique et Libertés et du RGPD que les personnes soient informées des traitements qui seront faits de leurs données de manière intelligible, accessible, claire, non ambiguë.

Au regard du projet de loi, elle a ainsi souligné la nécessité de prévoir pour les donneurs une information particulièrement approfondie, lesquels devront avoir pleinement conscience de ce que leur don s'accompagne par ailleurs d'un consentement à la transmission de leurs données à l'enfant né du don.

Ces principes, en plus de ceux prévus par le code de la santé publique, ont aussi été rappelés s'agissant du recours au traitement algorithmique que prévoit le projet de loi dans le cadre du soin des patients. Il s'agit ici pour le citoyen de « garder la main » sur l'algorithme, comme souligné par la CNIL dans son rapport de 2017 sur les enjeux éthiques des algorithmes et de l'intelligence artificielle.

Cette maîtrise est possible si le patient est clairement informé en amont de ce que le professionnel de santé recourt au traitement algorithmique et dès lors

2 « Délibération n° 2019-097 du 11 juillet 2019 portant avis sur un projet de loi relatif à la bioéthique », CNIL, légifrance.gouv.fr

qu'il est mis en mesure de distinguer, lors de la communication des résultats, ce qui relève de la machine de ce qui relève de l'analyse effectuée par le professionnel de santé.

Prévoir des garanties appropriées

C'est en vertu de ces mêmes principes généraux, qu'en matière de recherche génétique dans le domaine scientifique, la CNIL recommande de développer des solutions adaptées pour rendre l'information individuelle des personnes effective et leur garantir l'exercice du droit d'opposition (en ayant par exemple recours à des dispositifs innovants aménageant une information individuelle initiale renvoyant à un site web détaillant chaque projet au fil de l'eau, etc.). Dans son avis, la CNIL a ainsi insisté sur la nécessité de prévoir des garanties appropriées compte tenu de l'extrême sensibilité des échantillons biologiques et données génétiques qui constituent des sources de données intarissables, dans un contexte de multiplication des bases de données et de banalisation de l'analyse génétique, propice au développement d'un écosystème de plus en plus fertile aux risques de ré-identification.

La question des tests dits « récréatifs »

Enfin, si la CNIL ne s'est pas formellement prononcée sur un éventuel encadrement des tests génétiques récréatifs, dans la mesure où le projet de loi initial qui lui était soumis pour avis ne prévoyait pas de dispositions en ce sens, elle a fait état, lors d'auditions par l'Assemblée nationale et le Sénat, du décalage existant entre l'interdiction juridique en France de commercialiser des tests ADN grand public, et la pratique où l'on observe un recours croissant à ces tests par des dizaines de milliers de français confiant leurs données génétiques à des sociétés privées, situées essentiellement en dehors de l'Union européenne. Ce constat pose, en matière de protection de la vie privée, de nombreuses questions pratiques quant à l'exercice des droits des personnes, mais aussi éthiques quant à l'exploitation de ces données par des industriels, ainsi que leur conservation et leur sécurité. Ces questions sont d'autant plus importantes que ces données ne peuvent, par nature, être anonymisées.

PROJET DE LOI DE FINANCES 2020 ET COLLECTE DES DONNÉES SUR LES PLATEFORMES EN LIGNE : L'AVIS DE LA CNIL

La CNIL s'est prononcée le 12 septembre 2019 sur un article du projet de loi de finances pour 2020 permettant, à titre expérimental, la collecte de données personnelles publiées sur internet par les utilisateurs de plateformes en ligne (réseaux sociaux, plateformes de mise en relation et de partage de contenus) afin de détecter les infractions, considérées comme les plus graves, aux réglementations fiscales et douanières.

Un dispositif inédit

Si la CNIL a reconnu la légitimité de l'objectif poursuivi par le dispositif, à savoir la lutte contre la fraude, elle a souligné son caractère inédit. Dans un contexte d'évolution significative des méthodes de travail des administrations fiscales et douanières, il s'agit de permettre à ces administrations d'améliorer le ciblage des contrôles fiscaux à partir de nouvelles techniques (utilisation d'algorithmes de type « auto-apprenants »), ainsi que d'un volume important de données de toute nature dès lors qu'elles sont librement accessibles sur internet.

Des exigences à la hauteur des enjeux soulevés par le dispositif

La CNIL a relevé que la mise en œuvre du dispositif envisagé était susceptible de porter atteinte aux droits et libertés des personnes concernées notamment au droit au respect de la vie privée et à la liberté d'expression en ligne.

Dans ce contexte, elle a formulé plusieurs réserves de nature à assurer la stricte proportionnalité des données traitées au regard de l'objectif poursuivi et à préserver le délicat équilibre entre cet objectif et le respect des droits et libertés des personnes concernées.

Si la CNIL a relevé que des garanties étaient prévues pour encadrer le dispositif (absence de contrôles automatiques à partir des traitements mis en œuvre, interdiction de mettre en œuvre un dispositif de reconnaissance faciale, etc.), elle a estimé indispensable tant de renforcer certaines de ces garanties que d'en mettre en place de nouvelles.

En particulier, il est apparu indispensable que le périmètre du dispositif soit strictement encadré (en expliquant par exemple ce qu'il faut entendre par données librement accessibles ou en précisant les infractions visées).

Dans ce contexte, la CNIL a estimé que le périmètre des infractions concernées devait être précisément défini et limité aux manquements les plus graves, que la durée de conservation des données collectées soit limitée au strict nécessaire ou encore que les données sans rapport avec l'objet du traitement soient exclues. Au regard des enjeux très particuliers d'un point de vue des libertés de ce dispositif, elle a par ailleurs demandé qu'un bilan de l'expérimentation lui soit adressé de nature à lui permettre d'évaluer, de manière approfondie, le respect des principes Informatique et Libertés ainsi que des droits et libertés des personnes concernées.

Une vigilance qui ne s'arrête pas à l'examen du projet de texte : la CNIL particulièrement attentive aux conditions de mise en œuvre du dispositif

La CNIL a notamment souligné la nécessité d'évaluer de manière approfondie le respect, par les administrations concernées, du principe de proportionnalité et de minimisation des données : seules celles réellement nécessaires à la détection de la fraude doivent être traitées. Elle estime qu'il sera indispensable de s'en assurer à tous les stades : lors de l'élaboration des textes réglementaires d'application, au cours de l'expérimentation, selon des modalités adaptées pendant la phase d'apprentissage de l'algorithme, ainsi qu'à l'issue de celle-ci.

Un dispositif au cœur du débat public : les observations de la CNIL largement suivies par le Parlement

Le caractère très particulier du dispositif a conduit la CNIL à rappeler l'importance de l'intervention du législateur pour apprécier l'opportunité de la création d'un tel traitement de données personnelles et, le cas échéant, pour en fixer les règles au regard des garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques.
L'adoption de plusieurs amendements lors des débats parlementaires a ainsi permis d'introduire des garanties supplémentaires au dispositif : resserrement du champ d'application de l'expérimentation aux activités occultes, aux domiciliations fiscales frauduleuses, à certains manquements sur les alcools, le tabac et des métaux précieux, et à certains délits douaniers, une limitation de la collecte aux contenus « manifestement rendus publics par les utilisateurs des plateformes », une interdiction de la sous-traitance pour le traitement et la conservation des données personnelles ou encore le renforcement des conditions d'habilitation des agents de l'administration fiscale et des douanes.

Un dispositif validé par le Conseil constitutionnel au regard des garanties apportées

Dans une décision du 27 décembre 2019, le Conseil constitutionnel a, pour l'essentiel, conclu que le législateur avait assorti le dispositif de garanties propres à assurer « une conciliation qui n'est pas déséquilibrée » entre le droit au respect de la vie privée et la lutte contre la fraude fiscale et que l'atteinte à l'exercice de la liberté d'expression et de communication est « nécessaire, adaptée et proportionnée aux objectifs poursuivis ». Parmi celles-ci, il est possible de relever que plusieurs garanties avaient elles-mêmes été demandées par la CNIL lors de l'examen du projet de texte (strict respect du principe de proportionnalité, durée de conservation limitée des données, etc.). Le Conseil constitutionnel n'a prononcé au final qu'une censure très partielle, concernant le périmètre des infractions entrant dans le champ de l'expérimentation, qui faisait écho à des observations émises par la CNIL dans son avis.

L'AVIS DE LA CNIL SUR LE PROJET DE LOI RELATIF À L'ORGANISATION ET À LA TRANSFORMATION DU SYSTÈME DE SANTÉ

La CNIL a été saisie en janvier 2019 par le ministère des Solidarités et de la Santé, de certaines dispositions du projet de loi relatif à l'organisation et à la transformation du système de santé. Ce projet fait suite à la stratégie de transformation du système de santé français, définie par le président de la République, en septembre 2018.

Dans son avis rendu le 31 janvier 2019, la CNIL s'est prononcée sur trois changements majeurs :

- la création de la plateforme des données de santé (*« Health Data Hub »* en anglais) et l'élargissement du périmètre du Système national des données de santé (SNDS) ;
- la création d'un espace numérique en santé (ENS) pour tout usager du système de santé, à l'horizon 2022 ;
- le dispositif de télésoin, nouvelle pratique de soins à distance pour les pharmaciens et auxiliaires médicaux.

La loi relative à l'organisation et à la transformation du système de santé (OTSS) a été promulguée le 24 juillet 2019.

La création de la plateforme des données de santé et l'élargissement du périmètre du Système national des données de santé (SNDS)

La loi OTSS donne une assise législative à la plateforme des données de santé (au *« Health Data Hub »*), dont la création avait été annoncée par le président de la République à la suite de la publication du rapport du député Cédric Villani « Donner un sens à l'intelligence artificielle » en mars 2018.

Cette plateforme désigne à la fois la plateforme technologique, qui aura vocation à héberger les projets de recherche utilisant les données du SNDS et à mettre à disposition des chercheurs des bases de données d'intérêt mises dans son catalogue, ainsi que le nouveau groupement d'intérêt public qui remplace l'Institut national des données de santé (INDS).

Le projet de loi, sur lequel la CNIL a été saisi, prévoyait :

- l'intégration des missions actuelles de l'INDS par la nouvelle plateforme qui aurait comme nouveau rôle de « réunir, organiser et mettre à disposition les données du SNDS » ;
- l'élargissement du périmètre du SNDS aux données cliniques issues des dossiers médicaux, des pharmacies d'officine et laboratoires d'analyses médicales et un changement de nature du SNDS se traduisant par une architecture décentralisée permettant la mise à disposition des données aux demandeurs ;
- la possibilité d'apparier des données du SNDS avec des entrepôts de données après autorisation de la CNIL, compte tenu de la suppression de tout encadrement exprès des finalités dans la loi.

Dans son avis, la CNIL a notamment attiré l'attention sur :

- l'importance particulière, en ce domaine, d'un niveau élevé de garantie des droits des personnes, et notamment de parfaite information sur l'usage de leurs données personnelles. Conformément aux observations de la CNIL, les missions de la plateforme ont été complétées par une mission additionnelle d'information des patients et de promotion et de facilitation de leurs droits ;

- le nécessaire respect des principes de limitation et de minimisation de ces données, présentant un caractère extrêmement sensible, dans le contexte du développement des techniques d'intelligence artificielle en santé ;

- les risques inhérents à la concentration éventuelle de données sensibles sur la plateforme technologique, qui nécessiteront la mise en place de mesures de sécurité appropriées.

La création d'un espace numérique en santé (ENS) pour tout usager du système de santé, à l'horizon 2022

La loi OTSS a pour objet de permettre à chaque usager du système de santé de disposer gratuitement, d'ici 2022, d'un espace numérique de santé (ENS) comprenant ses données personnelles de santé et ses données de remboursement de soins et lui permettant également à terme d'accéder à des services et outils de santé numériques (tels que, notamment,l'usage d'une messagerie sécurisée, d'un service de prise de rendez-vous en ligne ou d'un service de « télésoin »). Ces outils et services additionnels pourront être proposés par des acteurs privés externes.

Dans la mesure où cette offre constitue un traitement de données personnelles, la CNIL s'est interrogée sur :

- l'intérêt et la nécessité de permettre l'accès des professionnels de santé à l'ensemble des informations de l'ENS au-delà des informations figurant dans le dossier médical partagé (DMP). Elle a ainsi suggéré que l'accès soit restreint à certains contenus de l'espace numérique et que les modalités selon lesquelles cet accès est permis soient précisées ;

- l'encadrement des croisements de données entre les différents services de l'ENS et sur les conditions d'une portabilité des données sécurisée et a demandé que la nature des informations de l'ENS soit détaillée par le décret en Conseil d'État qui serait pris après avis de la CNIL ;

- l'articulation de cette offre avec le dispositif DMP déjà existant. La CNIL a souligné qu'une confusion pourrait naître dans l'esprit des utilisateurs entre ces différents dispositifs dont les modalités de fonctionnement diffèrent. Elle a ainsi demandé une harmonisation des dispositions s'agissant de la base légale du traitement et a été suivie sur ce point.

En 2020, la CNIL devrait être saisie de plusieurs textes d'application concernant l'ENS.

FOCUS

Le nouveau dispositif de « télésoin »

La loi introduit aux côtés des dispositions relatives à la télémédecine, une nouvelle pratique de soins à distance pour les pharmaciens et auxiliaires médicaux appelée « télésoin ».

Le projet de loi prévoyait que seules les conditions de prise en charge des activités de télésoin seraient fixées par décret. Compte tenu des enjeux importants que soulève l'usage des technologies numériques et dans la mesure où le télésoin constitue un traitement de données à caractère personnel au sens de l'article 4-2 du RGPD, la CNIL a estimé dans son avis que le décret pris pour application du télésoin devrait également porter expressément sur les conditions de mise en œuvre. Son avis a été suivi sur ce point.


ASSEMBLÉE NATIONALE

ACCOMPAGNER
la conformité

L'accompagnement des organismes est l'une des missions fondamentales de la CNIL. Si l'entrée en application du RGPD a mis fin à la plupart des formalités préalables, la CNIL poursuit son engagement via la création de nouveaux outils afin d'accompagner le métier de délégué à la protection des données (DPO).

Justine
Juriste au service des questions sociales et ressources humaines

La mission du service, composé de cinq juristes et d'un chef de service, est d'accompagner les acteurs de la solidarité, du travail, du logement, du sport et de l'agriculture, dans leur mise en conformité et leur appropriation de la réglementation relative à la protection des données à caractère personnel.

Nos activités sont extrêmement variées : élaboration d'outils de conformité (cadres de référence, guides pratiques, foire aux questions, etc.), réponse à des demandes de conseil, organisation de rencontres avec les responsables de traitements, examen des demandes d'avis sur des projets de loi ou de décret, ou encore participation à des conférences et ateliers de sensibilisation au RGPD.

Bien que chaque juriste au sein du service soit en mesure de prendre en charge tout dossier relevant de la compétence du service, chacun dispose d'un secteur de prédilection. De mon côté, j'interviens plus précisément dans le secteur social et médico-social.

À cet égard, un des projets dans lequel j'ai été particulièrement impliquée en 2019 concerne le développement d'un kit d'information « protection des données » à destination des professionnels du secteur social et de la médiation numérique. Cet outil, à vocation pédagogique, a pour objectif de sensibiliser ces professionnels aux principes Informatique et Libertés et leur offrir de bons réflexes lorsqu'ils accompagnent leurs publics dans le cadre de leurs démarches en ligne.

Parmi les projets de l'année 2020 figure notamment la mise à jour des anciennes autorisations uniques relatives à l'accompagnement social et médico-social des personnes vulnérables.

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

Qu'est-ce qu'une analyse d'impact (AIPD) ?

L'analyse d'impact est un outil précieux pour les responsables de traitement puisqu'il permet de construire un traitement respectueux de la réglementation tout en respectant les droits et libertés des personnes concernées.

Le RGPD prévoit qu'un organisme doit, lorsqu'il n'arrive pas à réduire son niveau de risque résiduel de façon satisfaisante, consulter son autorité de contrôle (la CNIL en France) préalablement à la mise en place du traitement. S'il s'avère impossible de réduire suffisamment les risques à l'issue de cette phase d'échanges, alors l'autorité de contrôle peut rendre un avis indiquant que le traitement envisagé constitue une violation du RGPD.

Les responsables de traitements dans le champ de la directive « Police-Justice » doivent transmettre une AIPD à la CNIL lorsqu'il la saisit d'une demande d'avis sur un traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

La liste des traitements pour lesquels il n'est pas nécessaire de réaliser une AIPD

Au mois d'octobre 2019, la CNIL a publié la liste des traitements pour lesquels la réalisation d'une AIPD n'est pas obligatoire. Cette liste vient compléter celle des traitements pour lesquels une analyse est, au contraire, requise, publiée en novembre 2018. La nouvelle liste comporte douze types d'opérations de traitement mais n'est pas exhaustive, dans la mesure où des traitements qui n'y figurent pas peuvent également ne pas nécessiter une AIPD : c'est le cas des traitements qui ne présentent pas de risque élevé pour les droits et libertés des personnes physiques car ils ne répondent à aucun des critères issus des lignes directrices du G29.

Lors de l'adoption de cette liste, la CNIL a rappelé qu'un traitement figurant sur cette liste d'exemption doit tout de même respecter les autres obligations prévues par le RGPD (par exemple en matière de sécurité du traitement).

INFOSPLUS

Une bonne maîtrise de la méthodologie est indispensable pour mener à bien son analyse d'impact

Un tutoriel vidéo a été mis en ligne sur le site web de la CNIL afin d'aider les organismes à appréhender l'utilisation de l'outil PIA publié par la CNIL, qui a été traduit en 18 langues. Il identifie les différents acteurs impliqués dans cet exercice et comprend des explications audiovisuelles sur le fonctionnement de l'outil.

L'ACCOMPAGNEMENT DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Après une année 2018 consacrée à l'accompagnement des délégués à la protection donnée via des ateliers dédiés, l'accent a été mis en 2019 sur la formation du secteur public avec l'organisation de plusieurs ateliers de sensibilisation à l'attention des ministères. Ces journées de mise en situation ont permis aux participants d'échanger entre spécialistes de la protection des données tout en renforçant leur propre savoir-faire.

Le délégué à la protection des données (DPO) ayant un rôle de conseil et de pilotage de la conformité, ce professionnel se place au cœur du RGPD. Au-delà des obligations juridiques, c'est toute une pratique du métier qui se développe et qui permet d'enrichir un écosystème en constante évolution.

Un métier étudié

La CNIL a participé aux travaux menés par la délégation générale à l'emploi et à la formation professionnelle (DGEFP) du ministère du Travail sur une étude permettant de « Comprendre et accompagner les enjeux en termes d'emploi et de compétences des délégués à la protection des données » (voir encadré page 71 du rapport).

Cette dynamique est un des moyens pour la CNIL de veiller au bon développement d'un métier dont l'exercice renvoie, par ailleurs, aux obligations du responsable de traitement ou sous-traitant, qui ont la qualité d'employeur du DPO dans la plupart des cas. Par ce biais, la connaissance des différents écosystèmes métier (formation initiale, profils d'origine, expériences, positionnement, moyens, difficultés, perspectives) et des activités satellites à cette professionnalisation (organismes de formation, expertises des prestataires de services, opérateurs de compétences) peut être régulièrement affinée.

64 900

organismes ont désigné un délégué en 2019

1/3

de ces organismes sont issus du secteur public

21 000

DPO en tant que « personnes physiques », par l'effet des mutualisations entre organisme

42 %

des DPO sont des femmes

900

personnes accueillies à la CNIL lors des ateliers réalisés dans les locaux de la CNIL

4 500

appels reçus à la permanence juridique dédiée aux DPO

Premiers agréments en matière de certification des compétences du DPO

La certification des compétences du DPO repose sur un mécanisme volontaire permettant à tout professionnel, DPO ou non, de justifier qu'il répond aux exigences de compétences et de savoir-faire lui permettant d'assumer les missions assignées aux délégués à la protection des données par le RGPD. Cela constitue un vecteur de confiance à la fois pour l'organisme faisant appel à ces personnes certifiées mais également pour ses usagers, clients, fournisseurs, agents ou salariés. Acteur-clé de la conformité au RGPD, le DPO doit, en effet, disposer de connaissances spécialisées du droit et des pratiques en matière de protection des données.

La loi Informatique et Libertés donne désormais à la CNIL une nouvelle compétence en matière de certification de personnes : la CNIL a, de ce fait, adopté en 2018 deux référentiels en matière de certification des compétences du DPO, qui ont donné lieu à la délivrance des premiers agréments d'organismes de certification en 2019, leur permettant ainsi de faire passer les examens au personnes intéressées.

Pour rappel, la certification n'est pas obligatoire pour exercer le métier de délégué à la protection des données. Inversement, il n'est pas exigé d'être désigné en tant que délégué pour être candidat à la certification des compétences du DPO.

La certification des compétences permet de vérifier les connaissances du candidat sur 3 domaines de compétences (règlementation, responsabilité et sécurité) qui se distinguent des qualités relatives au « savoir-être » du candidat, traditionnellement vérifiées au stade du recrutement.

La CNIL lance sa formation en ligne : l'Atelier RGPD

La CNIL propose depuis de nombreuses années des ateliers dans ses locaux sur différentes thématiques intéressant la protection des données. Depuis l'entrée en application du RGPD, la CNIL a reçu plusieurs milliers de personnes dans ses locaux. En effet, que ce soit une présentation des grands principes et notions clés de la protection des données ou des grands traitements relatifs aux ressources humaines, les évènements proposés par la CNIL nécessitaient néanmoins aux participants de se déplacer à Paris pendant au moins une journée.

Grâce à sa formation en ligne ouverte à tous (MOOC) intitulée « L'atelier RGPD », la CNIL propose aux professionnels, depuis le 11 mars 2019, de découvrir ou mieux appréhender le RGPD. Ce MOOC s'adresse principalement aux délégués à la protection des données, aux futurs délégués et aux professionnels voulant appréhender le RGPD. Il convient aussi bien aux profils techniques que juridiques et peut être suivi par toute personne curieuse de cette matière. Élaboré par les juristes et experts de la CNIL, il est composé de vidéos, de textes, d'illustrations, de cas concrets et propose des quiz et des évaluations. **Il permet ainsi aux professionnels d'initier une mise en conformité de leur organisme et d'aider à la sensibilisation des opérationnels.**

Cet outil de formation **gratuit est accessible à tous.** Une fois son compte créé, **l'utilisateur progresse à son rythme et sans avoir à se déplacer. Une attestation de suivi** est délivrée à tout participant ayant parcouru la totalité des contenus et ayant répondu correctement à 80 % des questions par module.

Forte de ce succès et de retours très positifs des utilisateurs, la CNIL envisage d'enrichir le MOOC de nouveaux modules en lien avec des pratiques sectorielles (par exemple pour les collectivités locales, la santé, le marketing ou les ressources humaines).

+ de 62 000

comptes créés sur le MOOC de la CNIL

15 000

attestations de suivi délivrées

Accompagnement des réseaux de DPO

Le nombre de DPO ayant considérablement augmenté avec le RGPD, la CNIL a dû adapter son accompagnement à ce changement d'échelle. Elle a ainsi souhaité nouer de nouveaux partenariats, en particulier à destination des communes et intercommunalités qui ont engagé la transition numérique de leur action. C'est dans ce contexte qu'une convention de partenariat entre la CNIL et l'association des maires de France (AMF) a été signée en novembre 2019.

Cette convention a pour objectifs :

- **la mise en œuvre du RGPD** et, plus particulièrement, l'accompagnement et la promotion de la mise en place de la fonction de délégué à la protection des données dans les services communaux et intercommunaux ;
- **l'élaboration** d'outils de conformité au RGPD répondant aux besoins spécifiques des communes et intercommunalités ;
- **l'organisation** de campagnes de sensibilisation aux règles de protection des données personnelles, en particulier dans le cadre de la communication à l'occasion des campagnes électorales.

Dans cette veine, la CNIL a procédé aux renouvellements des conventions de partenariats signées avec la conférence des présidents d'université (janvier 2019) et le Conseil national des barreaux (juin 2019).

Par ailleurs, afin d'aider les DPO à créer leur réseau professionnel par secteur d'activités et par zone géographique, la CNIL publie dans un format ouvert et aisément réutilisable *« open data »* la dénomination et les coordonnées professionnelles des organismes ayant désigné un délégué à la protection des données, ainsi que les moyens de contacter ce délégué.

> **« Il est essentiel que les délégués soient associés aux projets dès le stade de la réflexion interne pour être en capacité de guider efficacement les métiers.**

FOCUS

Étude sur le métier de DPO

Les conditions d'exercice, les formes d'emploi, les parcours ou compétences détenues ou attendues pour l'exercice du métier de DPO ont besoin d'être mieux identifiés et compris afin d'apporter les bonnes réponses en termes d'emploi et de formation professionnelle. La CNIL s'est engagée aux côtés de la Délégation générale à l'emploi et à la formation professionnelle (DGEFP, ministère du Travail), de l'Agence nationale pour la formation professionnelle (AFPA) et de l'Association française des délégués à la protection des données à caractère personnel (AFCDP) afin de mieux identifier les dynamiques et les enjeux en termes d'emploi et de formations liées au RGPD. La DGEFP a confié à l'AFPA la réalisation d'une étude de grande ampleur sur le métier de DPO.

Cette enquête en ligne a été réalisée de mars à avril 2019, avec pour objectif de mieux comprendre les conditions d'exercice, les formes d'emploi ou d'activité, les parcours ou compétences détenues ou attendues pour l'exercice du métier de délégué à la protection des données.

Ce sont 1 598 professionnels de la conformité au RGPD qui y ont répondu : 859 DPO internes, 196 DPO internes mutualisés, 210 DPO externes et 333 professionnels en charge de la protection des données personnelles (personnes non désignées auprès de la CNIL tels que les relais Informatique et Libertés, adjoints du DPO, etc.).

Il ressort notamment que :

- les DPO de profils techniques sont les plus nombreux (39 %) ;
- 39,7 % des DPO disposent d'un budget propre ;
- 59 % des DPO estiment que leurs recommandations sont toujours ou souvent écoutées et suivies par le responsable de traitement ;
- 40,3 % des DPO disent être « systématiquement » ou « très souvent » consultés en amont des projets ;
- 73,7 % des DPO recommanderaient « sans hésiter » ou « probablement » leur métier à un jeune ;
- près des ¾ sont satisfaits de leur fonction de DPO ;
- 40,5 % des DPO externes ont moins de deux ans d'expérience. 20,5 % d'entre eux disent avoir plus de dix ans d'expérience dans le domaine ;
- 24,6 % des DPO externes indiquent ne pas maîtriser le sujet (« Plusieurs concepts importants m'échappent encore » et « Je suis encore très loin de maîtriser tous ces textes ») ;
- près de 72 % des DPO disent avoir suivi une formation de un à cinq jours ;
- et 40 % des DPO estiment que la fonction est stressante.

Ces résultats sont particulièrement riches d'enseignements et permettent d'orienter les actions de la CNIL qui encourage les professionnels en charge de la protection des données, DPO ou non, à participer à la prochaine grande enquête qui aura lieu au printemps 2020.

2019 : LA CONCRÉTISATION DE LA STRATÉGIE D'ACCOMPAGNEMENT DE LA CNIL EN MATIÈRE D'OUVERTURE DES DONNÉES PUBLIQUES (« OPEN DATA »)

Le renouvellement du cadre juridique applicable en matière d'ouverture des données publiques par la loi pour une République numérique du 7 octobre 2016 a conduit la CNIL, en partenariat notamment avec la Commission d'accès aux documents administratifs (CADA), à élaborer plusieurs contenus. Cette démarche d'accompagnement visait à répondre tant au besoin de clarification des règles applicables en la matière des administrations diffusant en ligne des données publiques qu'à celui des réutilisateurs de ces données.

L'ouverture des données publiques : des enjeux particuliers pour la protection des données

Dans un contexte de transparence de l'action administrative, de nombreux acteurs se sont engagés dans la mise en ligne des informations qu'ils détiennent. Cette politique s'est notamment traduite par la publication de plateformes dédiées où plusieurs milliers de jeux de données sont aujourd'hui disponibles, faisant de la France l'un des États les plus avancés en termes d'ouverture des données publiques.

Cette mise en ligne, qui vise en particulier à renforcer la transparence de l'action publique et de la vie démocratique tout en permettant de susciter l'innovation économique, doit s'accompagner de garanties afin de préserver la vie privée des personnes dont les données peuvent ainsi être diffusées.

La CNIL rappelle ainsi régulièrement que la publication d'un volume important de données en ligne a naturellement pour conséquence d'augmenter les risques potentiels pour les personnes concernées, et ce, même lorsque les données ne contiennent pas, initialement, de données directement identifiantes (comme le nom ou le prénom). En effet, la publication d'informations comme l'adresse peut permettre, par recoupement avec d'autres informations publiques ou avec d'autres données disponibles sur internet, l'identification ou la ré-identification d'un individu.

Concilier transparence administrative et protection des données personnelles nécessite de trouver un délicat équilibre, ce qui a conduit la CNIL à accompagner spécifiquement les acteurs concernés sur le sujet. Les travaux menés en la matière ont également été l'occasion de rappeler que les objectifs poursuivis par la politique d'ouverture des données publiques, dont la légitimité ne fait aucun doute, demeurent pleinement compatibles avec les grands principes applicables en matière de protection des données.

Le protocole de coopération entre la CNIL et la CADA a été renouvelé en 2019 et a permis de traiter les enjeux suivants :

1

Clarifier les modalités de répartition des demandes des usagers en matière de communication des documents administratifs.

2

Clarifier la répartition des demandes en cas de réutilisation des informations publiques comportant des données personnelles.

3

Améliorer les méthodes de travail pour renforcer les synergies entre les deux institutions dans le traitement de ces demandes.

La publication d'un guide CADA-CNIL dédié à l'*« open data »* : la concrétisation de travaux menés de longue date

La loi pour une République numérique, en renforçant les missions de la CNIL et de la CADA, a conduit à l'élaboration d'un travail entre les deux institutions afin de permettre une meilleure compréhension et appropriation du cadre juridique applicable.

Depuis 2017 et la première réunion du collège unique CADA-CNIL, les échanges se sont poursuivis autour d'un sujet d'intérêt commun : élaborer un guide pratique en matière d'ouverture et de réutilisation des données publiques afin d'accompagner les usagers au niveau local ou national.

Concrètement, ce travail conjoint a permis à la CNIL d'introduire des éléments portant plus spécifiquement sur les droits et obligations applicables en présence de données personnelles ainsi que sur les aspects techniques liés à l'occultation et à l'anonymisation des documents diffusés en ligne.

Au regard des enjeux liés à la question de l'ouverture et de la diffusion des données ainsi que de la préoccupation croissante de la société pour ces sujets, une consultation publique a été menée du 21 février au 4 avril 2019 après qu'un premier projet du guide a été présenté aux membres des collèges de la CADA et de la CNIL.

Cette consultation, qui a recueilli plus de 220 contributions, a permis de simplifier encore davantage le contenu proposé et d'amorcer la rédaction de fiches pratiques afin d'assurer le caractère opérationnel du document.

L'ensemble des documents produits a ainsi permis la publication d'un guide pratique le 17 octobre 2019, qui fournit aux administrations et réutilisateurs de données publiques les principales clés de compréhension du dispositif de l'*« open data »*. Après avoir rappelé les principales définitions à retenir, ce guide s'articule autour des points suivants :

- le rappel des obligations de publication en ligne attachées à certaines données ;
- le contenu des documents publiés ;
- les modalités de diffusion en ligne ;
- la réutilisation des données diffusées.

Vers un outil dynamique

Conçu comme un outil d'aide à visée opérationnelle, le guide pratique ainsi que les fiches qui l'accompagneront ont vocation à faire l'objet d'une actualisation régulière au fil des évolutions légales ou jurisprudentielles. L'année 2020 devrait ainsi être marquée par la publication de nouvelles fiches pratiques répondant à des besoins sectoriels, thématiques ou encore techniques.

De la même manière, cette année sera l'occasion pour la CNIL de continuer à s'investir pleinement dans les réflexions et travaux menés dans le cadre de législations sectorielles liés à ce mouvement d'ouverture, telle que la mise à la disposition du public des décisions de justice.

RENFORCER LA SÉCURITÉ : LA NOTIFICATION DES VIOLATIONS DE DONNÉES PERSONNELLES

Une violation de données personnelles est une action, intentionnelle ou non, portant atteinte à la sécurité des données, c'est-à-dire à la confidentialité, à l'intégrité ou à la disponibilité de ces données.

Les 2 287 notifications de violations de données personnelles reçues en 2019, qui font l'objet d'une instruction individuelle, constituent un baromètre permettant à la CNIL d'appréhender la maturité des organismes, d'évaluer les menaces qui pèsent sur les données personnelles et de veiller à une information appropriée des personnes concernées. Elles complètent l'obligation de sécurité existant depuis 1978.

Les informations issues de ces notifications permettent à la CNIL d'orienter au mieux son action de conseil ainsi que son action répressive et, finalement, mieux jouer son rôle dans l'écosystème de la cybersécurité.

Les notifications de violations de données personnelles en 2019

Le RGPD impose aux responsables de traitement trois niveaux d'obligations :

- d'abord, documenter, en interne, toutes les violations de données personnelles ;
- ensuite, notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL ;
- enfin, lorsque le risque est élevé, notifier la violation aux personnes concernées elles-mêmes, afin qu'elles puissent se protéger des conséquences de la violation.

Les organismes doivent donc mettre en place des mesures visant à :

- prévenir toute violation de données ;
- détecter les éventuelles violations de données ;
- réagir de manière appropriée en cas de violation, c'est-à-dire mettre fin à la violation, minimiser ses effets, notifier la violation à la CNIL et en informer les personnes si nécessaire.

Ces dispositions visent à préserver à la fois :

- les responsables du traitement en les poussant à sécuriser au mieux leurs données pour protéger leur patrimoine informationnel ;
- les individus affectés par la violation : afin d'éviter que celle-ci ne leur cause des dommages ou des préjudices, en leur permettant notamment de prendre les précautions qui s'imposent en cas d'incident.

La très grande majorité des notifications de violations de données reçues en 2019 concernent des atteintes à la confidentialité des données, c'est-à-dire un accès illégitime aux données.

2 287

Notifications de violations de données en 2019

2019, les notifications de violation en chiffres

Nature de la violation	Volume
Perte de la confidentialité[3]	1 760
Perte de la confidentialité et de la disponibilité	136
Perte de la confidentialité et de l'intégrité	91
Perte de la confidentialité, de l'intégrité et de la disponibilité	80
Perte de la disponibilité[4]	153
Perte de l'intégrité[5]	38
Perte de l'intégrité et de la disponibilité	29

Secteur d'activité des organismes	Volume
Administration publique[6] (Code NAF O)	360
Activités spécialisées, scientifiques et techniques (Code NAF M)	328
Activités financières et d'assurance (Code NAF K)	295
Commerce ; réparation d'automobiles et de motocycles (Code NAF G)	219
Information et communication (Code NAF J)	202
Santé humaine et action sociale (Code NAF Q)	174
Industrie manufacturière (Code NAF C)	125
Activités de services administratifs et de soutien (Code NAF N)	113
Autres activités de services (Code NAF S)	109
Transports et entreposage (Code NAF H)	95
Enseignement (Code NAF P)	94
Activités immobilières (Code NAF L)	53
Autre	120

Origine principale déclarée : le piratage arrive toujours en tête en 2019

Dans la continuité de sa démarche initiée en 2018, la CNIL privilégie, dans la plupart des cas, l'accompagnement : l'objectif étant, lorsque cela est pertinent, 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 cas, la CNIL peut toutefois être amenée à réaliser des investigations complémentaires afin de comprendre les circonstances de la violation, son étendue et ainsi d'être en mesure de déterminer quels sont réellement les moyens, techniques ou humains, mis en œuvre au sein de l'organisme ayant trait à la sécurité des données personnelles.

La CNIL utilise également les notifications de violation de données pour recenser les violations les plus courantes, les nouvelles attaques et évaluer la pertinence de ses recommandations en matière de sécurité informatique.

L'objectif est de faire en sorte que le niveau moyen de sécurité augmente chaque année, et ce, le plus rapidement possible au sein des entreprises et administrations françaises.

Deux causes principales transparaissent des notifications reçues par la CNIL : 50 % des violations sont dues à un **acte externe malveillant** et 23 % sont dues à un **acte interne accidentel**.
Parmi ces deux principales causes, émergent également des origines principales :

- au sein des actes externes malveillants, l'origine la plus importante en terme de volume est constituée par les piratages à distance suivis par les vols « physiques » ;
- au sein des actes internes accidentels, l'origine la plus importante en termes de volume est constituée par des données personnelles adressées au mauvais destinataire suivies par la publication non volontaire d'informations.

3 Perte de la confidentialité : les données sont rendues accessibles à une personne non autorisée.
4 Perte de la disponibilité : les données ne sont plus accessibles pendant un certain temps.
5 Perte de l'intégrité : les données sont modifiées illégitimement.
6 La catégorie « Administration publique » inclut les administrations centrales et déconcentrées, les collectivités locales et leurs opérateurs.

L'ACCOMPAGNEMENT DES TPE ET PME

Si les actions de pédagogie et de sensibilisation engagées par la CNIL ont été largement relayées auprès des entreprises, les plus petites d'entre elles peuvent connaître des difficultés à adapter leurs pratiques au RGPD, d'où l'importance de déployer un accompagnement dédié.

Les entreprises de petite taille composent la très grande majorité des entreprises en France[7] : s'appuyer sur les principaux intermédiaires naturels des entreprises pour les sensibiliser à la protection des données personnelles et les accompagner dans leur démarche de conformité au RGPD est donc un impératif.

En 2019, la CNIL a poursuivi son action de sensibilisation auprès des TPE et des PME afin de leur permettre de s'approprier le RGPD de façon opérationnelle et d'harmoniser les actions à mettre en place et les rendre plus transparentes, afin de permettre une plus grande efficacité collective.

En pratique, le déploiement de la stratégie dite « des têtes de réseaux » a consisté à intervenir auprès de plus de 50 fédérations ou associations professionnelles pour les aider et en faire des interlocuteurs de référence pour la CNIL. Les interventions ont aussi eu lieu auprès de certains acteurs institutionnels (pour des sujets particuliers tels que la création d'entreprise, l'export, le financement, etc.), qu'il s'agisse du groupe de la Caisse des dépôts avec BPIfrance, du CEA et sa direction de la recherche technologique, de Business France, etc.

Cette sensibilisation au travers d'interventions en comité directeur, assemblée générale, ou en ateliers de travail a permis la création des guides pratiques, quiz et FAQ élaborés par les professionnels avec le concours de la CNIL, comme l'auto-évaluation RGPD par la Confédération des petites et moyennes entreprises (CPME)[8].

Les réseaux de professionnels proches des TPE et PME qui les accompagnent au quotidien ont aussi été approchés pour relayer et amplifier l'action de la CNIL, tels que les experts comptables, les agences de développement économique ou encore le médiateur des entreprises.

Cette stratégie de la CNIL s'articule naturellement avec celle des politiques publiques mises en œuvre pour aider à la transition numérique des acteurs économiques, tant au plan national (la CNIL est partenaire de l'initiative France Num du ministère de l'Économie et des Finances, visant à aider à la transformation numérique des entreprises) qu'au plan européen.

Si le RGPD est un texte qui s'applique à tous les professionnels, quels que soient leur taille ou le secteur d'activité, les obligations des entreprises sont modulées en fonction de la nature, du contexte, des finalités du traitement et des risques des traitements.

Pour les TPE dont le cœur de métier n'est pas le traitement de données personnelles, les obligations sont en général bien moindres que pour une grosse société. Dans l'immense majorité des cas, les traitements n'étant pas à grande échelle, il n'y aura pas d'analyse d'impact à faire ou de délégué à la protection des données à désigner.

Si les moyens à déployer pour se mettre en conformité ne sont pas très importants, les gains sont, par contre, nombreux (renforcer la confiance entre employeur et salariés, rassurer les clients et les donneurs d'ordre, mieux gérer la structure, créer de la valeur ajoutée, etc.).

La CNIL a une approche pragmatique dans son rôle d'accompagnement des acteurs.

Elle produit :

- des référentiels spécifiques en fonction des activités (gestion client, fournisseurs et salariés) ou des secteurs ;
- des outils spécifiques tels que des modèles simplifiés de registre[9].

> **« Pour les petites structures, l'application du RGPD dépend du niveau de risque.**

INFOSPLUS

Les règles de sécurité applicables aux petites entreprises

Si aucune mesure de sécurité n'est absolue, quelques règles élémentaires doivent être suivies par tous :

- **sécuriser les accès aux locaux ;**
- **mettre à jour antivirus et logiciels ;**
- **verrouiller la session des ordinateurs** en cas d'absence, même de courte durée ;
- **gérer correctement ses mots de passe et les habilitations ;**
- **avoir une procédure de sauvegarde et de récupération des données en cas d'incident** (en faisant, par exemple, des sauvegardes régulières sur un autre disque dur ou en utilisant une solution de ***Cloud*** sécurisée).

7 « Photographie du tissu productif en 2017 », Les entreprises en France, INSEE
8 « Conformité au RGPD : auto-évaluez-vous gratuitement avec EvalRGPD ! », septembre 2019, cpme.fr
9 « Le registre des activités de traitement », cnil.fr

PARTICIPER
à la régulation internationale

L'année 2019 a permis à la CNIL et ses homologues européens de continuer à mettre en œuvre le nouveau modèle de gouvernance et les mécanismes de coopération entre autorités nationales de protection des données, instaurés par le RGPD. Ce nouveau cadre d'action incite les autorités à coopérer en ayant recours à des outils dédiés et vise à assurer une cohérence de leurs positions en vue d'une application harmonisée du RGPD à travers les États membres de l'UE.

Nana
Juriste au service des affaires européennes et internationales

Le service des affaires européennes et internationales est composé de 7 personnes et a pour rôle de conseiller, de développer et de défendre les positions de l'institution sur les sujets ayant une dimension européenne et internationale, en collaboration avec les autres services de la CNIL, au sein de différentes enceintes européennes et internationales.

C'est à ce titre que ma mission consiste plus particulièrement à participer aux activités des sous-groupes thématiques mis en place au sein du Comité européen de la protection des données (CEPD), et à porter les positions de la CNIL dans le cadre de l'élaboration de la doctrine en matière de protection des données, des positions ou avis formels du CEPD. J'ai ainsi été impliquée dans les travaux ayant conduit à l'adoption en 2019 des lignes directrices sur les codes de conduite et à la préparation de l'avis du CEPD sur les clauses types de sous-traitance proposées par l'autorité de protection des données du Danemark.

De plus, j'interviens plus spécifiquement sur les transferts de données personnelles en dehors de l'Union européenne, notamment en instruisant ou en répondant à des demandes de conseil sur la mise en œuvre des différents outils de transfert, en collaborant à la préparation et au suivi de l'évaluation annuelle du dispositif du Privacy Shield qui a donné lieu à l'adoption d'un rapport du CEPD, et en travaillant sur le développement de nouveaux outils de transferts proposés par le RGPD que sont les codes de conduite et la certification.

Je suis par ailleurs impliquée dans le suivi des activités du Conseil de l'Europe en matière de protection de données, menées par le Comité de la Convention 108 sur la protection des données personnelles, au sein duquel la CNIL a assuré jusqu'en 2019 la représentation du réseau international des commissaires à la protection des données.

LA CNIL AU COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

La CNIL joue un rôle moteur au sein du collectif européen en participant activement aux activités du Comité européen de la protection des données. Le CEPD est présidé depuis sa création par la présidente de l'autorité de protection des données autrichienne, Andrea Jelinek. Durant l'année 2019, 11 séances plénières du comité se sont tenues. Ces plénières sont alimentées par les travaux d'une dizaine de groupes d'experts en charge de thématiques spécifiques, auxquels la CNIL participe activement.

À titre d'illustration, le CEPD a été particulièrement actif sur la problématique de l'accès aux preuves électroniques par les autorités publiques étrangères. Il a adopté des avis sur le *Cloud Act*, sur la révision de la Convention de Budapest (sur la cybercriminalité) ou sur le projet de la Commission « E-evidence ».

Il a également élaboré des lignes directrices sur des sujets clés comme le champ d'application territorial du RGPD, la vidéosurveillance, les véhicules connectés, le *privacy by design* ou encore sur les codes de conduite afin de clarifier les procédures et leurs règles de soumission, d'approbation et de publication à la fois au niveau national et européen.

Par ailleurs, le CEPD a publié un avis approuvant l'arrangement administratif encadrant les transferts de données personnelles entre superviseurs financiers européens et leurs homologues non-européens. Le CEPD a, avec la participation de la CNIL, rendu ses trois premiers avis sur des projets de décisions nationales approuvant des règles d'entreprise contraignantes.

En outre, le comité a adopté un avis sur l'interaction entre la directive ePrivacy et le RGPD s'agissant notamment de la compétence, des tâches et du rôle des autorités de protection des données, ainsi que de l' application de ces deux textes.

Pour finir, la CNIL a fait partie de l'équipe chargée d'évaluer avec la Commission européenne, la décision d'adéquation « Bouclier de protection de la vie privée » (*Privacy Shield*) dont le rapport a été adopté par le Comité en novembre 2019.

L'intensification de la coopération européenne sur les cas transfrontiers

Si 2018 avait permis de poser les fondements de ce nouveau cadre d'intervention des autorités, à travers des outils, lignes directrices et procédures internes développées au sein du Comité européen de la protection des données (CEPD), 2019 est l'année où ces mécanismes ont pu être pleinement utilisés par la CNIL et ses homologues européens. Le CEPD est venu compléter ce dispositif cette même année en précisant son règlement intérieur et en développant de nouvelles procédures internes.

La coopération entre autorités s'est ainsi intensifiée, plus particulièrement dans le cadre du mécanisme dit « du guichet unique » mais aussi dans le cadre de la procédure de l'assistance mutuelle ou, plus largement, par une coopération informelle donnant lieu à des échanges réguliers entre les autorités européennes de protection des données. S'agissant du mécanisme du guichet unique, celui-ci permet aux autorités, en présence d'un traitement mis en œuvre par un organisme dans plusieurs États membres, ou en cas d'établissement unique ayant un impact sur les personnes dans plusieurs États membres, de décider ensemble de la mesure à adopter à son encontre. Ce mécanisme fait intervenir l'autorité chef de file, en charge de coordonner la procédure et seule interlocutrice de l'organisme à ce titre.

Dans ce contexte, les communications entre les autorités de protection des données interviennent dans le cadre d'une plateforme informatique de coopération entre autorités de protection des données « IMI », notamment pour la détermination de l'autorité chef de file et des autorités concernées ainsi que pour l'élaboration de projets de décisions.

Le point sur les lignes directrices RGPD au 31 décembre 2019

Champ d'application territorial	Adoption définitive
Codes de conduite	Adoption définitive
Base légale « contrat » pour la fourniture de services en ligne	Adoption définitive
Dispositifs vidéo	Adoption définitive
Protection des données dès conception et par défaut	Consultation
Critères du droit à l'oubli dans les moteurs de recherche	Consultation

807

cas soumis par les autorités sur IMI (un « cas » peut regrouper plusieurs dossiers liés, par ex. des réclamations similaires contre une même entreprise)

205

procédures du guichet unique

79

décisions finales ont été adoptées pour lesquelles la CNIL a été autorité chef de file pour 10 cas et autorité concernée pour 32 autres cas

En interne, la mise en œuvre des mécanismes de coopération a nécessité la mise en place d'une gouvernance adaptée tout en se matérialisant également par des interactions quasi quotidiennes entres les différents services de la CNIL et ceux de ses homologues.

La coopération entre autorités a vocation à s'amplifier pour l'année à venir. Dans cette dynamique, la CNIL et ses homologues continueront à consolider leur expérience et actions de coopération afin de concrétiser les promesses du RGPD en la matière. La CNIL contribuera aussi, sur ces aspects, aux réflexions et travaux de la Commission européenne en vue de dresser le bilan de la mise en œuvre du RGPD et d'identifier les éventuelles pistes d'amélioration dans le cadre d'un rapport attendu en mai 2020.

Une coopération internationale qui évolue et se structure

Lors de sa réunion annuelle à Tirana, en Albanie, le réseau international des commissaires à la protection des données a concrétisé les changements et nouvelles orientations actés l'année précédente sous la présidence, et à l'initiative, de la CNIL. Symbole de cette évolution stratégique, ce réseau qui rassemble désormais plus de 120 autorités à travers le monde change de nom pour devenir l'Assemblée mondiale de la vie privée (*Global Privacy Assembly*). L'organisation a également adopté son nouveau plan stratégique pour 2019-2021, qui vise à établir une véritable stratégie au niveau international en matière d'influence et de politique du numérique.

L'objectif de cette nouvelle stratégie est d'assurer que la voix des autorités de protection des données puisse se faire entendre au mieux dans les grands débats au niveau international sur les questions liées aux données personnelles, à la vie privée ou encore aux nouvelles technologies. Des travaux autour de standards internationaux pour la protection des données personnelles, de la coopération réglementaire et de l'économie numérique sont désormais engagés afin de contribuer aux messages et positions du réseau dans les années à venir.

> **Assurer que la voix des autorités de protection des données puisse se faire entendre au mieux dans les grands débats au niveau international**

La CNIL continue également de participer activement à l'animation et la gouvernance du réseau, en assurant la coprésidence de deux groupes de travail : celui sur l'éducation au numérique ainsi que celui sur l'éthique et la protection des données dans l'intelligence artificielle. Les priorités de ces groupes de travail ont été définies avec l'adoption de programmes pluriannuels et s'articuleront également avec les nouvelles orientations stratégiques de l'Assemblée mondiale.

Au-delà de sa forte implication au sein du réseau international des autorités, la CNIL a également fortement développé ses relations bilatérales avec les autorités de pays tiers, en particulier vis-à-vis d'autorités nouvelles ou en devenir. Une quinzaine de délégations ont ainsi été reçues à Paris en 2019 afin d'échanger sur les thématiques règlementaires communes, les évolutions internationales mais aussi le renforcement des capacités et le soutien aux nouvelles autorités.

Une nouvelle stratégie pour le réseau francophone

Depuis 2007, la CNIL participe activement à l'Association francophone des autorités de protection des données personnelles (AFAPDP), qui rassemble les autorités francophones de protection des données personnelles et les gouvernements intéressés par une telle loi et qui partagent l'usage de la langue française, mais aussi une tradition juridique et des valeurs communes. À la création de l'AFAPDP, 45 pays dans le monde disposaient d'une loi de protection des données personnelles – dont 24 pays francophones. Douze ans plus tard, 67 des 88 États et gouvernements francophones disposent d'une loi et 52 d'entre eux ont mis en place une autorité de protection des données personnelles.

L'AFAPDP constitue un pôle d'expertise et d'échange d'expérience servant d'appui à l'élaboration de textes législatifs nationaux ou d'instruments internationaux en matière de protection des données personnelles. Elle est régulièrement sollicitée pour apporter un soutien juridique, opérationnel et parfois politique aux gouvernements des pays souhaitant se doter d'une loi de protection des données personnelles. En 2019, l'AFAPDP s'est investie dans des activités de plaidoyer en ce sens, auprès des autorités camerounaises et libanaises.

Les membres de l'association se sont réunis en Assemblée générale à Dakar en septembre, à l'occasion de laquelle ils ont adopté une feuille de route ambitieuse pour la période 2020-2025 articulée autour de 3 principaux piliers : la promotion de la protection des données personnelles, le renforcement des capacités de ses membres et le rayonnement de la vision et de l'expertise francophones à l'international. Cette réunion a également été l'occasion d'accueillir le Bureau du Commissaire à l'information de l'île de Jersey, portant à 21 les membres de l'AFAPDP.

Une Conférence des autorités francophones de protection des données personnelles s'est tenue au lendemain de l'Assemblée générale, au cours de laquelle il a été question d'état civil, d'éducation au numérique, d'intégrité numérique et de droit à l'oubli. Les présidents d'autorités ont par ailleurs été reçus par le président de la République du Sénégal, S.E.M. Macky Sall, auprès duquel ils ont plaidé pour une meilleure prise en compte des questions liées à la protection de la vie privée dans les enceintes internationales, notamment francophones.

Audience des autorités francophones de protection des données personnelles
avec S.E.M. Macky Sall, Président de la République du Sénégal
Mercredi 18 septembre 2019
Palais présidentiel, 6 Avenue du Pr. L. Sedar Senghor, Dakar, Sénégal

AFAPDP

PROTÉGER
les citoyens

En cas de plainte, le plus souvent, la CNIL informe le responsable du fichier des faits soulevés par le plaignant afin que, en cas de manquement, il se mette en conformité et respecte les droits des personnes.
L'année 2019, première année pleine d'application du RGPD, a été marquée par un nombre toujours plus élevé de plaintes adressées à la CNIL, par la nécessité d'adapter les moyens d'actions des services de la CNIL à ce flux et par la montée en puissance de la coopération avec les homologues européens.

Dorine
Juriste au service des plaintes

Le pôle « internet, commerce, marketing » du service des plaintes de la CNIL, au sein duquel je travaille, est principalement dédié aux plaintes à l'encontre des acteurs d'internet (réseaux sociaux, moteurs de recherche, éditeurs de sites ou blogs...), de l'e-commerce et des opérateurs de télécommunications. Je m'intéresse en particulier aux problématiques liées aux nouvelles technologies (à l'instar du cloud computing ou des cookies).

Les plaintes portant souvent sur des traitements de données personnelles transfrontaliers, je suis particulièrement concernée par la coopération européenne. J'ai à ce titre eu l'occasion de participer à des échanges avec mes homologues européens pour mettre en place les moyens de cette coopération.

De manière plus générale, je travaille beaucoup en équipe, en échangeant notamment sur les plaintes reçues. Je suis en contact avec différents interlocuteurs (plaignants, responsables de traitement et homologues européens), ce qui me permet d'avoir une vision globale d'un problème. Je peux proposer un contrôle sur une plainte et prendre part aux investigations menées.

Au-delà du traitement de plaintes, je contribue également à la doctrine de l'institution en menant des réflexions sur des problématiques de fond. Cette année, j'ai ainsi participé à différents travaux menés en matière de déréférencement (analyse des arrêts rendus par la CJUE le 24 septembre 2019).

La diversité des missions, les conséquences concrètes des actions sur les situations personnelles et la possibilité d'influer sur les enjeux de la protection des données sont mes sources de motivation quotidienne.

LES PLAINTES

Un nombre record de plaintes

14 137

plaintes reçues en 2019

+ 27 %

par rapport à 2019

5 620 plaintes (+ 64 %) ont fait l'objet d'un traitement rapide de premier niveau. Les personnes reçoivent ainsi des réponses sur :

- leurs droits 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.

Pour exercer ses droits, la personne doit d'abord s'adresser directement à l'organisme concerné, ou à son délégué à la protection des données (DPO) s'il y en a un. Ce n'est qu'en cas de refus ou d'absence de réponse dans un délai d'un mois que la CNIL peut intervenir.

8 517 plaintes (- 8 %) ont nécessité un traitement plus approfondi.

Après un examen de l'objet de la plainte, d'éventuelles vérifications informelles ou demandes de complément d'information auprès du plaignant, le mode d'action le plus approprié est mis en œuvre.

La CNIL peut en effet intervenir, toujours par écrit, auprès du responsable du fichier mis en cause pour :

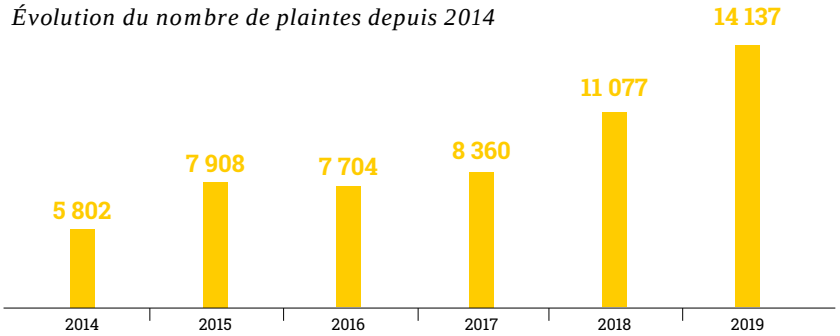
- lui rappeler ses obligations et l'inviter à prendre les mesures nécessaires ;
- investiguer plus précisément les conditions de mise en œuvre de son traitement de données personnelles (par exemple, la durée de conservation des données) et/ou demander des précisions sur la situation individuelle du plaignant ;
- obtenir tout justificatif utile.

Une action répressive plus coordonnée

L'entrée en application du RGPD a conduit à une hausse très forte des plaintes reçues, toujours plus complexes, techniques et médiatisées. Cela conduit la CNIL à redessiner ses pratiques d'intervention auprès des organismes mis en cause afin d'établir une priorité dans les actions et de les mener dans un cadre plus global.

En identifiant l'accumulation de plaintes contre un même acteur, un même secteur ou une même pratique, la CNIL peut procéder à des vérifications approfondies des mesures techniques et organisationnelles mises en place pour se conformer aux règles en matière de protection des données.

Évolution du nombre de plaintes depuis 2014



Au-delà de la situation individuelle des personnes qui saisissent la CNIL, son action peut ainsi avoir des répercussions positives pour l'ensemble des personnes concernées par le traitement de données personnelles en cause.

Pour y parvenir, la CNIL procède à plus de contrôles ayant pour origine des plaintes (42 % des contrôles réalisés en 2019). Des mesures correctrices (rappel à l'ordre, mise en demeure, sanction financière, injonction, etc.) peuvent également être adoptées sur la base de ces plaintes.

FOCUS

Mises en demeure d'établissements scolaires de mettre en conformité la vidéosurveillance

Des plaintes reçues par la CNIL avaient révélé l'existence de dispositifs excessifs et les échanges avec les établissements concernés n'avaient pas permis d'aboutir à une solution satisfaisante au regard de ces principes.

La Présidente de la CNIL leur a adressé, en décembre 2019, des mises en demeure concernant le fonctionnement de leur dispositif de vidéosurveillance. Elle a ainsi rappelé qu'il est tout à fait possible de filmer les accès aux bâtiments (entrées et sorties) et les espaces de circulation, notamment pour veiller à la sécurité des élèves, des agents et des biens et éviter, en particulier, les intrusions malveillantes. Elle a toutefois également rappelé que, sauf circonstances exceptionnelles, un système de vidéosurveillance plaçant des élèves ou des salariés sous surveillance systématique et continue, dans leurs lieux de vie et de travail, est excessif.

Une action sur les irritants du quotidien

Les plaintes apportent un éclairage essentiel sur les problématiques quotidiennes des personnes en lien avec la protection de leurs données personnelles. Elles reflètent 3 préoccupations majeures :

1 - Conserver la maîtrise de ses données et éviter qu'elles soient traitées à son insu

Près d'un tiers des plaintes porte sur la publication de données personnelles (identité, photographies, vidéos, etc.) sur internet (moteurs de recherche, réseaux sociaux, sites personnels, presse en ligne, annuaires, etc.).

Histoire vécue...

MADAME B. se rend compte que ses nom, prénom et photographie sont référencés sur un site de généalogie créé par un parent éloigné. Elle ne réussit pas à obtenir la suppression de ses données personnelles.

La CNIL a alors rappelé au responsable de ce site qu'en collectant et publiant sur internet les données personnelles de nombreuses personnes, il était soumis au RGPD et qu'il avait notamment l'obligation de répondre dans les meilleurs délais aux demandes des personnes.

Après intervention de la CNIL, les données personnelles de Mme B. ne sont plus en ligne.

En 2019, la CNIL a reçu **422 plaintes relatives au déréférencement** (+ 13 %) et a obtenu la résolution des situations dans 98 % des cas transmis aux moteurs de recherche.

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...

MADAME K. se marie et l'évènement fait l'objet d'un article dans la presse locale, illustré par une photographie. Quatre ans après, elle divorce et se remarie. Elle demande donc, sans succès, la suppression des données concernant son premier mariage.

La CNIL a rappelé ses obligations au journal, qui a supprimé le nom et la photographie de M^me^ K. Les moteurs de recherche ont été avertis afin qu'ils ne renvoient plus vers l'ancienne version de l'article.

La maîtrise de ses données personnelles ne se limite toutefois pas au monde numérique.

La surveillance des employés sur leur lieu ou pendant leur temps de travail, par des outils tels que vidéosurveillance, géolocalisation, écoutes téléphoniques, etc. génère toujours de nombreuses plaintes (10,7 % des plaintes reçues en 2019) qui visent des acteurs du secteur privé comme du secteur public.

La vidéosurveillance concentre le plus de plaintes, notamment lorsque les caméras filment les postes de travail en permanence ou les lieux de pause, enregistrent le son ou lorsque les images sont visibles à distance.

Histoire vécue...

MONSIEUR X. travaille dans une société qui contrôle l'accès aux locaux par empreinte digitale. Il indique être mal informé et ne pas comprendre pourquoi ses empreintes digitales sont collectées. Après intervention de la CNIL, la société a spontanément remplacé son dispositif par un contrôle d'accès par badge.

La collecte jugée excessive de données personnelles par des acteurs publics, ou leurs délégataires, conduit également les personnes à saisir la CNIL de plaintes.

Histoire vécue...

MADAME D. demande l'attribution d'un logement social. Sa candidature est acceptée sous condition de fournir au bailleur social un « justificatif Banque de France ».

La CNIL a rappelé au bailleur social que le « justificatif Banque de France » est réservé à l'usage exclusif des banques et des établissements de crédit. Un tel document ne peut pas être exigé par les bailleurs sociaux.

2 - Ne pas être dérangé, être entendu et considéré

Le droit à la tranquillité

Le nombre de plaintes relatives à la réception de prospection est particulièrement important (14,7 % des plaintes). Qu'il s'agisse de prospection commerciale, associative, politique, reçue par voies postale, téléphonique ou électronique, nombreuses sont les personnes qui saisissent la CNIL d'une plainte pour ces motifs.

Les personnes déplorent que leur consentement n'ait pas été recueilli et/ou de ne pas parvenir à faire cesser la réception de publicités. Les publicités par courrier électronique et par SMS génèrent le plus de plaintes.

L'action de la CNIL en 2019 a notamment permis à plusieurs grands groupes annonceurs de s'apercevoir que leur prestataire en charge du « stop SMS » n'effectuait pas correctement leur mission, les conduisant ainsi à rompre leur contrat et à faire appel à un nouveau sous-traitant.

La CNIL travaille enfin avec « Signal Spam » pour identifier les expéditeurs de spam et agir auprès d'eux.

FOCUS

La demande de la pièce d'identité lors de l'exercice des droits Informatique et Libertés

L'exigence systématique par les responsables de traitement d'une copie d'une pièce d'identité lors de l'exercice des droits aura été l'une des questions les plus fréquentes dans l'instruction des plaintes relatives aux droits des personnes en 2019. Ce point a également fait l'objet de nombreux échanges dans le cadre de la coopération européenne avec les autres autorités de protection des données de l'Union.

La CNIL rappelle ainsi qu'une telle demande de justificatif d'identité ne doit être faite qu'en cas de « doutes raisonnables » du responsable de traitement sur l'identité de la personne qui exerce son droit. En effet, pour exercer ses droits, la personne peut justifier de son identité « par tout moyen ». Ainsi, le niveau des vérifications à effectuer peut varier en fonction de la nature de la demande, de la sensibilité des informations communiquées, du contexte dans lequel la demande est faite et des données déjà détenues par le responsable du traitement.

Si une pièce d'identité peut par exemple être demandée en cas de suspicion d'usurpation d'identité ou de piratage de compte, il apparaît disproportionné de l'exiger automatiquement si le demandeur effectue sa démarche dans un espace où il est déjà authentifié (à partir de son compte client) ou lorsque la demande est faite à partir de l'adresse électronique attachée à son compte client.

En revanche, le fait de donner ses nom et prénom associés à une adresse électronique autre que celle connue du responsable de traitement ne lui permet pas d'assurer une sécurité suffisante des données personnelles et doit alors le pousser à demander des éléments complémentaires afin de prouver l'identité de la personne concernée.

3 - La prise en compte de ses droits

De manière générale, le non-respect des droits des personnes est générateur d'un grand nombre de plaintes.

L'exercice de ses droits auprès de son employeur, tant dans le secteur privé que dans le secteur public, génère un nombre élevé de plaintes (près de 400), dans un contexte généralement tendu entre employé et employeur.

La CNIL est également saisie pour des difficultés d'accès à des dossiers personnels (dossier médical, dossier CAF, Pôle emploi, etc.). **Le nombre de plaintes reçues en 2019 a augmenté de 42 % sur l'accès au dossier médical.**

Histoire vécue...

MONSIEUR G., artisan, souscrit des crédits pour développer son activité. Face à des difficultés financières, il ne peut pas honorer des chèques faits à ses fournisseurs et est inscrit au Fichier central des chèques (FCC).

Alors qu'il a mis fin à son activité et a bénéficié d'une procédure de liquidation judiciaire, sa banque ne procède pas à la suppression de son inscription dans ce fichier.

La CNIL a rappelé à la banque que la clôture d'une liquidation judiciaire suspend l'interdiction bancaire relative aux chèques qui aurait été émise avant cette procédure. M. G. n'est désormais plus inscrit au FCC.

À SUIVRE

En appeler aux têtes de réseaux

Fichiers d'incidents de la Banque de France : la CNIL interpelle les établissements de crédits

Les plaintes sur l'inscription par les banques et établissements de crédits de personnes physiques dans les fichiers d'incidents de la Banque de France ont conduit la CNIL à alerter la Fédération bancaire française (FBF) et l'Association des sociétés financières (ASF) sur la nécessité pour leurs membres de prendre des mesures de formation de leur personnel et d'assurer un meilleur contrôle interne du respect des procédures.La CNIL a appelé ce secteur à améliorer ses pratiques afin que les droits des personnes soient correctement respectés dans le cadre des procédures d'inscription dans les fichiers d'incident de la Banque de France.

Droit d'accès au dossier médical : la CNIL en appelle aux ordres professionnels

Devant le nombre de plaintes concernant l'accès au dossier médical, la CNIL a alerté l'ordre national des chirurgiens-dentistes et l'ordre national des médecins sur les difficultés rencontrées par les patients. Ces ordres ont relayé auprès de leurs adhérents, dans leurs magazines spécialisés, sur leur site et sur les réseaux sociaux, la nécessité de mettre en place une procédure garantissant au patient son droit d'accès à ses données personnelles contenues dans son dossier médical.

Enfin, en 2019, la CNIL a encore reçu plus de **400 plaintes concernant l'inscription de personnes dans les fichiers d'incidents de la Banque de France,** notamment le fichier d'incidents de remboursement des crédits aux particuliers (FICP) et le fichier central des chèques (FCC).

Savoir ses données en sécurité

Les défauts de sécurisation des données sont désormais un motif récurrent de plainte auprès de la CNIL : données accessibles sur internet ou communiquées à des tiers, mots de passe transmis en clair ou non suffisamment complexes, etc. Les citoyens sont désormais nombreux à être attentifs aux violations de données et se font régulièrement le relais, en plus des médias, de défauts de sécurité des données. Ces questions sont de plus en plus importantes (+ 100 %) dans le secteur médico-social.

Histoire vécue...

M. P reçoit un courrier électronique de confirmation de sa banque qui contient l'ensemble de ses coordonnées bancaires et informations fiscales et qui indique au client que : « la sécurité de la transmission par mail [n'est] pas garantie et que l'expéditeur ne [peut] être tenu responsable ».

Depuis l'intervention de la CNIL, la banque envoie de telles informations en pièce jointe chiffrée et travaille au déploiement d'un espace client qui permettra d'échanger avec ses clients de manière sécurisée.

Au cœur de la coopération européenne

Lorsque les fichiers concernés sont transfrontaliers au sein de l'Union européenne (c'est le cas lorsque le responsable du fichier est établi dans plusieurs États membres ou qu'il est établi dans un seul mais que son fichier vise des personnes dans plusieurs États), les plaintes sont traitées en coopération par les autorités de protection de données concernées.

Les autorités s'échangent ainsi des plaintes qui peuvent être particulièrement variées :

- provenant d'associations de défense des libertés sur internet, particulièrement complexes et larges dans leur périmètre, généralement à l'encontre des grands acteurs mondiaux de l'internet ;
- provenant de particuliers qui rencontrent des difficultés dans leur vie quotidienne avec des entreprises ou associations opérant sur tout ou partie du territoire européen.

En 2019, 596 dossiers de coopération concernaient des plaintes et la CNIL est « chef de file » sur 54 cas.

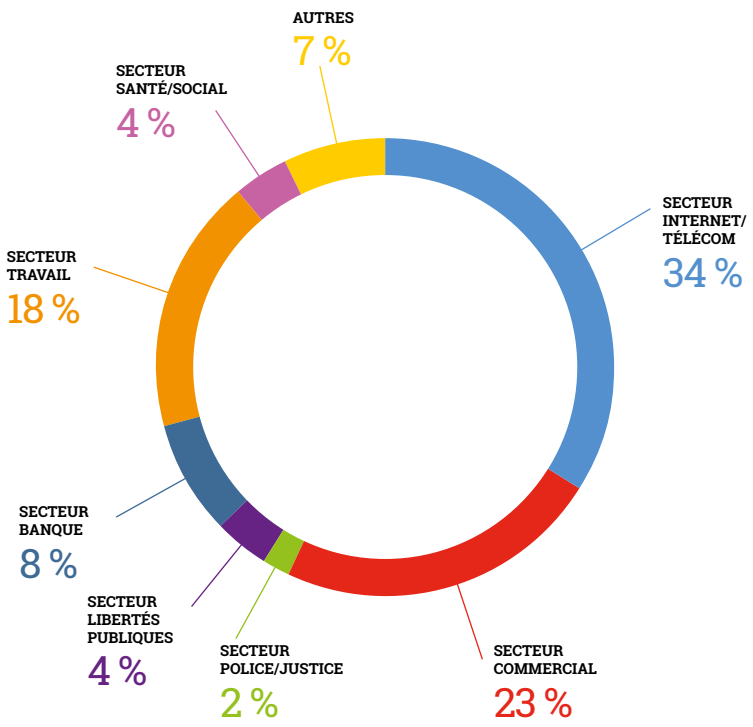
Grâce au mécanisme de coopération prévu par le RGPD et à l'action des autorités européennes de protection des données, près d'une centaine de situations individuelles ayant fait l'objet de plaintes ont été réglées.

Histoire vécue...

MESSIEURS X, B ET U, résidents allemands, ont saisi leur autorité de protection des données en indiquant recevoir de la prospection commerciale d'une société française sans avoir pu s'y opposer préalablement, ni en avoir été informés. Ces plaintes ont été transmises à la CNIL par son homologue.

À la suite de l'intervention de la CNIL, la société a mis en conformité son site web, sur chaque version nationale, en complétant les informations données aux personnes sur le formulaire d'achat en ligne et en insérant une case à cocher pour s'opposer à recevoir de la prospection commerciale.

Répartition des plaintes par secteur d'activité 2019



L'EXERCICE INDIRECT DES DROITS DES PERSONNES, PAR L'INTERMÉDIAIRE DE LA CNIL

FOCUS

Rappel du dispositif

Chaque personne peut, en principe, directement demander à un organisme s'il détient des données la concernant – il s'agit du droit d'accès. Elle peut par ailleurs lui demander de corriger, compléter voire supprimer ces données – il s'agit des droits de rectification et d'effacement.

Pour certains fichiers et dans certaines circonstances cependant, la personne ne doit pas s'adresser à l'organisme mais à la CNIL. La personne exerce alors ses droits par l'intermédiaire de la CNIL.

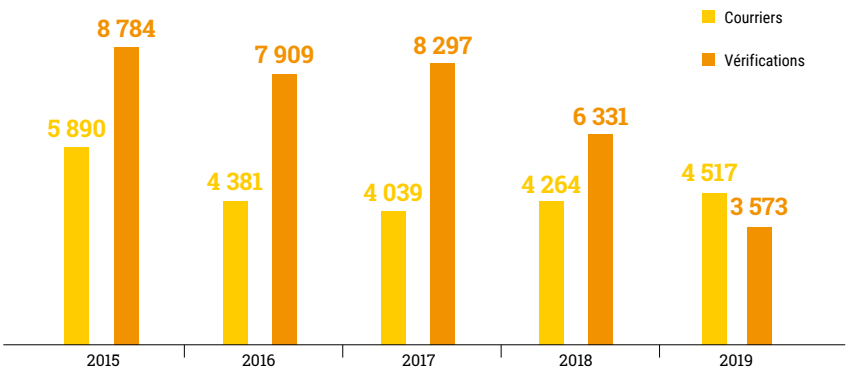
Les fichiers pour lesquels la personne doit s'adresser à la CNIL sont majoritairement mis en œuvre par des personnes publiques dans le cadre de missions régaliennes – sécurités intérieure et extérieure, justice, taxes et impôts, etc.

Une fois la demande reçue par la CNIL, un membre du collège de la CNIL vérifie, avec l'appui des services, que le responsable de traitement respecte effectivement les droits de la personne. Le membre du collège de la CNIL vérifie alors si des données concernant la personne figurent dans le traitement. Il peut également vérifier si ces données sont exactes ou complètes ou encore si leur collecte et leur utilisation sont conformes aux dispositions relatives à la protection des données personnelles.

À l'issue de ces vérifications, la CNIL informe le demandeur de leur résultat. Les dispositions de la loi Informatique et Libertés prévoient des hypothèses dans lesquelles le responsable de fichier peut s'opposer à la communication de toute information. Dans ce cas, la CNIL, comme la loi le prévoit, se borne à informer le demandeur qu'elle a procédé aux vérifications nécessaires.

Activité en 2019 : stabilité du nombre de demandes.

Nombres de courriers reçus et de vérifications effectuées



En 2019, plus de **4 200 personnes ont adressé 4 520 courriers** (sur papier ou électroniques) à la CNIL afin qu'elle intervienne auprès de gestionnaires de fichier pour faire valoir leurs droits. La quantité de telles correspondances est relativement stable par rapport à 2018 (6 %).

Comme les années précédentes, certains de ces courriers mentionnaient plusieurs fichiers. Ainsi, les 4 520 courriers reçus concernaient en réalité à peu près 5 000 demandes d'accès, de rectification ou d'effacement.

Plusieurs de ces demandes ont été adressées à tort à la CNIL. En effet, la CNIL ne peut intervenir que pour une liste limitée de fichiers : elle n'est ainsi pas compétente pour le fichier national des incidents de remboursement des crédits aux particuliers (FICP), pour le fichier central des chèques (FCC) ou encore pour le fichier automatisé des empreintes digitales (FAED).

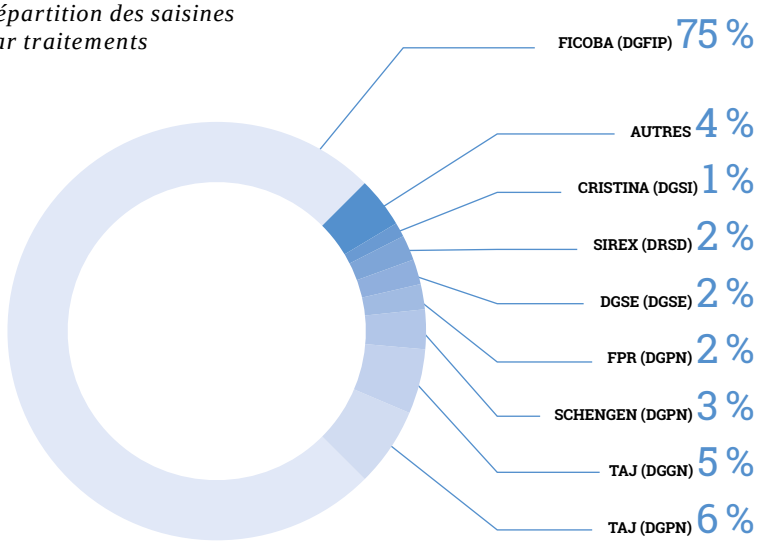
Par ailleurs, pour certains fichiers, les personnes doivent d'abord s'adresser au responsable du traitement ; ce n'est que si ce dernier refuse de répondre favorablement à tout ou partie de leurs demandes, qu'elles peuvent alors saisir la CNIL (voir encadré : les fichiers « Police-Justice » : vous devez adresser votre demande au gestionnaire du fichier). C'est notamment le cas pour le traitement d'antécédents judiciaires (TAJ).

Lorsqu'elle reçoit des demandes qu'elle ne peut pas traiter, la CNIL en informe évidemment la personne.

En 2019, la grande majorité des demandes valablement adressées à la CNIL concernait le fichier des comptes bancaires, ou FICOBA (75 %). Le nombre de demandes relatives à ce traitement a d'ailleurs fortement progressé (+ 40 % entre 2018 et 2019 après une croissance de + 35 % entre 2017 et 2018).

Ces demandes sont souvent motivées par la crainte d'une usurpation d'identité.

Répartition des saisines par traitements



Histoire vécue...

MADAME A. recherchait un logement à louer. En réponse à une annonce en ligne, elle a transmis par courriel divers documents (copie de sa pièce d'identité, des feuilles de salaire, etc.). Sa candidature est restée sans réponse mais elle reçoit depuis son envoi des courriers de diverses banques lui signalant que des prêts ont été contractés en son nom.

Afin de vérifier si des comptes ont été ouverts en son nom par un usurpateur, elle adresse à la CNIL une demande d'accès au FICOBA.

En retour, la CNIL lui adresse la liste de l'ensemble des comptes ouverts et clos en son nom. Cet envoi lui permet d'identifier les comptes inconnus. Grâce à ces informations, elle peut préciser sa plainte et engager des démarches auprès des banques.

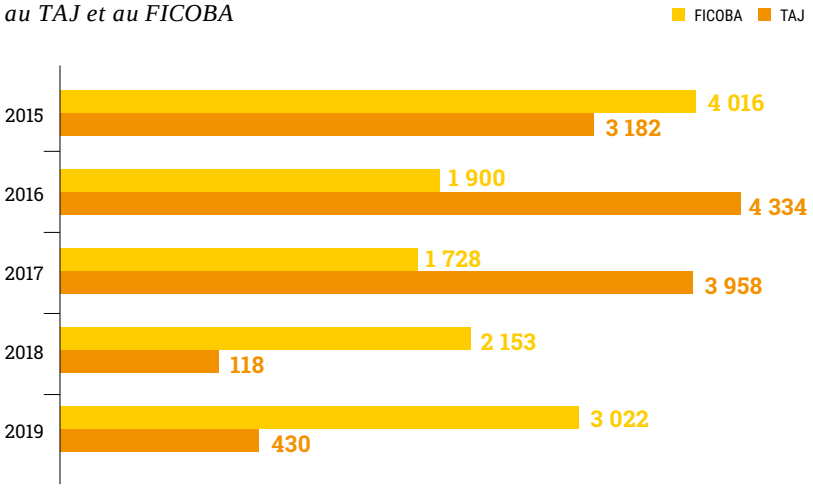
L'accès au FICOBA peut également permettre à certaines personnes de retrouver des comptes ouverts, avec bienveillance, par des proches.

La CNIL a également reçu des demandes relatives au Traitement d'antécédents judiciaires (TAJ). La CNIL ne peut intervenir que si la personne a préalablement saisi le ministère de l'Intérieur. Ce fichier est géré par deux administrations : la direction générale de la police nationale et la direction générale de la gendarmerie nationale. Dans de nombreux cas, la CNIL doit donc se rendre auprès de ces deux administrations pour exercer les droits des personnes.

En 2019, la CNIL a effectué 3 500 vérifications. Au cours de celles-ci, elle a pu contrôler que des données relatives au demandeur figuraient dans le fichier concerné et, si tel était le cas, que ces données étaient exactes, complètes et détenues conformément aux dispositions relatives à la protection des données personnelles.

Ce chiffre connaît une baisse significative depuis 2017. Cette évolution, déjà perceptible au cours de l'exercice précédent[10], tient principalement au fait que la CNIL, depuis l'entrée en vigueur du décret n° 2018-687 du 1er août 2018, ne peut plus être saisie en première ligne de certaines demandes de droit d'accès indirect (celles, pour l'essentiel, relevant du champ de la directive « Police-Justice »). Le demandeur doit d'abord s'adresser directement au gestionnaire du fichier et ce n'est que si celui-ci a préalablement refusé d'accéder à la demande d'accès, de rectification ou de suppression formulée par une personne, que la CNIL peut, dans un second temps, intervenir au titre du droit d'accès indirect.

Saisines relatives au TAJ et au FICOBA



10 Entre 2017 et 2018, le nombre de vérifications avait déjà diminué de 25 %. Ce chiffre restait cependant relativement élevé dans la mesure où la CNIL était compétente pour le TAJ sur les 8 premiers mois de l'année 2018 et a traité un stock important de demandes reçues au cours des exercices précédents (certaines dataient ainsi de 2014).

Histoire vécue...

MONSIEUR C. a effectué une mission auprès d'une entreprise du secteur nucléaire. Son travail jugé satisfaisant, l'entreprise souhaite lui proposer un emploi mais l'informe que son recrutement ne peut se poursuivre en l'état au regard des résultats d'une enquête administrative conduite.

En effet, cette enquête a permis d'identifier que Monsieur C. est inscrit dans le TAJ. L'entreprise invite alors le candidat à régulariser sa situation.

Monsieur C. sollicite le ministère de l'Intérieur afin d'obtenir l'accès et l'effacement des données inscrites dans le TAJ. Il indique alors avoir été mis en cause dans une affaire de violation de domicile : au cours d'une soirée étudiante, il était entré dans le jardin d'un particulier.

Sans réponse du ministère de l'Intérieur dans un délai de deux mois, il adresse sa demande à la CNIL.

Il ressort des vérifications conduites par la CNIL que Monsieur C. figure bel et bien dans le TAJ en tant que mis en cause pour des faits de violation de domicile. Sollicité, le procureur de la République compétent a néanmoins accepté l'effacement de ces données.

Dans ces circonstances, et sous le contrôle de la CNIL, les informations relatives à Monsieur C. ont été supprimées. Elles n'apparaîtront plus si une nouvelle enquête administrative est conduite.

Histoire vécue...

MONSIEUR B. souhaite ouvrir un livret A auprès d'une banque. Cette dernière s'y oppose au motif que Monsieur B dispose déjà d'un livret A dans un autre établissement.

Au cours d'un échange avec ses parents, ceux-ci évoquent un livret qui aurait été ouvert à sa naissance par ses grands-parents.

Monsieur B. adresse à la CNIL une demande d'accès au FICOBA.

En retour, la CNIL lui transmet la liste de ces comptes. Monsieur B. découvre alors qu'il dispose effectivement d'un livret A ouvert en son nom depuis plusieurs années.

À SUIVRE

Les fichiers « Police-Justice » : un an après, une réforme méconnue

UN BREF RAPPEL

Depuis août 2018, les personnes souhaitant effectuer une demande d'accès, de rectification ou de suppression de données personnelles qui seraient contenues dans un fichier lié à la recherche ou à la **prévention des infractions pénales,** ou encore aux enquêtes ou poursuites en matière pénale, doivent **s'adresser au seul responsable de ce fichier**. Il s'agit le plus souvent d'un service du ministère de l'Intérieur ou du ministère de la Justice.

Le service saisi doit alors répondre à votre demande dans le délai fixé par les textes, par exemple deux mois pour le Traitement d'antécédents judiciaires (TAJ). Pour certains fichiers (notamment le TAJ), le gestionnaire de traitement peut refuser de traiter une demande. En cas de refus (explicite ou en cas d'absence de réponse), la CNIL peut intervenir auprès du responsable du fichier.

LES CONSTATS DEPUIS LA RÉFORME

Après plus d'un an de mise en œuvre, il apparaît que le nouveau dispositif est encore mal compris ou mal connu du grand public. Ainsi, de nombreuses personnes s'adressent, à tort, à la CNIL sans avoir préalablement saisi le gestionnaire du fichier.

Quelques adaptations seront nécessaires afin que les responsables de traitement et la CNIL puissent intervenir dans de meilleures conditions. Par exemple, au cours des vérifications conduites par la CNIL, il peut apparaître que la demande initiale n'est pas parvenue au gestionnaire (erreur d'adresse, etc.) ou encore que le responsable de traitement a adressé une réponse après que la personne a saisi la CNIL.

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 grandes problématiques identifiées, des thèmes d'actualité et des plaintes dont la CNIL est saisie. À l'issue des contrôles, la Présidente de la CNIL peut décider, d'abord, de clôturer le dossier, le cas échéant après avoir rappelé à l'organisme ses obligations. Elle peut également prononcer une mise en demeure, susceptible d'être rendue publique. Elle peut, enfin, saisir la formation restreinte de la CNIL. La formation restreinte, composée de 5 membres et d'un Président distinct, peut prononcer diverses sanctions dont des amendes d'un montant maximal de 20 millions d'euros ou 4 % du chiffre d'affaires mondial. Ces sanctions peuvent être rendues publiques.

Maxime
Juriste au service des contrôles « Travail, santé et affaires publiques »

Tony
Auditeur des systèmes d'information au service des contrôles « Affaires économiques »

En pratique, notre travail consiste à conduire des enquêtes pour comprendre dans quel but et de quelle façon les données personnelles sont utilisées. Pour cela, nous effectuons différents types de contrôles : sur place dans les locaux de l'organisme, en ligne depuis les bureaux de la CNIL, sur pièces (examen de documents transmis par l'organisme) ou sur audition (la personne responsable du fichier est convoquée et entendue dans les locaux de la CNIL).

Nous réalisons chacun, sur l'ensemble du territoire français, environ 50 contrôles par an, le plus souvent sur place. Dans ce cas, nous nous rendons auprès de l'organisme et demandons à nous entretenir avec le DPO ou avec un responsable afin de lui présenter le cadre de la mission. L'objectif du contrôle est d'examiner un ou plusieurs traitements de données et d'en faire état dans un procès-verbal qui consigne l'ensemble des informations délivrées et des constats effectués. Nous prenons également copie de pièces au format numérique et papier, par exemple, des contrats, des extraits de base de données ou des documents de procédure internes. Ces éléments permettront par la suite d'évaluer la conformité du ou des traitement(s) et de proposer des orientations à donner (courrier, mise en demeure ou sanction).

Au cours de l'année 2019, nous avons, par exemple, contrôlé des entreprises du secteur de la prospection politique, des collectivités locales sur la thématique de la « Smart City » ainsi que de nombreux sites web présentant des défauts de sécurité pouvant conduire à des violations de données personnelles.

Afin d'assurer un haut niveau d'expertise, nous nous formons régulièrement dans nos secteurs de compétence respectifs, par exemple sur les aspects de sécurité des systèmes d'information.

CONTRÔLER

Au titre de ses missions, la CNIL conduit chaque année un grand nombre d'investigations qui prennent des formes diverses (demandes d'informations dans le cadre de l'instruction de plaintes, ouverture de procédures formelles de contrôle pouvant prendre la forme de contrôles sur place ou en ligne, de demandes de communication de pièces ou encore d'auditions).

Ce sont ainsi au total environ **7 000 actes d'investigation** qui ont été conduits par les services de la CNIL **en 2019**. Ces actes d'investigation sont effectués par différents services de la CNIL, en particulier le service des plaintes, le service des contrôles, le service des sanctions et le service du droit d'accès indirect.

La CNIL a, en particulier, ouvert **300 procédures formelles de contrôle** et a traité 80 signalements relatifs à des violations de données.

Comme chaque année, dans le cadre de ses procédures formelles de contrôle, la CNIL a procédé à des vérifications sur place, en ligne, sur audition ou sur pièces pour s'assurer de la conformité des traitements à la loi Informatique et Libertés et au RGPD. Ces différentes modalités peuvent s'appliquer de façon cumulative à l'égard d'un même organisme (par exemple, contrôle en ligne du site web édité par une société suivie d'un contrôle sur place).

Les plaintes : principale source d'ouverture de procédures formelles de contrôle

En 2019, la stratégie répressive de la CNIL est plus centrée sur les plaintes et les réclamations, qui deviennent les principales sources de contrôles (43 % des vérifications). La CNIL peut effectuer des contrôles de sa propre initiative, afin de réaliser en urgence des investigations et répondre à des sujets d'actualité ou à des inquiétudes liées à la mise en œuvre de nouveaux traitements. La CNIL contrôle également des organismes ayant fait l'objet de mesures correctrices afin de s'assurer que les mesures correctrices annoncées ont permis une mise en conformité du ou des traitement(s) de données. Enfin, comme les années précédentes, un quart des investigations porte sur les thématiques prioritaires identifiées pour l'année.

INFOSPLUS

L'origine des contrôles

43 %
s'inscrivent dans le cadre de l'instruction de plaintes ou de signalements.

31 %
sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité.

21 %
résultent des thématiques prioritaires annuelles décidées par la CNIL.

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

Les violations de données personnelles

À ces contrôles s'ajoutent désormais les vérifications effectuées lorsque la CNIL reçoit des signalements de violations de données personnelles dès lors que des données sont toujours accessibles sans mesure de protection, sur internet. Ces vérifications (80 en 2019), permettent à la CNIL de réagir dans un délai très court afin de faire cesser ces violations. Ainsi, après avoir procédé à la constatation de la violation, un appel téléphonique est effectué dans les quelques heures qui suivent le signalement. Dans la très grande majorité des cas, l'appel téléphonique au responsable de traitement conduit à stopper la violation de données personnelles.

300
PROCÉDURES FORMELLES DE CONTRÔLE

DONT :

53
CONTRÔLES EN LIGNE

45
CONTRÔLES SUR PIÈCES

10
CONTRÔLES SUR LA VIDÉOPROTECTION

AUXQUELS S'AJOUTENT

80
SIGNALEMENTS RELATIFS À DES VIOLATIONS DE DONNÉES PERSONNELLES

L'année 2019 a également été marquée par un accroissement des dossiers traités en coopération avec d'autres autorités. La CNIL a, en effet, contrôlé plusieurs traitements transfrontaliers nécessitant de se concerter avec ses homologues européens : soit en leur transmettant le dossier lorsque la CNIL n'est pas l'autorité de contrôle chef de file, soit en recueillant leurs avis sur les projets de décision de clôture, de mise en demeure ou de sanction. Ces procédures arriveront à leur terme en 2020.

La CNIL a également répondu à des demandes d'assistance mutuelle d'autorités de protection des données européennes en réalisant des contrôles depuis le territoire français afin de compléter leurs investigations.

Bilan du programme 2019

Le respect du droit des personnes

En 2018, environ 20 % des plaintes reçues par la CNIL concernaient l'exercice d'un droit. La CNIL a donc souhaité contrôler, en 2019, une vingtaine d'acteurs appartenant aux secteurs suscitant le plus ce type de réclamations (assurances, banques, recouvrement de créances, grande distribution, commerce en ligne, sites de rencontre, ministère, etc.)

Il a été constaté que l'information fournie aux personnes est souvent incomplète (en particulier du fait de l'absence d'information concernant les bases légales et les durées de conservation), difficilement accessible ou inintelligible.

Les bonnes pratiques

La délégation a néanmoins constaté que les organismes contrôlés ont, pour la plupart, bien pris en compte l'exigence de respecter les droits des personnes.

À cet égard, certaines bonnes pratiques doivent être soulignées :

- l'élaboration, par exemple, de réponses types à destination du service client pour gérer l'exercice des droits des personnes ;
- l'utilisation d'une adresse électronique dédiée par un service unique ;
- le traçage des demandes d'exercice des droits dans un outil spécifique.

Certaines modalités permettant de faciliter l'exercice des droits en ligne ont également pu être constatées. Il s'agit par exemple de la possibilité pour les personnes de télécharger elles-mêmes leurs données à partir de leur compte en ligne (exercice du droit d'accès et du droit à la portabilité).

Les mauvaises pratiques

À l'inverse, la délégation a pu constater certaines mauvaises pratiques récurrentes telles que :

- des délais excessifs pour répondre aux demandes d'exercice de droits ;
- l'absence de lien de désabonnement dans les courriels de prospection commerciale ;
- le fait qu'un client ne puisse pas supprimer son compte en ligne par lui-même.

Des suites répressives (rappels à l'ordre, mises en demeure ou sanctions) ont été données à certains de ces dossiers.

Répartition des responsabilités entre responsables de traitement et sous-traitants

En 2019, les services de contrôle ont souhaité porter une attention particulière aux conditions dans lesquelles un prestataire traite des données personnelles pour le compte d'un responsable de traitement. Des contrôles ont donc été effectués, sur cette thématique, auprès de 15 organismes, fournisseurs de services et solutions informatiques en ligne à destination d'organismes publics ou privés, de la TPE à la multinationale.

Il ressort des éléments constatés que :

- les sous-traitants ont dans l'ensemble bien pris conscience de l'évolution du cadre légal concernant leur activité. La majorité d'entre eux ont encadré leurs prestations par des clauses respectant les termes de l'article 28 précité ;
- les vérifications ont également mis en évidence de bonnes pratiques de la part de certains de ces acteurs, par exemple la mise à disposition de leurs clients de modèles d'information des personnes, de clauses contractuelles types ou d'outils permettant d'assurer l'exercice des droits des personnes (liens de désinscription automatique, outils de suivi des demandes des utilisateurs, boîtes mail de contact unique).

Toutefois, ces vérifications ont également révélé que certains acteurs pensent à tort ne pas être soumis au RGPD et ne pas devoir être qualifiés de sous-traitants. C'est notamment le cas lorsqu'ils réalisent une prestation de maintenance pour laquelle l'accès aux données à caractère personnel reste ponctuel et n'est qu'une conséquence « fortuite » de la prestation. La CNIL a donc décidé de renforcer sa démarche pédagogique pour sensibiliser les professionnels sur ces questions.

FOCUS

Le traitement des données des mineurs

La CNIL a souhaité s'assurer du respect des droits des mineurs, particulièrement vulnérables, en effectuant des contrôles auprès d'une dizaine d'organismes intervenant dans une multitude de secteurs : applications mobiles de révision et de soutien scolaire, outils de gestion de la vie scolaire ou dispositifs de vidéosurveillance dans les écoles. Un objet connecté à destination des enfants ainsi qu'un site de rencontre dédié aux 15-25 ans ont également fait l'objet d'investigations.

Les contrôles réalisés ont permis de constater que, d'une manière générale, les mineurs ne bénéficient pas d'une protection satisfaisante. En effet, des manquements aux principes essentiels de la protection des données, portant sur l'information des personnes, les durées de conservation et la sécurité des données, ont pu être relevés.

Par ailleurs, certains organismes contrôlés ne mettent pas en œuvre de garanties techniques ou organisationnelles suffisantes vis-à-vis des données particulièrement sensibles collectées, qu'il s'agisse des données des mineurs eux-mêmes ou des données, notamment bancaires, de leurs parents. Il a par ailleurs été constaté, que bien souvent, les organismes traitant des données de mineurs ne s'interrogent pas sur la nécessité de réaliser une analyse d'impact relative à la protection des données alors que le fait de traiter des données de mineurs est un critère à prendre en compte pour conduire une telle analyse.

Il a également été constaté que le principe de recueil d'un consentement conjoint du titulaire de l'autorité légale et du mineur de 15 ans (et moins) est mal pris en compte par les organismes proposant des services en ligne fondés sur le consentement de la personne.

Les investigations sont toujours en cours.

Aspiration de données/ démarchage téléphonique

FOCUS

Plusieurs plaintes ont été déposées auprès de la CNIL pour dénoncer les pratiques de sociétés récupérant de façon automatique des données personnelles disponibles à partir de sources publiquement accessibles sur internet afin d'effectuer de la prospection commerciale. Il s'agit par exemple de sociétés collectant et réutilisant les coordonnées téléphoniques des personnes figurant sur des annonces diffusées sur un site web ou des annuaires en ligne afin de les prospecter, alors même que les personnes concernées avaient indiqué s'opposer au démarchage commercial.

Or, une donnée, bien que publiquement accessible, reste une donnée personnelle. Dès lors, elle n'est pas librement utilisable par tout responsable de traitement à l'insu de la personne concernée. Son utilisation doit se faire dans le respect des règles fixées par le RGPD.

En 2019, la CNIL a donc diligenté plusieurs contrôles qui ont conduit à constater les manquements suivants :

- l'absence d'information des personnes démarchées au titre de l'article 14 du RGPD et, en particulier, sur la source d'où proviennent les données ;
- l'absence de recueil du consentement des personnes démarchées par les sociétés avant de leur adresser par message électronique ou automate d'appel une prospection directe concernant ses produits ou services ;
- l'absence de prise en compte du droit d'opposition des personnes (absence de procédure permettant de s'assurer efficacement que les personnes ne soient pas contactées après s'être opposées au démarchage téléphonique sur la liste anti-prospection d'un opérateur téléphonique, auprès du dispositif BLOCTEL ou de la société).

Ces contrôles illustrent l'attention particulière que porte la CNIL quant au respect des droits des personnes, y compris dans le contexte des pratiques de démarchage téléphonique qui sont une préoccupation du quotidien des citoyens.

Des suites répressives (rappels à l'ordre, mises en demeure ou sanctions) ont été données à certains de ces dossiers.

La prévention de la délinquance par les mairies

FOCUS

Une série de contrôles menée auprès de communes a permis de mettre en évidence la récurrence de certains manquements (collecte systématique de données sensibles ou relatives à des infractions, condamnations et mesures de sûreté, l'utilisation d'un champ de texte libre « motif du signalement », conservation des fiches individuelles ou collectives de suivi sans limites de temps, absence d'information des personnes concernées du traitement de leurs données, défaut de sécurité pour l'accès aux données).

Ces contrôles ont débouché sur une communication, publiée en janvier 2020, visant à rappeler aux mairies les bonnes pratiques à adopter, au regard des mauvaises pratiques ayant pu être constatées sur le terrain.

À la suite de ces contrôles, une des communes concernées a été mise en demeure de mettre en conformité ses traitements, notamment sur l'accès par des tiers non autorisés aux données d'infraction.

Enfin, ce programme annuel a été l'occasion de nourrir les réflexions d'un groupe de travail interne permettant d'établir une grille d'analyse concernant la conformité des clauses encadrant la relation de sous-traitance au regard de l'article 28 du RGPD.

Bilan des actions coordonnées au niveau français et européen

Consolidation de la coopération européenne en matière de contrôle

Depuis 2019, les équipes de contrôleurs sont de plus en plus souvent confrontées à des vérifications portant sur des traitements transfrontaliers, ce qui impose de respecter le mécanisme du guichet unique et de notifier les décisions prises (mise en demeure, délibération de la formation restreinte) aux autres autorités concernées.

Ainsi, durant l'année écoulée, 35 contrôles ont porté sur des traitements transfrontaliers, soit plus de 20 % des missions menées par le service des contrôles. Il s'agit principalement de traitements concernant les clients et prospects de sociétés de e-commerce proposant leurs produits et services

INFOSPLUS

Le guichet unique

Le guichet unique est une nouvelle procédure mise en place par le RGPD. Il permet aux entreprises établies dans l'Union européenne d'avoir un seul interlocuteur (l'autorité chef de file) parmi les autorités de protection des données de l'UE. Il a vocation à harmoniser au niveau européen les décisions des autorités de protection des données concernant les traitements transfrontaliers. Ces autorités (l'autorité chef de file et les autres autorités dites « concernées ») doivent désormais se coordonner sur l'ensemble de ces décisions.

dans plusieurs pays de l'Union européenne ou de traitements mis en œuvre par les gros acteurs du numérique. Cela a conduit des contrôleurs à se rendre dans un autre État membre de l'Union européenne à plusieurs reprises pour mener des vérifications avec les autres autorités de protection de données.

De même, la CNIL participe activement aux sous-groupes du CEPD relatifs à la coopération et à l'action répressive afin de contribuer à l'élaboration de la stratégie européenne d'investigation et d'échanger sur des procédures en cours.

Les partenariats de la CNIL

Afin d'être au plus proche des préoccupations des citoyens et cibler ce qui, au quotidien, les irritent le plus, la CNIL coopère avec plusieurs autres autorités. En janvier 2019, elle a signé un nouveau protocole de coopération avec la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) afin de renforcer leur collaboration et de l'adapter aux nouveaux enjeux numériques. La CNIL a ainsi conduit plusieurs contrôles cette année à la suite des signalements de la DGCCRF.

De même, la CNIL dispose également d'un partenariat avec l'association Signal Spam, qu'elle a rencontré à plusieurs occasions en 2019, pour l'aider à cibler les plus gros acteurs du pourriel en France. Des agents de la CNIL se rendent ainsi régulièrement aux assemblées générales de l'association pour connaître les nouvelles méthodes utilisées par ceux qui envoient des pourriels et les meilleurs moyens de les identifier.

Enfin, le service des contrôles échange également régulièrement avec les directions régionales des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (DIRECCTE) afin de faciliter le traitement de signalements provenant de l'inspection du travail en cas d'atteinte aux droits Informatique et Libertés des salariés.

« La formation restreinte peut prononcer plusieurs mesures correctrices dans une même délibération comme, par exemple, une amende administrative et une injonction avec astreinte.

SANCTIONNER

Les sanctions

En 2019, la formation restreinte a prononcé 8 sanctions, dont 5 publiques, ainsi que 2 délibérations aboutissant à un non-lieu. Ces sanctions se composent de 7 amendes administratives d'un montant total de 51 370 000 euros et 5 injonctions sous astreinte allant de 200 euros à 3 000 euros par jour de retard. Une même délibération peut prononcer plusieurs mesures correctrices.

Cette année, 5 amendes administratives prononcées par la formation restreinte concernaient notamment des atteintes à la sécurité des données personnelles. Par ailleurs, 5 délibérations de sanction ont souligné un manquement à l'obliga-

Date	Nom ou type d'organisme	Manquements principaux / Thème	Décision adoptée
21/01/2019	Moteur de recherche	Manque de transparence, information insatisfaisante et absence de consentement valable	Sanction pécuniaire de 50 000 000 euros
31/01/2019	Moteur de recherche	Déréférencement	Abandon des poursuites
31/01/2019	Société de gestion immobilière	Sécurité et durées de conservation des données personnelles	Abandon des poursuites
31/01/2019	Établissement public national à caractère administratif	Défaut de sécurité des données personnelles	Injonctions sous astreintes
28/05/2019	Société de gestion immobilière	Défaut de sécurité des données personnelles et non-respect des durées de conservation	Sanction pécuniaire de 400 000 euros
13/06/2019	Société de traduction de documents	Données non adéquates et excessives, non pertinence, information insatisfaisante, défaut de sécurité des données personnelles Vidéosurveillance	Sanction pécuniaire de 20 000 euros et injonction sous astreinte
18/07/2019	Société intermédiaire en assurance	Défaut de sécurité des données personnelles	Sanction pécuniaire de 180 000 euros
10/10/2019	Société de photographies liées à la petite enfance	Non-respect du droit d'accès, non-respect du droit à l'effacement, défaut de sécurité et de confidentialité des données	Sanction pécuniaire et injonction sous astreinte
21/11/2019	Société d'installation d'équipements d'isolation	Non adéquation, non pertinence et caractère excessif des données, défaut d'information des personnes, non-respect du droit d'opposition, non coopération avec l'autorité de contrôle, transfert non encadré de données hors de l'UE	Sanction pécuniaire de 500 000 euros et injonction sous astreinte
30/12/2019	Société d'aide à domicile des personnes âgées et handicapées	Manquement au principe de limitation de la durée de conservation, défaut d'information des personnes, manquement à l'obligation d'assurer la sécurité des données traitées par un sous-traitant	Sanction pécuniaire et injonction sous astreinte

tion d'information à destination des personnes concernées, 2 un manquement aux durées de conservation et, pour la première fois, la formation restreinte a eu à se prononcer sur le non-respect du droit d'accès prévu par le RGPD.

Par ailleurs, en 2019 les recours contentieux devant le Conseil d'État ont fortement augmenté. En 2018, 16 recours avaient été enregistrés. Cette année, ce sont 27 recours devant le Conseil d'État et 30 mémoires qui ont été rédigés par le service des sanctions.

Les mises en demeure

La Présidente de la CNIL a, pour sa part, prononcé 42 mises en demeure, dont 2 ont été rendues publiques en raison de la caractéristique des manquements retenus qui ont une incidence particulièrement importante sur la vie privée et la liberté individuelle des personnes concernées (dans le domaine de la vidéosurveillance et sur les données collectées lors du déplacement en véhicule des personnes).

L'année 2019 a été marquée par la mise en œuvre de mesures correctrices issues du RGPD et de la loi Informatique et Libertés dans sa version consolidée. Ainsi, 54 mesures correctrices, au total, ont été prises par la CNIL.

Les 42 mises en demeure font suite à :

- l'instruction de plaintes (52 %) ;
- la réalisation de contrôles sur le fondement de plaintes (17 %) ;
- 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 (31 %).

L'année 2019 montre une tendance inversée par rapport à 2018 s'agissant de l'origine des mises en demeure puisque celles-ci ont dorénavant comme source principale les plaintes que reçoit la CNIL. Les mises en demeure ont d'ailleurs, pour plus de la moitié d'entre elles, porté sur les droits des personnes : demandes de déréférencement et droit d'opposition, non réponse à des demandes de droit d'accès. À cela s'ajoute 7 mises en demeure qui sont intervenues en matière de vidéosurveillance sur le lieu de travail et dans les écoles.

L'année 2019 est donc marquée par une plus grande prise en compte des droits des personnes.

La Présidente a également eu recours à une nouvelle mesure correctrice issue du RGPD : l'avertissement. La Présidente peut ainsi avertir un responsable de traitement ou un sous-traitant lorsque les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement. Cette mesure correctrice a donc une finalité préventive puisqu'elle intervient avant que le traitement ne soit mis en œuvre.

42
MISES EN DEMEURE

DONT :

2
PUBLIQUES

2
RAPPELS À L'ORDRE

2
AVERTISSEMENTS

INFOSPLUS

L'injonction sous astreinte

Le pouvoir d'injonction avec astreinte, nouveau pouvoir de la formation restreinte issu du RGPD, a été largement utilisé et a montré son efficacité. La formation restreinte peut, lorsqu'un responsable de traitement ou un sous-traitant ne respecte pas le RGPD ou la loi Informatique et Libertés, prononcer une injonction de mettre en conformité le traitement ou de satisfaire aux demandes d'exercice des droits des personnes. Cette injonction peut être assortie d'une astreinte, sauf dans les cas où le traitement est mis en œuvre par l'État. Son montant ne peut excéder 100 000 euros par jour de retard à compter de la date fixée par la formation restreinte.

L'injonction est utilisée lorsqu'un manquement est constitué mais que le responsable de traitement ou le sous-traitant ne s'est pas mis en conformité au jour où la formation restreinte se prononce. Cette mesure correctrice permet ainsi d'atteindre la mise en conformité dans un délai contraint puisqu'une fois ce délai dépassé, une astreinte commence à courir jusqu'à ce que le responsable de traitement ou le sous-traitant se soit mis en conformité.

L'organisme doit alors fournir, dans le délai fixé par la délibération de sanction, les justificatifs permettant d'établir qu'il s'est mis en conformité. Si les documents n'établissent pas de la mise en conformité et que le délai est expiré, alors l'astreinte fixée par la formation restreinte court. La formation restreinte se réunit afin de voir si l'organisme s'est mis en conformité et procéder le cas échéant, s'il ne s'est pas conformé à l'injonction, à la liquidation de l'astreinte (c'est-à-dire décide qu'il y aura lieu de payer l'astreinte en fonction du nombre de jours de retard).

En 2019, les organismes qui ont fait l'objet d'une injonction avec astreinte se sont tous mis en conformité dans les délais fixés par la formation restreinte.

INFOSPLUS

Les droits des personnes face au démarchage téléphonique

Une société spécialisée dans l'isolation thermique des particuliers utilisait les services de centres d'appel situés en dehors de l'Union européenne pour réaliser des campagnes de prospection téléphonique. Un plaignant avait indiqué à la CNIL qu'il recevait de très nombreux appels de cette société alors qu'il avait demandé à ne plus être contacté.
Des agents de la CNIL se sont donc rendus au siège de la société pour procéder à un contrôle sur place. Lors de ce contrôle, il est apparu que plusieurs personnes avaient fait l'objet d'un démarchage téléphonique malgré leur opposition.

D'autres manquements ont également été relevés. Des commentaires insultants ou faisant état de l'état de santé des personnes ont été trouvés dans les fichiers de la société. Il est également apparu que les personnes n'étaient pas correctement informées et que leurs données étaient transférées hors de l'Union européenne sans que ces transferts soient protégés par des clauses spécifiques dans les contrats passés entre la société et ses sous-traitants.

À l'issue de ce contrôle, la CNIL a demandé la communication d'un certain nombre de documents. Si la société a partiellement répondu, l'ensemble des documents demandés n'a pas été communiqué malgré plusieurs prorogations du délai imparti.

Au regard des manquements constatés, une mise en demeure a été notifiée à cette société, exigeant la mise en conformité des traitements dans un délai de deux mois. Cette durée a été prolongée de deux mois sur demande de la société.

Les mesures attendues n'ayant pas été prises par cette société, la Présidente de la CNIL a décidé de désigner un rapporteur pour qu'une procédure de sanction soit engagée à son encontre.

Le 21 novembre 2019, la formation restreinte de la CNIL a prononcé une amende administrative d'un montant de 500 000 euros et une injonction de mettre le traitement en conformité au regard des manquements retenus. Elle a également décidé de rendre publique la sanction prononcée.

Cinq manquements au RGPD ont été retenus par la formation restreinte dans le cadre de cette sanction :

- absence de prise en compte du droit d'opposition des personnes (aucune procédure ne permettait de s'assurer efficacement que les personnes s'étant opposées au démarchage téléphonique ne soient plus appelées) ;
- présence de données non pertinentes (commentaires injurieux ou en lien avec la santé des personnes) dans le fichier client de la société ;
- information insuffisante des personnes démarchées sur le traitement de leurs données personnelles et les droits dont elles bénéficient ;
- défaut de coopération avec la CNIL ;
- encadrement insuffisant des transferts de données personnelles vers des prestataires situés hors de l'Union européenne.

Par cette décision, la CNIL a principalement entendu rappeler l'attention toute particulière qu'elle porte au respect des droits des personnes et à la coopération qu'elle attend des responsables de traitement.

Cette sanction a ainsi été l'occasion pour la CNIL de souligner la nécessité de mettre en place des procédures de gestion des demandes d'opposition à la prospection commerciale effectives et respectant le délai de réponse d'un mois prévu par l'article 12 du RGPD.

Compte tenu des nuisances que constituent de telles pratiques pour les personnes dont les droits ne sont pas respectés, la formation restreinte de la CNIL a considéré que ce manquement était d'une particulière gravité.

Par ailleurs, la CNIL a également rappelé que les responsables de traitement ont une obligation générale de coopération avec les autorités de contrôle. La formation restreinte a constaté que la CNIL avait fait preuve d'une volonté marquée d'accompagnement en faisant systématiquement droit à toutes les demandes de prorogation de délais formulées par la société, cherchant à aboutir à la mise en conformité des pratiques de la société. La formation restreinte de la CNIL a relevé l'inertie de cette société jusqu'à l'engagement d'une procédure de sanction.

Le déroulé de cette procédure illustre la double mission de la CNIL : accompagner les acteurs économiques et protéger les personnes. L'articulation entre ces missions s'effectue en prenant en compte le niveau de maturité des acteurs concernés, les moyens dont ils disposent pour se mettre en conformité, la nature des traitements mis en œuvre et les enjeux associés.

En tout état de cause, la conduite de la conformité ne peut se réaliser qu'avec la participation résolue des responsables de traitement qui doivent s'engager, en lien avec la CNIL, dans une démarche de mise en conformité.

Par la suite, la société a pris les mesures permettant de satisfaire à l'injonction prononcée dans la délibération de sanction. Cette mise en conformité a été actée par une délibération de la formation restreinte du 30 janvier 2020, publiée sur le site web de la CNIL.

La CNIL rappelle que des fiches pratiques concernant chacun des manquements relevés en l'espèce sont présentes sur son site web. Elles reprennent les règles applicables ainsi que les moyens d'aboutir à un traitement conforme aux règles posées par le RGPD.

FOCUS

La sanction contre Google

Le 21 janvier 2019, la CNIL a prononcé une amende de 50 millions d'euros à l'encontre de Google pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité.

À la suite de plaintes déposées par les associations **La Quadrature du Net** et **None of your business** en mai 2018, la CNIL a procédé à des investigations relatives aux traitements de données personnelles effectués par la société Google LLC. Elle a ainsi analysé le parcours d'un utilisateur lors de la création d'un compte Google à partir d'un téléphone fonctionnant avec le système d'exploitation Android.

Sur la base de ces investigations, la formation restreinte de la CNIL - chargée de prononcer les sanctions - a principalement retenu deux manquements au RGPD.

Tout d'abord, la formation restreinte a considéré que les informations fournies à l'utilisateur au moment de la création d'un compte n'étaient pas toujours claires et facilement accessibles. En particulier, la formation restreinte a relevé que des informations essentielles (sur les finalités, les durées de conservation ou les catégories de données pour la personnalisation de la publicité) étaient éparpillées sur plusieurs pages et que l'utilisateur devait parfois accomplir jusqu'à six actions pour y accéder. Elle a, en outre, relevé que les informations mises à disposition par Google étaient rédigées de façon trop vague, ce qui ne permettait pas aux utilisateurs de comprendre l'ampleur du traitement effectué par Google. La formation restreinte a en effet souligné que les données des utilisateurs étaient collectées à partir de nombreux services tels que Google mail, Google Maps ou YouTube, ce qui avait pour effet de rendre le traitement massif et intrusif.

Ensuite, la formation restreinte a estimé que le consentement des utilisateurs n'était pas valablement recueilli pour le traitement relatif à la personnalisation de la publicité. Elle a en effet relevé que le recueil du consentement se faisait au moyen d'une case pré-cochée par défaut, ce qui n'était pas conforme aux exigences du RGPD.

En conséquence, la formation restreinte a décidé de prononcer une amende administrative publique de 50 millions d'euros à l'encontre de la société GOOGLE LLC. Il s'agit de la première sanction de la formation restreinte faisant application des nouveaux plafonds de sanctions prévus par le RGPD. **Pour déterminer le montant de l'amende, la formation restreinte a notamment tenu compte de la place prépondérante qu'occupe le système d'exploitation Android sur le marché français, du nombre d'utilisateurs concernés et des gains financiers générés par la publicité personnalisée.**

ANTICIPER
et innover

Au-delà de ses missions d'accompagnement et de contrôle, la CNIL poursuit, au quotidien, son objectif d'anticipation de l'innovation technologique et de ses enjeux pour la vie privée et les libertés individuelles. En 2019, la CNIL a notamment pu continuer son exploration sur la thématique du design, à la suite de son Cahier IP 6 « La forme des choix » et du site web Données & Design, et conduire une réflexion sur les *civic tech*.

Juliette
Conseillère à la Présidence, responsable de la mission éthique

La réflexion éthique porte sur des choix de société décisifs. Elle ne saurait se construire indépendamment d'une prise en compte de cette dimension pluraliste et collective. Ceci est d'autant plus vrai quand il s'agit d'un objet aussi transversal à toutes les dimensions de notre vie individuelle et sociale que la démocratie participative.

Pour ce sujet, la CNIL a fait le choix d'organiser un format d'événement original, sur-mesure et interactif. À noter que son objectif n'était pas de produire de la doctrine juridique, qui existe déjà dans le cadre du RGPD, mais bien de nourrir une réflexion intellectuelle sur des débats de société.

Elle a confié la conduite du débat au média Usbek & Rica et co-organisé la soirée d'échanges dans l'hémicycle du Palais d'Iéna avec le Conseil économique, social et environnemental (CESE). Le dernier cahier « Innovation et Prospective » de la CNIL, édition spéciale Mission éthique sur ces mêmes enjeux, y a été distribué. La soirée a été croquée en direct par le dessinateur de presse Xavier Gorce. Sa retransmission est disponible sur notre site web, ainsi que du LINC et du CESE.

LA CNIL POURSUIT SON ACCOMPAGNEMENT DES ENJEUX DU DESIGN DANS LES SERVICES ET PRODUITS NUMÉRIQUES

La CNIL a continué, en 2019, son exploration et l'accompagnement de la thématique du design, à la suite de son Cahier IP 6 « La forme des choix », à travers l'alimentation de son site web Données & Design et l'organisation régulière d'ateliers. Cette plateforme dédiée et ces rencontres physiques ont pour objectif de fédérer une communauté de designers soucieux d'intégrer au mieux la protection des données et des libertés dans leurs interfaces, services et produits.

« La forme des choix » propose une exploration des enjeux du design dans la conception des services numériques, au prisme de la protection des données et des libertés. Ce cahier vise notamment à promouvoir l'émergence d'un design des interfaces plus responsable et respectueux des principes de protection des données. À l'instar des questions juridiques et techniques, le design des interfaces doit désormais être au centre des préoccupations du régulateur, tout comme il est déjà au cœur des relations entre les individus et les fournisseurs de services. C'est l'un des enjeux de ce cahier qui propose également des pistes de recommandation pour permettre aux professionnels d'échanger sur leurs pratiques respectives et de co-construire un design éthique de la vie privée. Il s'agit donc, pour la CNIL, d'accompagner les professionnels de la conception de service pour « construire une approche non-concurrente et *open source* des bonnes pratiques de design ».

Construire une approche non-concurrente et *open source* des bonnes pratiques de design.

La CNIL souhaite ainsi 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. L'objectif est de permettre aux concepteurs de services de se saisir des solutions offertes par le design pour accompagner positivement les utilisateurs dans la compréhension et la maîtrise du fonctionnement des services numériques et des traitements de données afférents.

Pourquoi s'intéresser aux designers ?

Le paysage des solutions proposées en termes de vie privée, de protection des données, d'interfaces et de parcours utilisateurs est trop pauvre. Les interactions qu'ont les personnes, concernant l'usage des données personnelles, avec les services qu'ils utilisent se résument encore trop souvent à cocher une case matérialisant l'acceptation de conditions d'utilisation.

Dans le contexte des données et services associés, le travail du designer répond souvent à des injonctions économiques (qu'il peut être difficile de mesurer) au détriment des droits de l'individu. Cette influence s'est progressivement traduite par des interfaces normalisées autour du paradigme d'expérience « sans couture » (ou fluide), où la facilité des interactions entre l'utilisateur et l'interface est le marqueur principal de la qualité de l'expérience. Cette approche, sans friction, a relégué au second plan les considérations de respect des droits, et par extension de la personne ou du citoyen. Certaines interfaces utilisateurs soulèvent de possibles questions de conformité vis-à-vis des exigences du RGPD : il peut s'agir par exemple de politiques de confidentialité trop longues pour être lues de façon réaliste, de demandes de consentement incitant les utilisateurs à sélectionner de manière plus ou moins libre les options moins respectueuses de la vie privée, ou de modalités d'exercice des droits difficiles d'accès…

Le design pour solution

Il ne s'agit pas d'être fataliste face à ce constat, bien au contraire : les designers sont bien placés pour proposer des solutions afin d'améliorer cette situation et redonner la maîtrise de leurs données aux personnes. En effet, l'information des personnes, le recueil du consentement ou bien l'exercice des droits sont des questions sur lesquelles les designers sont fondamentalement à même d'agir grâce à leur savoir-faire. Le manque de propositions pour des modèles vertueux provient principalement, comme l'ont révélé des entretiens que nous avons effectués auprès de designers, d'un manque de connaissance de la loi de leur part. Avec le site web Données & Design[11], la CNIL souhaite outiller les designers d'un socle de connaissances appliqué à leur domaine pour qu'ils soient en mesure de participer à la création de nouveaux modèles plus vertueux tout en mariant intérêts économiques, exigences juridiques, réalité technologique et besoins utilisateurs.

La plateforme dédiée Données & Design comme espace et support de co-création

Données & Design est une plateforme visant à créer des opportunités de collaboration et des espaces d'échange entre des designers pour co-construire des parcours respectueux de la vie privée.

11 Données & Design, design.cnil.fr

Divers contenus expliquant et illustrant les points de la réglementation sur lesquels les designers peuvent, et devraient, agir sont mis à disposition. Outre la dimension pédagogique et pratique, l'objectif est une intégration effective de ces réflexions dans le quotidien des designers afin de permettre d'argumenter leurs choix et de travailler en plus proche collaboration, sur la protection des données personnelles, avec d'autres fonctions telles que chefs de produits (*product owner*), chefs de projets (*project manager*) ou les départements juridiques.

Concrètement, Données & Design est structurée autour de trois approches complémentaires :

- **Une acculturation à trois grands concepts du RGPD :** l'information des personnes, le consentement, l'exercice des droits. Pour chacun de ces concepts, les caractéristiques principales de mise en œuvre sont illustrées au travers d'exemples ;
- **La diffusion d'études de cas :** co-construites progressivement avec la communauté, ces études sont l'occasion de voir comment les concepts peuvent s'inscrire de façon originale dans les parcours utilisateurs et les modalités d'interaction avec des services et produits numériques ;
- **La création d'espaces d'échanges :** aussi bien en ligne (par un canal de discussion Slack, dans un premier temps) qu'en présentiel, ces espaces sont autant d'occasion d'échanger, de recueillir les problèmes spécifiques rencontrés par les designers dans leurs pratiques et d'imaginer ensemble les solutions possibles.

En 2019, la CNIL a organisé **7 ateliers** regroupant des designers, entrepreneurs, juristes et autres profils afin d'explorer des manières de créer des interfaces, produits et services respectueux de la vie privée. **Près de 150 personnes ont ainsi participé à la création d'études de cas,** qui documentent la démarche, les choix de présentation, mais également les limites ou les perspectives d'évolution. Ces études de cas sont disponibles sur le site Données & Design ainsi que les supports et méthodologies d'ateliers, afin que chacun puisse s'en saisir et construire ses propres outils.

Sur le service de messagerie Slack, 644 personnes ont rejoint la communauté pour échanger sur ces différents sujets et faire des retours sur les ateliers ou les études de cas.

CIVIC TECH, UN OBJET POLITIQUE ET TECHNOLOGIQUE À IDENTIFIER

69 %

des Français ressentent de la méfiance vis-à-vis des politiques[12]

Un écosystème hétérogène

Des *civic tech* aux *pol tech*, sans oublier les *gov tech*, nombreuses sont les applications, les plateformes et les API (*Application Programming Interface* en anglais ou interface de programmation d'application) qui tentent de mettre les nouvelles technologies au service d'un renouveau de la démocratie. Il s'agit souvent de résoudre la crise de défiance qui frappe les institutions publiques, dont l'une des conséquences se constate dans l'accroissement du taux d'abstention de ces dernières années.

Au-delà des questions de terminologie et des langages informatiques utilisés, ces initiatives présentent une grande diversité :

- **d'objectifs** (augmenter et faciliter la participation citoyenne, promouvoir une plus grande transparence politique, désintermédier le dialogue entre élus et administrés) ;
- **de statuts** (de l'association à la startup en passant par les institutions ou fondations d'entreprise) ;
- **de modèles économiques** (prestation de services auprès du public, partenariat avec des entreprises, levées de fond, subventions publiques ou privées, exploitation de données, appel aux dons)...

Des projets politiques divers

Plus crucial encore, les acteurs de la *civic tech* ne partagent pas forcément le même projet politique. Certaines innovations se limitent à doter les institutions représentatives de nouveaux moyens de connaissance des réalités sociales. D'autres misent sur la promotion d'un **gouvernement ouvert** dans lequel citoyens et autorités pourraient travailler main dans la main à des solutions concrètes, voire à co-construire des lois. D'autres, enfin, imaginent des initiatives plus radicales qui contraindraient les représentants à tenir compte des volontés de leurs électeurs et permettraient aux citoyens d'accéder à des fonctions de pouvoir, sans coloration partisane.

Enfin, la question de la **représentativité des participants** aux initiatives se pose également. En effet, si la plupart des 10 *civic tech* cherchent avant tout à rétablir un rapport de confiance entre l'État et les citoyens, elles semblent pour l'instant n'intéresser qu'une part très réduite de la population, souvent issue des classes supérieures et déjà très politisées, ou au moins conscientisée.

12 Baromètre de la confiance politique réalisé en 2019 par CEVIPOF auprès d'un échantillon de 2 084 personnes inscrites sur les listes électorales issues d'un échantillon de 2 200 personnes représentatif de la population française âgée de 18 ans et plus.

L'objet du débat

Pour assoir sa légitimité et aider à réformer durablement les institutions et le processus démocratiques, l'écosystème *civic tech* se trouve face à des défis importants :

- Comment réduire la **fracture numérique** pour assurer leur large diffusion ?
- Comment **co-exister avec des dispositifs existants** et compléter intelligemment leur apport sans tomber dans l'écueil d'une démocratie numérique froide et décentralisée ?
- Comment garantir la **protection des données personnelles** ?
- Sur quel projet politique pourraient s'accorder a minima les différents acteurs et parties prenantes pour **éviter une ubérisation de la démocratie** ?

Pour en débattre, la CNIL a invité des représentants du monde politique, associatif et citoyen, à **un débat le 9 décembre 2019** au Conseil économique, social et environnemental (CESE) :

- Patrick Berckmans, responsable du département de démocratie numérique de l'État fédéral belge ;
- Valentin Chaput, co-fondateur d'Open Source Politics, expert en innovations démocratiques et civiques ;
- Catherine Dufour, ingénieure informaticienne, chroniqueuse au Monde Diplomatique et écrivaine de romans de science-fiction ;
- Clément Mabi, chercheur à l'UTC Compiègne, spécialiste des questions d'expérimentation démocratique.

Julia Reda, ancienne députée européenne membre du parti pirate allemand et Marine Albarède, cheffe de projets innovation et données à la Turbine.coop, étaient présentes par l'intermédiaire d'un témoignage vidéo.

Compte-rendu des échanges

Prendre en compte les limites de la participation

Les technologies politiques rassemblent l'ensemble des initiatives visant à transformer les règles du jeu démocratique en intégrant une culture du numérique. Elles peuvent ainsi susciter des **craintes de recomposition du pouvoir** au profit d'un petit nombre ou d'entreprises privées. À l'inverse, elles sont parfois vues comme **objet de communication sans prise sur le processus politique.**

L'idée que les dispositifs de participation n'ont de sens que s'ils ont un effet sur l'action publique a été avancée. Pour cela, les intervenants ont insisté sur la nécessaire volonté politique de partager et d'inclure véritablement les citoyens dans la fabrique des politiques publiques.

La technologie n'est pas neutre

Le choix de l'outil contraint les possibilités de participation : les plateformes de *civic tech* tendent à privilégier les contributions écrites alors qu'une large part de la population est mal à l'aise avec ce média. Le design des interfaces est souvent un frein à la participation des individus tout comme les termes administratifs ou institutionnels, qui doivent être traduits en propos compréhensibles par le grand public.

Le postulat selon lequel le citoyen a l'envie et les moyens de participer au débat a été déconstruit, au profit de celui du caractère collectif de la démocratie et de l'importance de **ne pas individualiser la démocratie** pour chacun au travers des *civic tech*.

La question de la collecte des données personnelles a fait l'objet d'un débat, jugé nécessaire pour certains afin d'être en **capacité de situer qui parle** pour analyser les contributions, expliciter les différents régimes de légitimité et éviter tout biais représentatif.

Le rôle de l'État

Alors que les initiatives participatives portées par des acteurs privés, startups ou géants du numérique, se multiplient, la place et le rôle de l'État sont rapidement apparus dans le débat entre les intervenants.

Une première vision considère que l'État est le seul garant de la protection des données personnelles et de la détermination de l'intérêt général. Une seconde consiste à défendre le **modèle des communs**, dans lequel l'État doit jouer un rôle d'impulsion, en citant le cas de la mairie de Barcelone à l'origine du développement de l'outil open source de participation Decidim.

Il faudrait alors adapter le dispositif au contexte et aux finalités de la participation et faire du sur-mesure sans négliger l'articulation avec les dispositifs présentiels. La participation serait davantage une question d'artisanat que d'ingénierie.

Des pistes de réflexion pour la CNIL

Le débat s'achevait sur les recommandations complémentaires : développer une éducation réflexive sur le numérique pour Clément Mabi, investir dans les écosystèmes vertueux et les communs numériques pour Valentin Chaput, maîtriser et encadrer par l'État les technologies politiques pour Patrick Berckmans, donner aux citoyens le pouvoir de formuler le contenu des votes pour Catherine Dufour.

PRIX CNIL-INRIA 2019 POUR LA PROTECTION DE LA VIE PRIVÉE

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 2019, Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador et Narseo Vallina-Rodriguez ont ainsi été récompensés pour leur article *« An Analysis of Pre-installed Android Software »*[13].

L'article examine les problèmes de confidentialité et de sécurité associés aux logiciels préinstallés sur les appareils Android. Contrairement aux logiciels installés par l'utilisateur, les applications préinstallées disposent de privilèges étendus et peuvent fonctionner sans le consentement de l'utilisateur, en contournant le système de permission Android, sans aucune possibilité de désengagement. L'étude menée est impressionnante par le nombre d'applications, de modèles d'appareils et de fournisseurs analysés, ainsi que par la profondeur des analyses menées. Ce travail revêt un grand intérêt tant pour sensibiliser les utilisateurs d'appareils Android que pour l'application de la réglementation en matière de protection des données, car il décrit les stratégies et moyens par lesquels les entreprises qui créent des applications peuvent contourner les garanties de protection des données. Il attire l'attention sur la nécessité de développer des outils d'audit des systèmes pour les applications mobiles qui ne tiennent pas seulement compte du comportement des applications, mais aussi de leurs interactions.

Plus de quarante-cinq articles ont été soumis, ce qui témoigne de l'intérêt toujours croissant de la communauté scientifique pour cet événement.

De gauche à droite : Guillaume Prunier, directeur général délégué d'Inria, Juan Tapiador, Narseo Vallina et Julien Gamba, lauréats et Nataliia Bielova et François Pellegrini, présidents du jury.

13 Gamba, Julien and Rashed, Mohammed and Razaghpanah, Abbas and Tapiador, Juan et Vallina-Rodriguez, Narseo, *An Analysis of Pre-installed Android Software*, 2020

Les sujets de réflexion en 2020

Portabilité : une opportunité à saisir

Si le RGPD vise, de manière générale, à ce que tout citoyen européen puisse conserver la maîtrise de ses données, l'article 20 permet à chacun de pouvoir librement les réutiliser. La portabilité des données personnelles offre de nouvelles perspectives pour les utilisateurs, mais aussi pour des entreprises souhaitant créer des services innovants.

Une innovation portée par le droit

Le droit d'accès existe depuis plus de 40 ans dans la loi Informatique et Libertés ; il est complémentaire du droit à l'information puisqu'il apporte de la transparence sur les données effectivement conservées par les responsables de traitement. La portabilité est un droit nouveau apparu en 2018 avec le RGPD, qui permet notamment aux personnes de recevoir les données personnelles qu'elles ont fournies à un responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine. Ces données peuvent ensuite être transmises à un autre responsable de traitement, et elles peuvent même être transmises directement d'un responsable de traitement à un autre, lorsque cela est techniquement possible. La portabilité vient ainsi donner corps à la libre circulation de ces données figurant dans le titre du règlement européen.

Sortir de l'enfermement propriétaire

Ce droit offre ainsi un nouveau levier aux individus afin de contrer les éventuels enfermements propriétaires (ou « *lock-in* ») qui rendent les utilisateurs captifs de certains services. Par exemple, l'historique d'écoute d'un site de musique en streaming permet d'obtenir une recommandation de musiques plus adaptée à ses goûts et ses centres d'intérêts. Sans la portabilité, passer à un nouveau service impliquerait, pour les utilisateurs, la perte de cet historique d'écoute et de l'ensemble des playlists qu'ils ont créées. Le coût de transaction non monétaire d'un changement de service pourrait, à lui seul, contrebalancer l'intérêt qu'offrirait cet éventuel nouveau service.

Les données concernées par la portabilité

La portabilité ne s'étend pas à l'ensemble des données personnelles détenues par un acteur. D'une part, elle concerne uniquement les données dont le traitement repose soit sur le contrat, soit sur le consentement. D'autre part, elle ne concerne que les données déclarées activement et consciemment par la personne concernée, telles que des données fournies pour créer un compte en ligne (par exemple : adresse électronique, nom d'utilisateur, âge), les données générées par l'activité de la personne concernée, lorsqu'elle utilise un service ou un appareil (par exemple les données brutes collectées par des compteurs communicants, les achats enregistrés sur une carte de fidélité, un historique d'événements, etc.). Elle exclut donc les données personnelles qui sont dérivées, calculées ou inférées à partir des données fournies par la personne concernée. Dans le cas d'une plateforme de streaming musical, les listes de recommandations ne sont, par exemple, pas concernées.

Des opportunités pour les personnes

La portabilité des données donne plus de contrôle aux personnes sur leurs données et leur permet de fluidifier le passage à de nouveaux services, notamment car :

- il facilite la capacité des personnes à déplacer, à copier ou à transmettre facilement des données à caractère personnel d'un environnement informatique à un autre ;
- il limite notre dépendance aux services que nous utilisons (par exemple en cas de changement de la politique de confidentialité ou en cas de fermeture imminente d'un service) ;
- il évite le « démarrage à froid » lors de l'inscription à un nouveau service doté d'un système de recommandation.

Des modalités à réinventer

Encore faut-il que ce passage entre les services soit à la portée de tous. Le RGPD n'est pas prescriptif sur la manière d'exercer son droit (pour les personnes) et de répondre à celui-ci (pour les professionnels), même s'il doit néanmoins répondre à des exigences générales de sécurité.

L'acteur concerné doit pouvoir ainsi s'assurer que les données sont transmises à la bonne personne (ou à la bonne destination en cas de transfert direct) et doit, également, sécuriser les transferts de données tout en continuant à protéger les données qui restent dans son système. Cela peut notamment passer par la possibilité d'exercer ce droit depuis son compte authentifié, et la mise en place d'un lien direct de passage d'un service à un autre.

L'extension des usages de la portabilité dépendra nécessairement de la facilité qu'auront les utilisateurs à extraire leurs données des services, et la capacité pour ceux à qui elles sont transférées de les réutiliser afin d'améliorer ou créer de nouveaux services. Il appartient donc aux acteurs de s'accorder sur des **formats interopérables** qui permettront la portabilité des données.

Un cadre pour les acteurs innovants

Tout un écosystème de startups françaises et européennes souhaite déjà s'appuyer sur la portabilité pour créer de nouveaux modèles dans le sillage de l'expérimentation MesInfos de la Fing, à laquelle la CNIL avait participé dès 2013, et qui propose aux individus de reprendre le contrôle de leurs données par la centralisation de celles-ci dans un *cloud* personnel.

D'autres acteurs innovants proposent de nouveaux outils de facilitation de l'exercice des droits, des outils de gestion des droits clés en main pour les responsables de traitement, ou de nouveaux modèles permettant d'actionner une forme de portabilité « complémentaire », entre des services non concurrentiels mais pour lesquels le partage de données, sous le contrôle de l'individu, pourrait apporter de nouveaux services.

Dans le secteur public aussi, des acteurs s'organisent, à l'image des villes du Grand Lyon, La Rochelle et Nantes Métropole, qui explorent la possibilité de faire émerger de nouveaux services à partir de la portabilité des données, dans une logique de portabilité citoyenne, telle que développée dans les recommandations du cahier IP 5, *la Plateforme d'une ville*. C'est tout un écosystème qui s'engage dans la portabilité, chacun à sa manière, explorant ce nouveau champ des possibles.

Pourtant, il reste encore des progrès à faire dans la mise en œuvre de ce droit. Si certains acteurs internationaux, et quelques français et européens, ont déjà travaillé à l'élaboration de systèmes techniques de partage de données, ce droit et son exercice pourraient souvent être facilités, également dans une logique d'entreprise plus offensive et servicielle, basée sur la relation de confiance avec les utilisateurs.

Si elle bouscule le monde ancien, la portabilité en tant que nouveau paradigme offre, et offrira, des opportunités pour tous les acteurs qui sauront s'en saisir, sous le contrôle des individus concernés.

« Il appartient aux acteurs de s'accorder sur des formats interopérables qui permettront la portabilité des données. »

INFOSPLUS

La CNIL organisera un évènement sur le droit à la portabilité en 2020. Une occasion pour explorer, avec les parties prenantes, les opportunités d'innovation offertes par ce nouveau droit.

Comment bâtir une protection de la vie privée « inclusive » pour tous ?

La protection des personnes au quotidien est l'un des axes stratégiques de la feuille de route 2019-2021 de la CNIL.
Or, les usages du numérique dans la vie quotidienne restent mal appréhendés. Mieux comprendre les pratiques, dans leur diversité, est indispensable pour pouvoir mieux accompagner les personnes dans l'exercice de leurs droits.

Des usages numériques diversifiés

Plusieurs travaux récents sur les pratiques numériques mettent en avant les différences d'usage du numérique selon les classes sociales et les territoires.

L'essor du mobile multifonction (smartphone) a fait entrer internet dans la vie quotidienne d'une majorité de Français, comme en témoignent les travaux de Dominique Pasquier auprès de familles modestes de l'ouest de la France[1]. La sociologue révèle l'existence d'un « autre internet » dont les usages diffèrent profondément de ceux des classes plus aisées. Leur rapport parfois compliqué à l'écrit a généré des pratiques particulières avec notamment un faible usage du courriel, tandis que l'individualisation des outils d'accès à internet entre en tension avec les valeurs du collectif familial. Elle observe cependant une obligation de transparence forte des pratiques entre les membres des familles, avec par exemple des adresses courriel ou des comptes partagés sur les réseaux sociaux.

Lors de la promotion de ce livre, Dominique Pasquier a été interrogée à plusieurs reprises sur le rapport de ses enquêtés à la protection de la vie privée et des données personnelles. Or, comme elle l'indique : « Personne ne m'en a parlé [des questions de vie privée]. Je n'ai jamais recueilli quoi que ce soit sur le problème des données personnelles, comme si le débat qui agitait la presse à ce sujet restait celui des élites, un sujet qui ne les concernait pas, comme s'il n'y avait pas les mêmes problèmes publics dans tous les milieux sociaux. Est-ce que ça veut dire que c'est une inquiétude qui n'a pas traversé

1 Dominique Pasquier, *L'Internet des familles modestes*. Enquête dans la France rurale, Paris, Presses des Mines, 2018, 222 p.

« Au travers de l'analyse des pratiques numériques et des rapports quotidiens à la vie privée, la CNIL souhaite proposer un accompagnement à la protection des données personnelles adapté à l'ensemble des personnes. »

cette zone sociale ? C'est possible. » Ainsi, tout autant que les usages varient selon les situations sociales, le rapport à la vie privée diverge également selon les contextes et les caractéristiques sociales des individus. Les débats sur la souveraineté numérique et la collecte massive de données personnelles par des acteurs publics ou privés ont un écho limité au sein des classes populaires. Par contre, la protection de l'intimité familiale et les craintes d'usurpation d'identité sont des préoccupations très fortes au sein des classes populaires, pour lesquelles la préservation de leur capital réputationnel est un enjeu crucial[2].

La protection de la vie privée au quotidien et le recours aux droits

Cette compréhension fine des usages numériques souligne en creux les stratégies, volontaires ou involontaires, mises en œuvre par les individus pour protéger leur vie privée. Loin de s'afficher totalement, la réputation en ligne est le fruit d'un travail de sélection, retrait, modification de certaines données, qui visent à se montrer tout en se cachant[3]. Ces pratiques témoignent d'une évolution de la conception de la vie privée. « Construite comme un droit de protection, la vie privée est de plus en plus conçue comme une liberté. Elle ne disparaît pas : elle s'individualise », comme l'affirme Dominique Cardon[4]. Les individus souhaitent de plus en plus tracer eux-mêmes la frontière entre le public et le privé. Ils sont particulièrement sensibles aux usages malveillants de ce qu'ils ont souhaité cacher.

Le RGPD confie aux individus des droits supplémentaires sur le traitement de leurs données personnelles. La mise en œuvre effective de ces droits est un point central pour le régulateur. Si les individus peuvent être conduits à s'en saisir de manière différenciée selon les contextes, les milieux sociaux, leurs parcours, leur situation individuelle, les droits fondamentaux reconnus par les textes – droit à la protection des données, droit à la vie privée – doivent au final être garantis, en tout état de cause, pour tous, au même niveau, sans « exclusion numérique ». La CNIL, service public de la régulation des données personnelles, y est attachée. L'exploration des pratiques individuelles qui sera menée en 2020 vise ainsi à mesurer les effets du RGPD sur les comportements, les attitudes et les représentations des citoyens vis-à-vis de la vie privée, et à mieux comprendre les déterminismes sociaux qui influent sur la sensibilité aux données personnelles et au recours au droit. Au travers de l'analyse des pratiques numériques et des rapports quotidiens à la vie privée, la CNIL souhaite proposer un accompagnement à la protection des données personnelles adapté à l'ensemble des personnes.

2 Benoît Coquard, *Ceux qui restent. Faire sa vie dans les campagnes en déclin*. La Découverte, 2019, 280 p.
3 Sonia Livingstone, « Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression ». *New Media & Society*, 2008, 10 (3). pp. 393-411
4 Dominique Cardon, *Culture numérique*, Paris, Les Presses de Sciences Po, 2019, 430 p.

Un bac à sable réglementaire en matière de données personnelles

Alors que les termes « bac à sable » et « expérimentation » sont de plus en plus revendiqués par les acteurs de l'innovation, du secteur privé comme du secteur public, quelles spécificités et quelles voies explorer pour la protection des données personnelles ?

L'expérimentation, un cadre général pour donner la priorité à l'innovation

L'approche du « bac à sable » *(sandbox)* est utilisée pour expérimenter dans plusieurs champs réglementaires. Au Royaume-Uni, la Financial Conduct Authority (FCA) permet à certaines *FinTechs* (« technologie financière ») — dans le cadre d'un suivi étroit et avec le soutien actif de l'autorité de régulation — de tester pour une durée limitée un modèle d'affaires en s'abstrayant du cadre réglementaire. En France, la loi pour une République numérique (loi n°2016-1321 du 7 octobre 2016) permet à l'ARCEP d'expérimenter des bacs à sable réglementaires sur une durée maximale de deux ans dans le domaine des communications électroniques.

Favoriser l'innovation

L'objectif principal d'un tel dispositif pour les pouvoirs publics est de favoriser l'innovation en apportant sécurité juridique et accompagnement aux acteurs retenus, qui ont besoin de proportionnalité dans l'application de la réglementation. Le public peut ainsi bénéficier des avantages que lui apportent ces projets, dans le cadre d'une supervision proche et attentive. Le régulateur, quant à lui, en tire une meilleure anticipation des risques émergents et des nouvelles thématiques dans son domaine de compétence, en lien étroit avec l'écosystème dans une logique de corégulation.

INFOSPLUS

Dans les pays anglophones, la *sandbox* désigne un environnement préconfiguré pour permettre à une entreprise d'expérimenter de nouvelles technologies, y compris en matière de régulation lorsque l'application pleine et entière d'une réglementation est supposée faire obstacle au développement de l'innovation.

Définir une méthodologie solide

Ce dispositif présente un caractère temporaire et doit déboucher, finalement, sur l'adaptation du modèle d'affaires ou technologique au cadre réglementaire, ou sur une adaptation de ce dernier si des barrières non souhaitables à l'innovation sont relevées. Il repose sur une méthodologie solide visant à définir des objectifs précis et à conduire une évaluation rigoureuse des effets positifs et négatifs du produit ou service expérimenté mais aussi de l'expérimentation elle-même. À ce titre, il peut être rapproché du droit à l'expérimentation permis en droit français depuis la révision constitutionnelle de 2003, et rejoint les conclusions de l'étude du Conseil d'État publiée en octobre 2019[5].

Le cas spécifique de la protection des données personnelles

La protection des données personnelles a ceci de spécifique qu'elle procède d'un droit fondamental et ne saurait, à ce titre, faire l'objet d'un affaiblissement ; l'expérimentation ne peut avoir pour objectif ou conséquence, par exemple, de mettre en question les droits reconnus aux personnes. Des dérogations réglementaires, même expérimentales, ne sont d'ailleurs guère possibles dès lors que le RGPD est un instrument juridique européen d'harmonisation forte et d'effet direct, qui ne prévoit pas expressément de « bac à sable » formalisé.

Apporter une sécurité juridique

Une application progressive et dynamique de la réglementation par la CNIL, dans une logique de « bac à sable » est, en revanche, parfaitement envisageable. D'une part, la CNIL est amenée à décliner l'application des règles du RGPD au moyen de divers instruments de conformité qu'elle élabore ; d'autre part, elle considère nécessaire dans le cadre de son mandat d'apporter de la sécurité juridique dans des domaines eux-mêmes émergents où les équilibres de conformité ne sont pas encore établis. Accompagner l'innovation est ainsi au cœur de son activité.

Développer des facteurs de confiance

Le RGPD est également un vecteur d'innovation. Il pose un cadre pour la création de services et de modèles d'affaires sains dans l'univers numérique, facteurs de confiance pour les individus et de réussite pour les projets, y compris en termes de crédibilité. Le rôle de conseil de la CNIL en matière de conformité lui permet de fournir des clés de compréhension, outils et suggestions techniques pour parvenir à cet objectif.

Si l'autorité de protection des données britannique (ICO) a mis en place en 2019 une *sandbox* sans dérogation au RGPD pour les services et produits innovants utilisant des données personnelles et présentant un intérêt pour le public — dix projets ont ainsi été sélectionnés pour recevoir un accompagnement spécifique — en France, la CNIL n'a pas attendu pour accompagner l'innovation par l'expérimentation.

FOCUS

CNIL et expérimentation, une histoire qui n'est pas nouvelle

Dès 2013, une banque a eu la possibilité, dans le cadre d'une demande d'autorisation préalable, d'expérimenter, sur un échantillon restreint et pour une durée limitée, l'utilisation de la biométrie pour authentifier des paiements en ligne. Cette expérimentation a ainsi pu être mise à disposition de tous les clients de cet établissement bancaire en 2016. Le suivi de l'expérimentation a pu permettre de vérifier que l'utilisation faite des données était maîtrisée, sûre et conforme aux objectifs initiaux.

En 2016, la CNIL a autorisé un intermédiaire en financement participatif à proposer une plateforme de financement participatif *(crowdfunding)* dédiée à des prêts étudiants. La plateforme évaluait, pour chaque étudiant présentant un projet de financement de ses études, son risque statistique de défaillance et, d'autre part, sélectionnait les demandes correspondant à un niveau de risque de défaillance jugé satisfaisant. La CNIL s'est notamment penchée sur les données utilisées par le promoteur du projet.

De même, la CNIL a autorisé, en 2017, une société à mettre en œuvre à titre expérimental un traitement de données personnelles ayant pour finalité la mesure d'audience et de fréquentation de dispositifs publicitaires dans un espace public. Le dispositif consistait à implanter dans les mobiliers publicitaires des boîtiers permettant de collecter les adresses MAC des appareils des personnes passant à proximité, puis d'anonymiser ces données afin de les restituer sous forme de graphe de flux de passage. Cela permettait de fournir à une régie publicitaire des informations de comptage sur le nombre de personnes passées d'un point à un autre, sans pour autant qu'un parcours individuel puisse être établi.

5 « Améliorer et développer les expérimentations pour des politiques publiques plus efficaces et innovantes », 3 octobre 2019, conseil-etat.fr

Une nouvelle étape dans la politique d'accompagnement de l'innovation de la CNIL

La CNIL dispose d'une expérience indéniable en matière de soutien à l'innovation. Elle a décidé de se tourner résolument vers les acteurs innovants dans le cadre de sa « stratégie *startups* », afin de répondre au mieux aux besoins spécifiques des jeunes pousses amenées à collecter et traiter des données personnelles. Elle anime des ateliers thématiques, notamment au sein de Station F, qui ont donné lieu à la publication d'une page *hub* « *Startup* » sur le site de la CNIL et participe au collectif animé par la *French Tech*. Elle a développé une approche originale sur le design des interactions autour d'un site dédié, design.cnil.fr, et d'une communauté de designers (voir page 97 de ce rapport d'activité). Elle également récemment publié un guide RGPD pour les développeurs, sous forme de répertoire Git, pour permettre à ces derniers d'intégrer la protection des données dès la conception (*privacy by design*). Elle souhaite, enfin, être ambitieuse en termes d'accompagnement renforcé dans ce domaine.

INFOSPLUS

Les ateliers thématiques

Depuis 2018, la CNIL a animé 31 ateliers à destination des *startups*, pour une audience de 828 représentants de *startups*. Début 2020, et dans la continuité de la publication d'une page *Hub Startup*, elle publie un guide développeur sur la plateforme GitHub (en Français et bientôt en anglais). En seulement deux semaines, et après avoir été en *« trends git »* (sujet tendance du jour de la plateforme à son lancement), il était vu par 1 600 visiteurs uniques (et 5 600 vues au total).

Évaluer les bénéfices pour l'écosystème et le public

La mise en place d'une approche en mode « bac à sable » pourrait faire sens pour la CNIL. Il ne s'agirait pas de mettre en place des dérogations aux obligations du RGPD, ce que ni le législateur français ni la CNIL ne peuvent faire, mais plutôt de structurer et de formaliser une approche plus expérimentale de l'action du régulateur. Cela passerait par un effort d'accompagnement renforcé, notamment de jeunes entreprises, et pourrait se traduire, si l'expérimentation montre que c'est nécessaire, par une adaptation des outils et de la doctrine de la CNIL
.
Il y aurait de nombreux bénéfices à tirer d'une telle approche, pour le grand public qui souhaite voir ses données mieux protégées, pour le dynamisme de l'innovation dans notre pays ainsi que pour la CNIL elle-même, qui sera d'autant plus efficace en comprenant les enjeux émergents, les nouvelles architectures techniques et les modèles d'affaires de demain. De leur côté, les jeunes entreprises ont tout intérêt à intégrer la conformité au RGPD à leur projet dès sa conception, afin de minimiser les risques juridiques pour elles et les risques pour la vie privée de nos concitoyens.

La CNIL poursuit, en 2020, ses réflexions et son dialogue avec l'écosystème pour articuler une approche ambitieuse en termes d'accompagnement renforcé à l'innovation, en partenariat le cas échéant avec les autres régulateurs concernés.

À SUIVRE

Missions éthique 2020

En 2020, et dans la continuité du débat sur les *civic tech*, la CNIL organisera un nouveau colloque pour faire vivre la mission éthique et animer le débat.

FOCUS

Collaboration avec le Comité Consultatif National d'Éthique

Le Comité Consultatif National d'Ethique (CCNE) a été chargé de constituer un comité pilote d'éthique du numérique, dont la CNIL est membre. Ce comité pluridisciplinaire est constitué de spécialistes du numérique, académiques ou issus des entreprises, des philosophes, des médecins, des juristes, des membres de la société civile ainsi que des membres du CCNE et de la CERNA.

Cette initiative s'inscrit dans le cadre de la stratégie nationale de recherche en intelligence artificielle et dans la continuité des recommandations du rapport « Donner un sens à l'intelligence artificielle » de Cédric Villani. Ce comité pilote sera chargé « à la fois de remettre des premières contributions sur l'éthique du numérique et de l'intelligence artificielle et de déterminer les équilibres pertinents pour l'organisation du débat sur l'éthique des sciences et technologies du numérique et de l'intelligence artificielle ».

Ses premiers avis porteront sur :

- **Les agents conversationnels** présents dans les téléphones, les interfaces avec les services en ligne ou encore les appareils domestiques tels les enceintes connectées. Les enjeux éthiques concernent notamment la transparence sur le traitement des données récoltées, le respect des individus d'une part et la commodité de l'utilisation de telles applications de l'autre, ou encore la mise en œuvre de stratégies d'influence par de tels agents ;
- **Le véhicule autonome :** le comité analysera les tensions existantes entre automatisation et maîtrise humaine dans le contrôle du véhicule, ou encore les responsabilités partagées entre constructeur, assureur et utilisateur, en lien avec la mission confiée à Mme Anne-Marie Idrac ;
- **Le diagnostic médical et l'intelligence artificielle :** il s'agira de discuter la tension entre proposition de décision algorithmique et garantie humaine, de se demander quels sont les risques encourus lorsqu'on ne suit pas le « conseil » d'un algorithme de prédiction ou encore de promouvoir la transparence et l'explicabilité du fonctionnement de ces algorithmes tant pour les professionnels de santé que pour les usagers du système de santé.

Le Comité devra également s'attacher à mettre en place les moyens nécessaires à la sensibilisation, à l'information et à la prise de décision des personnes, entreprises, administrations, institutions, etc.

Les Ressources

LES RESSOURCES HUMAINES

En 2019, la CNIL s'est attachée, sur la base des 15 créations de poste qui lui ont été attribuées, à renforcer certains de ses domaines d'intervention, en particulier ses activités répressives et de conformité. Elle a aussi poursuivi le développement d'expertises pointues en technologies de l'information.

De plus, l'année 2019 a été marquée par la poursuite de la valorisation des compétences des collaborateurs et le renforcement de sa politique de ressources humaines, notamment avec la révision du règlement de gestion en application depuis le 1er janvier 2020, la poursuite du déploiement du télétravail ainsi que la mise à jour de son référentiel des métiers.

Au 31 décembre 2019, la CNIL comprend 215 agents en activité et a accueilli 37 stagiaires. Son plafond d'emplois a été exécuté à 99 %.

DONNÉES SOCIALES

215 postes fin 2019

63% de femmes

37% d'hommes

39 ans Âge moyen

8 ans l'ancienneté moyenne à la CNIL

80% des agents occupent un poste de catégorie A

48% des postes occupés par des juristes

22% des postes occupés par des assistants

19% des postes occupés par des ingénieurs / auditeurs des systèmes d'information

58% des agents travaillant à la CNIL sont arrivés entre 2014 et 2019

LES RESSOURCES FINANCIÈRES

En 2019, le budget alloué à la CNIL s'élève à **18 506 734 €** en autorisations d'engagement et en crédits de paiement, répartis comme suit :

- **15 162 970 €** pour la masse salariale (titre 2)
- **3 343 764 €** pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6), budget auquel s'ajoute une réallocation de **180 000 €** en autorisations d'engagement.

Le budget consacré à la masse salariale (titre 2) comprend la rémunération (charges comprises) des agents de la CNIL et les indemnités versées aux membres du Collège. Il a été exécuté à hauteur de 97 %.

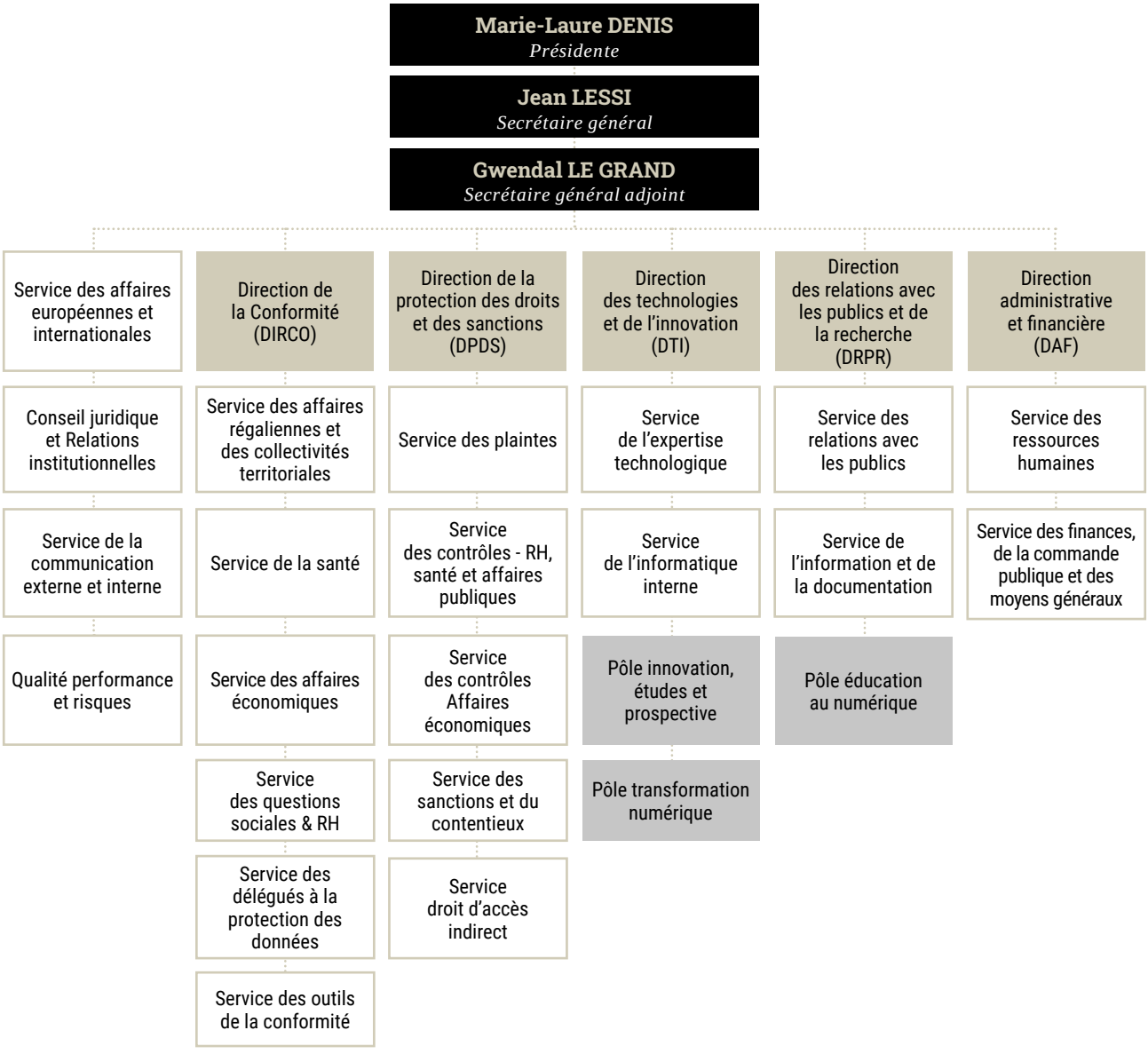
Quant au budget de fonctionnement, sa consommation a été conforme aux prévisions annoncées dans les documents budgétaires antérieurs, avec un taux de 105,2 % en autorisations d'engagement et de 98,5 % en crédits de paiement.

Les réalisations marquantes en 2019 portent sur la mise en place de nouveaux outils informatiques comme le compte usager (qui sera expérimenté en 2020 et contribuera à l'amélioration des téléservices en facilitant la relation avec les usagers de la CNIL), le développement du télétravail ainsi que des actions de projection sur des évènements telles que la présence de la CNIL au Forum international de la cybersécurité, au Salon des Maires organisé par l'AMF, ainsi que l'organisation de l'évènement *Civic tech* au Conseil économique, social et environnemental. Il est à noter que la refacturation des prestations mutualisées au bénéfice de la direction des services administratifs et financiers des services du Premier ministre s'élève à **228 400 €** en autorisations d'engagement (AE) et en crédits de paiement (CP).

Enfin, la CNIL s'attache à rationaliser ses coûts de fonctionnement dans un souci de maîtrise des dépenses publiques et de transparence des achats, en recourant notamment, dans la mesure du possible, aux marchés publics interministériels et mutualisés des services du Premier ministre.

CRÉDITS 2019	Autorisations d'engagement	Crédits de paiement
Budget LFI	**18 791 573**	**18 791 573**
Titre 2	15 239 165	15 239 165
Hors Titre 2	3 552 408	3 552 408
Budget disponible	**18 506 734**	**18 506 734**
Titre 2	15 162 970	15 162 970
Hors Titre 2	3 343 764	3 343 764
Réallocation	180 000	
Budget consommé	**17 978 353**	**17 751 930**
Titre 2	14 459 349	14 459 349
Hors Titre 2	3 519 004	3 292 581

Organigramme des Directions et Services



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