2020

Rapport d'activité

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

2020

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

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

Impression : Direction de l'information légale et administrative
Tél. 01 40 15 70 10 / www.ladocumentationfrancaise.fr

Crédit photos : CNIL, Adobe stock

Date de publication : Mai 2021

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.

LA CNIL, RÉGULATEUR DES DONNÉES PERSONNELLES

Créée par la loi Informatique et Libertés du 6 janvier 1978, la Commission Nationale de l'Informatique et des Libertés est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Au quotidien, la CNIL s'assure que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Le rôle de la CNIL

Informer et protéger les droits

La CNIL répond aux demandes des particuliers et des professionnels. Elle mène des actions de communication auprès du grand public et des professionnels que ce soit à travers ses réseaux, la presse, son Site web, sa présence sur les réseaux sociaux ou en mettant à disposition des outils pédagogiques.

Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

Accompagner la conformité et conseiller

Afin d'aider les organismes privés et publics à se conformer au RGPD, la CNIL propose une boîte à outils complète et adaptée en fonction de leur taille et de leurs besoins.

La CNIL veille à la recherche de solutions leur permettant de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens.

Anticiper et innover

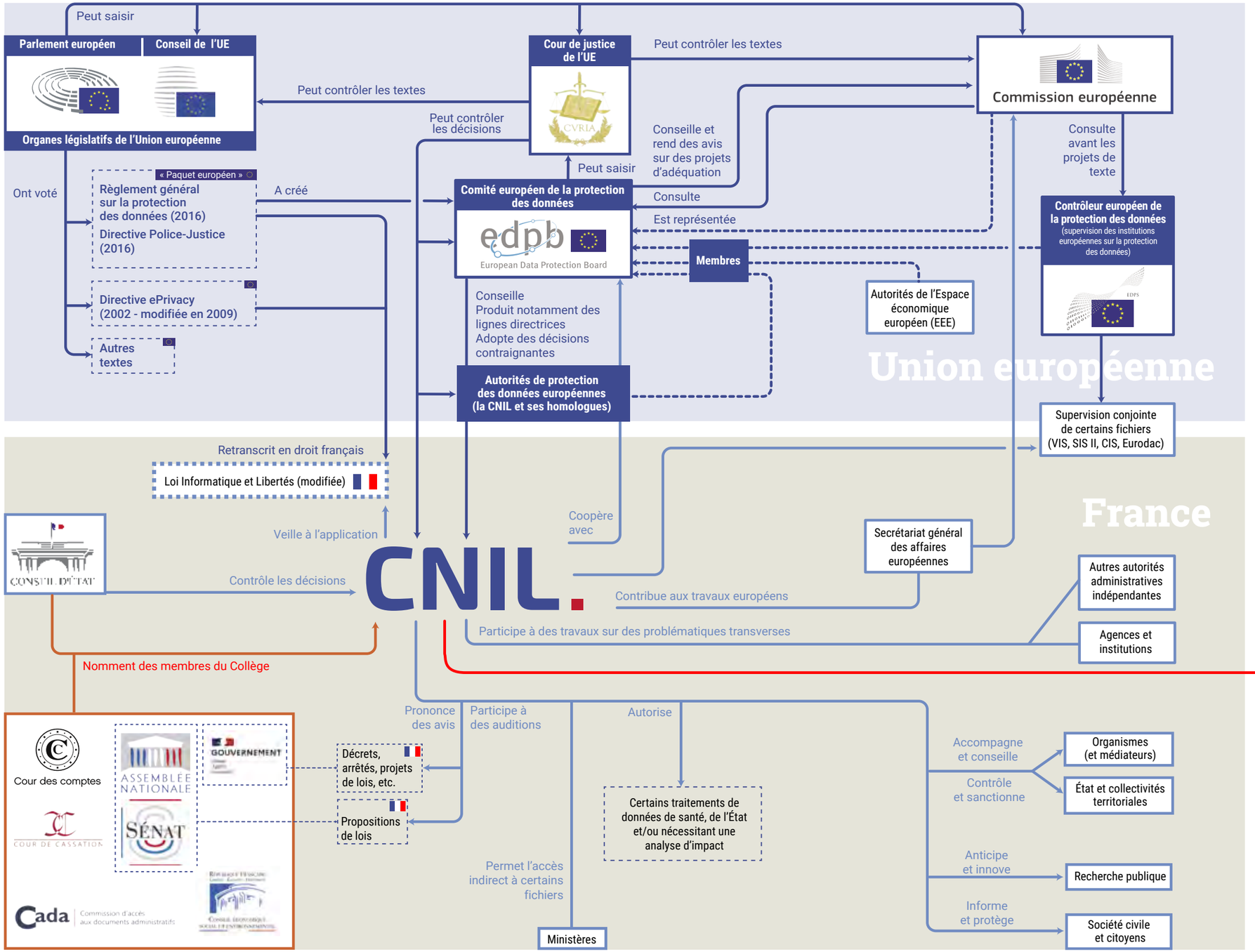
Pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée, la CNIL assure une veille dédiée.

Elle contribue au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de *privacy by design*.

Contrôler et sanctionner

Le contrôle permet à la CNIL de vérifier la mise en œuvre concrète de la loi. Elle peut imposer à un acteur de régulariser son traitement (mise en demeure) ou prononcer des sanctions (amende, etc.).

L'environnement de la CNIL



La protection des données dans les grandes lignes

Au-delà de son activité de régulation, la CNIL entretient des liens étroits, souvent prévus par des textes (par exemple des lois ou des règlements), avec un grand nombre d'entités publiques françaises et européennes.

Toutes ces relations, qu'il s'agisse d'échanges ou d'avis, sont primordiales : elles participent, ensemble, à une prise en compte globale de tous les enjeux sur la protection des données et à une meilleure protection des droits de tous les individus.

Cette carte, qui n'offre qu'un aperçu de l'environnement de la CNIL, présente ses relations avec les organismes publics, des collectivités françaises aux institutions européennes et mondiales. À cela peuvent donc s'ajouter, par exemple, tous les liens que la CNIL entretient au quotidien avec les organismes privés via un accompagnement individuel ou par la stratégie dite « des têtes de réseau ».

LES CHIFFRES CLÉS 2020

CONSEILLER & RÉGLEMENTER

20 AUDITIONS PARLEMENTAIRES

8 QUESTIONNAIRES ADRESSÉS AU PARLEMENT OU À UN PARLEMENTAIRE EN MISSION

423 AUTORISATIONS DE RECHERCHE EN SANTÉ DONT

89 AUTORISATIONS DE RECHERCHE SUR LA COVID-19

45% DES DOSSIERS COVID-19 TRAITÉS EN MOINS DE DEUX JOURS

139 DÉLIBÉRATIONS DONT

96 AVIS SUR DES PROJETS DE TEXTE

ACCOMPAGNER LA CONFORMITÉ

73 331 ORGANISMES ONT DÉSIGNÉ UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

25 494 DPO DÉSIGNÉS

+ 21 % PAR RAPPORT À 2019

109 472 COMPTES CRÉÉS SUR LE MOOC* ATELIER RGPD**

2 825 NOTIFICATIONS DE VIOLATIONS DE DONNÉES

PROTÉGER

13 585 PLAINTES QUI ONT CONDUIT À

4 528 RÉPONSES RAPIDES

9 057 ÉTUDES PLUS APPROFONDIES

3 996 DEMANDES VALABLES DE DROIT D'ACCÈS INDIRECT (DAI)

3 286 VÉRIFICATIONS EFFECTUÉES

1 MOOC : Massive Open Online Course (outil de formation à distance).
2 RGPD : règlement général sur la protection des données.

INFORMER

121 439 APPELS REÇUS

20 452 REQUÊTES REÇUES PAR VOIE ÉLECTRONIQUE +18%

9 677 000 VISITES SUR LES SITES WEB DE LA CNIL +21%

124 059 *FOLLOWERS* SUR TWITTER +7%

37 418 FANS SUR FACEBOOK +7%

133 053 ABONNÉS SUR LINKEDIN +16%

CONTRÔLER & SANCTIONNER

247 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT

- **82** CONTRÔLES EN LIGNE
- **74** CONTRÔLES SUR PIÈCES

49 MISES EN DEMEURE DONT

- **3** PUBLIQUES
- **4** ADOPTÉES EN COOPÉRATION AVEC D'AUTRES CNIL EUROPÉENNES

38 rappels à l'ordre prononcés par la présidente
2 avertissements prononcés par la présidente

14 SANCTIONS DONT

- **11** AMENDES D'UN MONTANT TOTAL **DE 138 489 300 EUROS**
- **2** RAPPELS À L'ORDRE DE LA FORMATION RESTREINTE
- **1** INJONCTION SOUS ASTREINTE NON ASSOCIÉE À UNE AMENDE

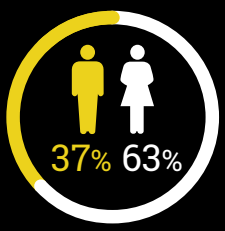
1 NON-LIEU

RESSOURCES HUMAINES

BUDGET : **20,1** MILLIONS D'EUROS

8 ANS ANCIENNETÉ MOYENNE DES AGENTS DE LA CNIL

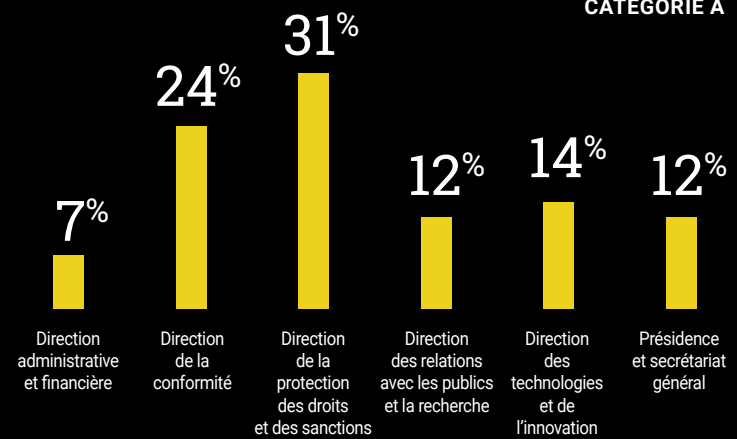
225 emplois



39 ans
Âge moyen

59% D'AGENTS ARRIVÉS ENTRE 2015 ET 2020

80% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A



LE COLLÈGE DE LA CNIL

Autorité administrative indépendante, la CNIL est composée d'un Collège pluridisciplinaire de 18 membres élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent, par le Premier ministre et les présidents des deux assemblées.

QUI COMPOSE LA COMMISION ?

18
MEMBRES COMPOSENT LA CNIL

6
REPRÉSENTANTS DES HAUTES JURIDICTIONS
(Conseil d'État, Cour de cassation, Cour des comptes)

4
PARLEMENTAIRES
(2 députés, 2 sénateurs)

5
PERSONNALITÉS QUALIFIÉES

2
MEMBRES DU CONSEIL ÉCONOMIQUE, SOCIAL ET ENVIRONNEMENTAL

1
MEMBRE DE LA COMMISSION D'ACCÈS AUX DOCUMENTS ADMINISTRATIFS

Les séances plénières

Les 18 membres de la CNIL se réunissent en séance plénière une fois par semaine sur un ordre du jour établi à l'initiative de la présidente.
Une partie importante de ces séances est consacrée à l'examen de projets de loi et de décrets soumis à la CNIL pour avis par le Gouvernement. Le Collège est également en charge de l'analyse des actes de droit souple tels que les lignes directrices, les référentiels ou les recommandations.
Lors d'une séance, un rapporteur présente son rapport ainsi que le projet de délibération aux membres du Collège. Ces derniers sont ensuite invités par la présidente à prendre la parole pour une discussion générale. À tout moment, pour éclairer les débats, la présidente peut donner la parole au secrétaire général ou à un autre agent de la CNIL en charge du dossier.
En cas de besoin, le vice-président délégué exerce les attributions de la présidente.

La formation restreinte

La formation restreinte est l'organe de la CNIL en charge de prononcer les sanctions. Composée de 5 membres du Collège et d'un président distinct du président de la CNIL, elle peut infliger diverses sanctions à l'égard des responsables de traitement qui ne respecteraient pas la loi et décide de rendre publique ou non une sanction.

Son président veille à son impartialité et à prévenir toute forme d'incompatibilité entre la mission des membres de la formation restreinte et leur situation.

Les séances de la formation restreinte

Lors d'une séance de la formation restreinte, le président de séance donne la parole au rapporteur pour un exposé de l'affaire, à l'organisme mis en cause ou son conseil, ainsi que, le cas échéant, au secrétaire général ou à tout agent de la CNIL désigné par ce dernier, puis au commissaire du Gouvernement.

Au terme de ces observations, et après avoir donné la parole en dernier à l'organisme mis en cause, le président prononce la clôture des débats.

FOCUS

Les avis de la CNIL

La CNIL peut être saisie par différents acteurs publics sur des projets de texte. Les avis rendus permettent d'éclairer les pouvoirs publics sur des enjeux Informatique et Libertés mais ne constituent pas une « validation », une « autorisation » ou encore un « refus ».
Le conseil aux pouvoirs publics est l'une des missions de la CNIL prévues par la loi Informatique et Libertés.

La CNIL exerce notamment cette mission au travers des avis qu'elle rend sur des projets de texte (lois, décrets, etc.), avant leur adoption. Elle conseille tout particulièrement le Gouvernement, qui doit obligatoirement demander son avis pour certains projets.

96 avis rendus sur des projets de texte ont été rendus en 2020.

Qu'est-ce qu'un avis de la CNIL ?

L'avis rendu par la CNIL :

- a pour objectif d'éclairer le Gouvernement, le Parlement ou toute autre autorité publique (par exemple une collectivité locale) ayant saisi la CNIL ;
- peut entraîner des modifications pour tenir compte des observations formulées dans la délibération (mais l'auteur de la saisine n'est pas tenu de modifier son projet en ce sens).

Pour cette raison, la CNIL rend un avis sur un projet de texte qui peut être différent de celui finalement déposé devant le Parlement ou publié.

Dans certains cas, l'avis de la CNIL doit obligatoirement être recueilli mais elle peut aussi être saisie pour avis à titre facultatif.

Important : cet avis ne constitue pas une « validation » ni un « refus » de la CNIL. Elle ne rend pas d'autorisation ni d'avis contraignant sur les projets de texte dont elle est saisie.

Sur quels textes la CNIL rend-t-elle des avis ?

Les projets de texte sont le plus souvent soumis par le Gouvernement ou le Parlement. Ils peuvent concerner la création ou la modification de traitements de données personnelles (par exemple : création d'un nouveau fichier, ajout de nouvelles finalités ou de nouveaux destinataires, etc.) ou, de manière plus générale, la protection des données personnelles.

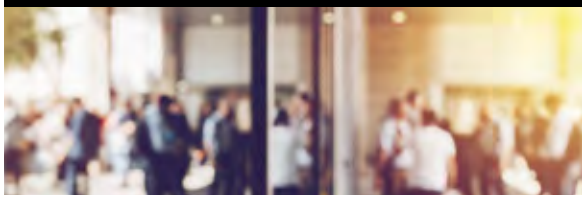
Concrètement, il peut s'agir de propositions de loi, de projets de loi ou d'ordonnance, de projets de décret ou de projets d'arrêté.

La CNIL peut être consultée sur l'intégralité d'un projet de texte ou seulement sur une ou plusieurs dispositions de ce projet qui peuvent présenter des enjeux pour la protection des données personnelles.

SOMMAIRE

3 Sujets de réflexion

4 Ressources



LES TEMPS FORTS 2020

Janvier

23/01 > Le prix CNIL-Inria est décerné à une équipe européenne

28-30/01 > Participation au 12e Forum international de la cybersécurité

28/01 > Publication du guide RGPD pour les développeurs

31/01 > Brexit : début d'une période transitoire pour la protection des données

Février

06/02 > Clôture de la mise en demeure contre FUTURA INTERNATIONALE

11/02 > Mise en demeure d'EDF et d'ENGIE

Mars

19/03 > Premier confinement national : publication de la CNIL sur les SMS adressés par le Gouvernement

25/03 > Nouveau calendrier d'adoption de la recommandation « Cookies et autres traceurs »

26/03 > Recherches sur la COVID-19 : la CNIL se mobilise

27/03 > Le Conseil d'État précise la portée géographique du déférencement à la suite d'un arrêt de la Cour de justice de l'Union européenne (CJUE)

Avril

07/04 > Les rappels de la CNIL sur la collecte de données par les employeurs

08/04 > Crise sanitaire : audition de la présidente de la CNIL, Marie-Laure Denis, devant la commission des lois

09/04 > Clôture de la mise en demeure contre BOUTIQUE.AÉRO

15/04 > Publication d'un référentiel pour la gestion des ressources humaines

22/04 > Avis de la CNIL sur l'arrêté relatif à l'organisation et au fonctionnement du système de santé

26/04 > Avis de la CNIL sur StopCovid

Mai

13/05 > Déconfinement : avis de la CNIL sur les fichiers SI-DEP et Contact Covid

18/05 > Le Conseil d'État suspend l'utilisation des drones pour contrôler le déconfinement

20/05 > Les rappels de la CNIL sur la surveillance des examens en ligne

26/05 > Avis de la CNIL sur la mise en œuvre de l'application StopCovid

28/05 > Rapport de la personnalité qualifiée sur le contrôle du blocage administratif des sites

Juin

04/06 > Lancement du programme de contrôles de la CNIL sur SI-DEP, Contact Covid et StopCovid

17/06 > La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques

19/06 > Le Conseil d'État rend une décision sur les lignes directrices sur les cookies et autres traceurs

30/06 > Lancement de la 5e édition du prix CNIL-Inria

Juillet

02/07 > Publication d'un guide pour une reprise d'activité par la task-force nationale de lutte contre les fraudes et escroqueries

10/07 > Publication d'un guide sur les tiers autorisés

16/07 > Invalidation du *Privacy Shield* par la Cour de justice de l'Union européenne (CJUE)

20/07 > Mise en demeure du ministère des Solidarités et de la Santé sur StopCovid

24/07 > Codes de conduite : publication du référentiel d'agrément des organismes de contrôle

28/07 > Publication de 3 référentiels pour le secteur de la santé

Août

05/08 > Sanction de 250 000 euros et injonction sous astreinte à l'encontre de SPARTOO

25/08 > Mise en demeure contre certaines communes pour mauvaise utilisation de LAPI (lecture automatisée des plaques d'immatriculation)

27/08 > Mise en demeure contre plusieurs employeurs pour collecte excessive de données par badgeuse photo

Septembre

01/09 > Publication de la charte des contrôles de la CNIL

04/09 > Clôture de la mise en demeure à l'encontre du ministère des Solidarités et de la Santé sur StopCovid

07/09 > Publication du premier livre blanc de la CNIL sur les assistants vocaux

11/09 > Rançongiciels : l'ANSSI et le ministère de la Justice publient un guide pour sensibiliser les entreprises et les collectivités

14/09 > 1er avis trimestriel de la CNIL sur SI-DEP, Contact Covid et StopCovid

16/09 > Signature d'un partenariat avec les Régions de France

16/09 > Signature d'un partenariat avec le médiateur des entreprises

22/09 > Rappel à l'ordre à l'encontre du rectorat de Normandie et d'une députée

29/09 > Signature d'un partenariat avec le Conseil supérieur de l'ordre des experts-comptables

Octobre

01/10 > Début du cybermoi/s 2020

01/10 > Publication des lignes directrices modificatives et de la recommandation de la CNIL sur les cookies et autres traceurs, ainsi que de nombreux contenus pour les professionnels et les particuliers

07/10 > Les recommandations de la CNIL sur les cahiers de rappel

14/10 > Le Conseil d'État demande au Health Data Hub des garanties supplémentaires pour limiter le risque de transfert vers les États-Unis, à la suite de l'invalidation du *Privacy Shield*

23/10 > La CNIL revient sur l'évolution de l'application « StopCovid », devenue « TousAntiCovid »

Novembre

02/11 > Sanction de 20 millions de livres pour British Airways et de 18,4 millions de livres sterling pour Marriott par l'autorité britanique de protection des données

09/11 > Évènement air2020 : quelles mutations dans le monde du travail ?

26/11 > Sanctions de 2 250 000 euros et de 800 000 euros pour les sociétés CARREFOUR FRANCE et CARREFOUR BANQUE

Décembre

08/12 > Renouvellement du partenariat entre la CNIL et l'Assemblée des Départements de France

10/12 > Sanctions d'un total de 100 millions d'euros à l'encontre de Google et de 35 millions d'euros à l'encontre d'Amazon

11/12 > Publication de l'avis de la CNIL sur les décrets relatifs aux fichiers PASP, GIPASP et EASP

17/12 > Sanction de 6 000 euros et de 3 000 euros à l'encontre de deux médecins

31/12 > Sanction à l'encontre de PERFORMECLIC

LES MEMBRES DE LA CNIL

LE BUREAU

PRÉSIDENTE

Marie-Laure DENIS

Conseiller d'État, présidente de la CNIL depuis février 2019

VICE-PRÉSIDENTE DÉLÉGUÉE

Sophie LAMBREMON

Conseiller honoraire à la Cour de cassation, vice-présidente déléguée de la CNIL

Secteurs : Intérieur / Recherche médicale

VICE-PRÉSIDENT

François PELLEGRINI

Professeur des universités à l'université de Bordeaux, vice-président de la CNIL

Secteurs : Commerce et publicité / Cybersécurité / Europe et international

LES MEMBRES (COMMISSAIRES)

Marie-Hélène BOIDIN-DUBRULE

Membre du Conseil économique, social et environnemental

Secteurs : Vie politique et citoyenne, transports

LES MEMBRES ÉLUS DE LA FORMATION RESTREINTE

- Alexandre LINDEN (président)
- Philippe-Pierre CABOURDIN (vice-président)
- Anne DEBET
- Alain DRU
- Bertrand DU MARAIS
- Christine MAUGÜE

Philippe-Pierre CABOURDIN

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

Secteurs : Banque, assurance et fiscalité

Anne DEBET

Professeur des universités

Secteurs : Données publiques et recherche, nouveaux outils de conformité

Alain DRU

Membre du Conseil économique, social et environnemental

Secteurs : Environnement et énergie

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

Secteurs : Social, logement et immobilier

Loïc HERVÉ
Sénateur de la Haute-Savoie

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

Christian KERT
Ancien député des Bouches-du-Rhône

Secteurs : Sport, médias et culture

Isabelle LATOURNARIE-WILLEMS
Conseillère maître à la Cour des comptes

Alexandre LINDEN
Conseiller honoraire à la Cour de cassation, président de la formation restreinte de la CNIL

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

Bertrand DU MARAIS
Conseiller d'État

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

Christine MAUGÜE
Conseiller d'État

Secteur : Justice

Jean-Luc NEVACHE
Conseiller d'État, président de la CADA (Commission d'accès aux documents administratifs)

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

Secteurs : Santé et assurance maladie

Sylvie ROBERT
Sénatrice d'Ille-et-Vilaine

Secteurs : Éducation et enseignement supérieur (hors sujets recherche)

COMMISSAIRE DU GOUVERNEMENT : Benjamin TOUZANNE **Adjoint :** Damien MILIC

AVANT-PROPOS DE LA PRÉSIDENTE

Marie-Laure DENIS
Présidente de la CNIL

L'ANNÉE 2020 AURA BOULEVERSÉ LE LIEN QUE NOUS ENTRETENONS AVEC LES DONNÉES PERSONNELLES

Les données à caractère personnel ont été utilisées pour **répondre aux multiples défis de la crise sanitaire :** dans les systèmes d'information de lutte contre la propagation du virus mis en place par l'État, dans le cadre des recherches médicales mais aussi, plus largement, dans tous les usages quotidiens du numérique qui ont explosé depuis le premier confinement, qu'il s'agisse des réseaux sociaux, de la visioconférence ou encore d'achats en ligne. En outre, certaines pratiques, jusque-là plutôt marginales, comme le télétravail, la télémédecine et le téléenseignement se sont intensifiées sans doute de manière durable, présageant une évolution de fond de nos habitudes et accentuant vraisemblablement certaines inégalités sociales face au numérique.

« La CNIL a autorisé de nombreuses recherches médicales pour étudier l'épidémie »

Cette accélération de la digitalisation de la société a généré beaucoup d'interrogations. C'est pourquoi la CNIL a tout particulièrement veillé, en 2020 dans ce contexte de foisonnement d'usages, à protéger la vie privée numérique en s'appuyant sur deux de ses missions essentielles : l'accompagnement et la répression.

La CNIL a conseillé très activement les pouvoirs publics afin de contribuer à garantir, en recherchant le délicat équilibre entre sécurité sanitaire et protection des libertés, que la mise en œuvre des systèmes d'information sanitaires (StopCovid devenu TousAntiCovid, SI-DEP, Contact Covid ou le SI Vaccin Covid) soit respectueuse des droits des personnes concernées.

La CNIL a ainsi rendu, en 2020, 10 avis liés à la gestion de la crise. Elle a aussi autorisé de nombreuses recherches médicales pour étudier l'épidémie (sur 423 autorisations délivrées, 89 sont en lien avec la COVID-19 dont près de la moitié ont été délivrées en moins de 48 heures.) ; elle a publié des recommandations à destination des particuliers et des professionnels et elle a répondu à de nombreuses questions concernant la mise en œuvre de ces solutions innovantes. La CNIL a ainsi apporté des éclairages sur les prises de température par les employeurs publics et privés, les distributions de masques faites par les collectivités locales à partir de fichiers, la télémédecine, l'enseignement à distance (par exemple, la surveillance des examens en ligne) ou encore l'envoi de SMS par le Gouvernement pour rappeler les consignes sanitaires dans le cadre de la lutte contre l'épidémie. Par ailleurs, la CNIL a priorisé le traitement des plaintes liées à la COVID-19 ainsi que les contrôles des dispositifs mis en œuvre en réaction à la crise, soit une trentaine de contrôles sur des sujets aussi différents que les cahiers de rappel présentés à l'entrée des bars et des restaurants ou l'usage des drones équipés de caméras pour surveiller le respect des mesures de confinement.

Somme toute, l'année 2020 aura mis à l'épreuve le RGPD, en faisant émerger dans le débat public de nombreux points de tension susceptibles de déplacer les perceptions et les préoccupations concernant les données personnelles et la protection de la vie privée. **La CNIL en tire plusieurs leçons.**

LA CRISE SANITAIRE A PROUVÉ LA GRANDE ROBUSTESSE DES PRINCIPES POSÉS PAR LE RGPD

En premier lieu, **le RGPD s'est révélé suffisamment souple** pour permettre aux États membres de l'Union européenne de prendre en compte la nécessité de traiter et de partager des informations dans un contexte sanitaire exceptionnel.

Concrètement, les principes traditionnels de finalité, de nécessité, de proportionnalité, de minimisation des données, de limitation de la conservation des données et de sécurité ont constitué des **éléments essentiels de la confiance** dans les traitements de données sensibles en situation d'urgence. La crise a également montré **l'intérêt des approches intégrant la vie privée dès la conception *(by design)*** que les différents porteurs de projets se sont efforcés d'intégrer dans leurs protocoles de gestion de données.

Enfin, **le rôle de la CNIL a été essentiel non seulement pour garantir la vie privée mais aussi pour accompagner les administrations et les entreprises privées.**

LE RGPD A CONTINUÉ À FAIRE SON CHEMIN AU SEIN DU GRAND PUBLIC.

Nos études récentes relèvent que **87 % des Français se déclarent sensibles à l'enjeu de protection des données** et que 68 % des Français déclarent connaître la CNIL[3]. Les personnes ont non seulement entendu parler du RGPD, mais elles connaissent aussi leurs droits et les exercent. En 2020, comme en 2019, la CNIL a reçu environ 14 000 plaintes, soit une augmentation de 62,5 % depuis la mise en œuvre du RGPD. Cette prise de conscience s'inscrit dans la durée.

3 Sondage IFOP pour la CNIL réalisé auprès d'un échantillon de 1 006 personnes représentatif de la population française âgée de 18 ans et plus, décembre 2020.

LA SOUVERAINETÉ NUMÉRIQUE A ÉTÉ UN DES SUJETS RÉCURRENTS DE 2020

Un certain nombre d'autres faits majeurs se sont produits en 2020 : **l'arrêt Schrems II** rendu par la Cour de justice de l'Union européenne, annulant le *Privacy Shield* qui encadrait le transfert de données entre l'Europe et les États-Unis ; l'engagement de l'État de transférer dans un délai de deux ans l'hébergement de la Plateforme nationale des données de santé, le ***Health Data Hub***, vers une solution technique permettant de ne pas exposer ces données sensibles à d'éventuelles demandes d'accès illégales au regard du RGPD ; les initiatives **législatives européennes** en matière de marché unique européen avec le *Digital Governance Act*, le *Digital Services Act* et le *Digital Markets Act*, prochainement suivis du *Data Act*.

Ce contexte exceptionnel offre un **alignement inédit des intérêts entre la régulation en matière de protection des données et la politique de relance industrielle**. Il est de notre responsabilité de parvenir à nous en saisir collectivement pour mener une politique ambitieuse en matière de souveraineté numérique européenne, pour laquelle le respect du RGPD sera un facteur essentiel de succès.

ENFIN, LA CNIL A DÉCLINÉ EN 2020 LES PRINCIPES DE LA RÉGULATION EN MATIÈRE DE DÉPÔT DE COOKIES

Les nouvelles lignes directrices et la recommandation d'octobre 2020 tirent les conséquences du RGPD et de la directive ePrivacy, afin d'assurer l'amélioration de l'information fournie aux internautes, ainsi qu'un consentement effectif au dépôt des cookies par les sites web. Si le travail n'est pas terminé, chacun devrait voir évoluer les interfaces communément utilisées.

En parallèle, à la fin de l'année 2020, la CNIL a prononcé **des sanctions de respectivement 100 millions d'euros et de 35 millions d'euros à l'encontre de Google et d'Amazon**, en raison de manquements aux règles relatives aux cookies. Ces sanctions, aux montants inédits en matière de protection de données à l'échelle de l'Union européenne, soulignent que les GAFAM n'échappent pas aux règles relatives à la protection des données et, d'une façon plus générale, rappellent la détermination de la CNIL à garantir que les internautes aient davantage de contrôle sur leurs données dans le quotidien de leurs pratiques numériques.

EN 2021, LA CNIL SE FIXE COMME OBJECTIF D'AMÉLIORER LA MISE EN CONFORMITÉ DE TROIS SECTEURS CLÉS

La première priorité concerne donc le **consentement aux cookies** : la CNIL poursuivra son action pour obtenir l'information requise sur les bandeaux cookies des pages d'accueil des sites internet et une réelle faculté d'être en mesure de les refuser aussi aisément qu'il est proposé de les accepter. Après un délai raisonnable de 6 mois pour se mettre en conformité, la CNIL se réserve la possibilité, depuis avril 2021, de poursuivre les manquements observés.

Le deuxième secteur prioritaire est celui de l'hébergement des données dans un **cloud souverain**. C'est la meilleure protection vis-à-vis de législations étrangères trop intrusives et cette ambition ne se limite pas aux données de santé. Nous savons que tout ne peut pas changer du jour au lendemain mais les fortes semonces de la Cour de justice de l'Union européenne doivent amener tous les acteurs concernés à agir en ce sens.

Enfin, le troisième champ prioritaire de mise en conformité est celui de la **cybersécurité**, dont le RGPD est un instrument à part entière mais encore trop méconnu. Il n'y a pas de protection des données sans cybersécurité et l'on doit continuer à faire évoluer les pratiques au service d'une société numérique de confiance.

LA CNIL RENOUVELLERA ÉGALEMENT SA STRATÉGIE D'ACCOMPAGNEMENT.

L'année 2020 a été également l'occasion pour la CNIL de poursuivre son action d'accompagnement de l'innovation, par exemple en publiant un livre blanc sur les assistants vocaux. Début 2021, la CNIL a lancé un dispositif de **« bac à sable »** consacré aux projets innovants dans le domaine de la santé numérique, dans le but de fournir un accompagnement renforcé, temporaire, à des projets particulièrement innovants et promouvoir une logique de *privacy by design*.

Un second levier de renouvellement de notre stratégie d'accompagnement sera le nouveau volet de **stratégie *startups***. Les contenus mis à disposition et les actions de communication, notamment auprès de l'incubateur Station F, seront encore élargis à de nombreux nouveaux sujets. Tels sont les principaux chantiers qui guideront l'action de la CNIL en 2021. Alors que la transition numérique s'intensifie et que la relance de l'économie française s'appuiera en partie sur les atouts du numérique, les enjeux de protection des données et de souveraineté européenne seront plus que jamais essentiels au développement durable d'une économie numérique fondée sur la confiance. La CNIL s'attachera, comme elle l'a fait en 2020, à faire respecter le droit à la vie privée tout en veillant à ce que la protection des données favorise l'innovation et soit un des marqueurs de l'action des entreprises et des administrations.

MOT DU SECRÉTAIRE GÉNÉRAL

Louis DUTHEILLET DE LAMOTHE
Secrétaire général de la CNIL

LA PROTECTION DES DONNÉES À L'ÉPREUVE DE LA CRISE SANITAIRE

Sans surprise, le bilan de l'année écoulée est marqué, pour la CNIL, par la crise sanitaire qui s'est déclenchée au premier trimestre de l'année 2020. D'une façon plus personnelle, l'année 2020 aura été celle de mon arrivée, au moment même où la maison CNIL entrait en confinement, comme toutes les administrations et les entreprises. Une façon pour le moins inhabituelle mais très forte de rencontrer cette communauté de travail remarquable que constitue la CNIL.

Du point de vue de l'accomplissement de ses missions en 2020, trois points peuvent être soulignés : la solidité de la CNIL face à cette épreuve, un baptême du feu pour le RGPD et, dans le cadre de la crise sanitaire comme au-delà, la confirmation du besoin d'allier sécurisation et responsabilisation des acteurs.

L'ADAPTATION DE LA CNIL À L'URGENCE SANITAIRE

J'ai pu constater à mon arrivée que la CNIL est une administration agile, qui s'est très rapidement adaptée au confinement puis à la poursuite des contraintes liées à la crise sanitaire. La CNIL a recouru massivement au télétravail pour ses agents et aux visioconférences pour les réunions du Collège ou du Comité européen à la protection des données. Ces modes de fonctionnement perdurent encore aujourd'hui. Je crois que nous pouvons être fiers du travail accompli dans ces circonstances très particulières.

Les chiffres rendant compte de l'activité de la CNIL, détaillés tout au long du présent rapport, témoignent de l'engagement total de ses équipes et de ses membres durant cette année. La CNIL a ainsi priorisé toutes les actions (conseil, avis, autorisation, instruction de plaintes, contrôles, etc.) en lien avec l'épidémie de COVID-19 et a traité ces dossiers dans des délais plus resserrés que jamais. Le nombre de séances plénières tenues en 2020, d'autorisations de traitements de données de santé délivrées, d'avis rendus aux pouvoirs publics concernant les outils numériques mis en œuvre pendant l'état d'urgence, par exemple, illustrent cette intense mobilisation. Dans le

même temps, la CNIL a continué d'assurer l'ensemble de ses missions. Dans le cadre du traitement des demandes d'information et de conseils comme des plaintes et réclamations, elle a maintenu son activité et a continué à œuvrer, à l'égard de l'ensemble de ses usagers, pour une meilleure protection des données personnelles.

Ainsi, la CNIL a fait front et peut, je crois, être fière de son bilan. Elle n'en a naturellement pas l'apanage : notre engagement s'inscrit dans celui de l'État et de tous les services publics.

LA CONSÉCRATION PRATIQUE DES PRINCIPES DE PROTECTION DES DONNÉES

L'année 2020 a également plongé le RGPD dans le grand bain : celui de la confrontation à une réalité tragique, impliquant des mesures impérieuses et immédiates. La plasticité des principes de protection des données, si souvent mise en avant, allait-elle résister à la crise sanitaire ? La nécessité de déployer des outils numériques pour faire face à l'épidémie devait-elle avoir pour corollaire d'affaiblir la protection de la vie privée des citoyens et résidents ? En d'autres termes, la protection des données constitue-t-elle un obstacle à la gestion d'une telle crise et, dès lors, potentiellement à la poursuite d'autres impératifs légitimes ?

Le pari a, me semble-t-il, été remporté : la crise a au contraire démontré la robustesse des principes de protection des données, à la fois protecteurs des individus et de la société dans son ensemble et ne nuisant aucunement à l'efficacité de la stratégie sanitaire. C'est heureux, car le RGPD jouait là une partie de sa crédibilité. Le respect de ces principes, notamment grâce aux nombreux avis de la CNIL, suivis de contrôles continus sur les instruments de la politique sanitaire, a également contribué à la confiance des Français dans ces outils. Ce rapport aborde largement cette question de la conciliation entre protection des données et impératifs de santé publique, mais on peut en tirer une conclusion : la crise sanitaire a mis en lumière la nécessité de garantir le respect de ces principes, et non point d'en modifier la portée.

Au-delà de la crise, le RGPD continue de déployer progressivement ses effets, par la puissante attraction de la notion de « traitement de données à caractère personnel ». C'est ainsi que les drones, les caméras thermiques ou les dispositifs de repérage de foules denses ou sans masque ont été passés en 2020 au crible des principes de protection des données personnelles. L'arrêt dit « Schrems II », du 16 juillet 2020, constitue de ce point de vue, à l'évidence, la décision la plus forte de l'année : en invalidant la décision d'adéquation liée au *Privacy Shield*, par des motifs particulièrement sévères pour la législation américaine, la Cour de justice de l'Union européenne a lancé à toute l'Europe un formidable défi qui doit être lu à la lumière de la nécessité d'augmenter notre souveraineté numérique.

MAINTENIR LE CAP POUR FAIRE DU RGPD UN SUCCÈS OPÉRATIONNEL

Dans le cadre de la gestion de la crise sanitaire comme dans les autres contextes, l'année 2020 a enfin dessiné les deux objectifs prioritaires qui s'imposent à la CNIL en vue d'une régulation efficace, pragmatique et équilibrée : il faut, d'un côté, sécuriser les acteurs et, de l'autre, les responsabiliser.

Côté pile : la sécurité juridique et la sécurité informatique.

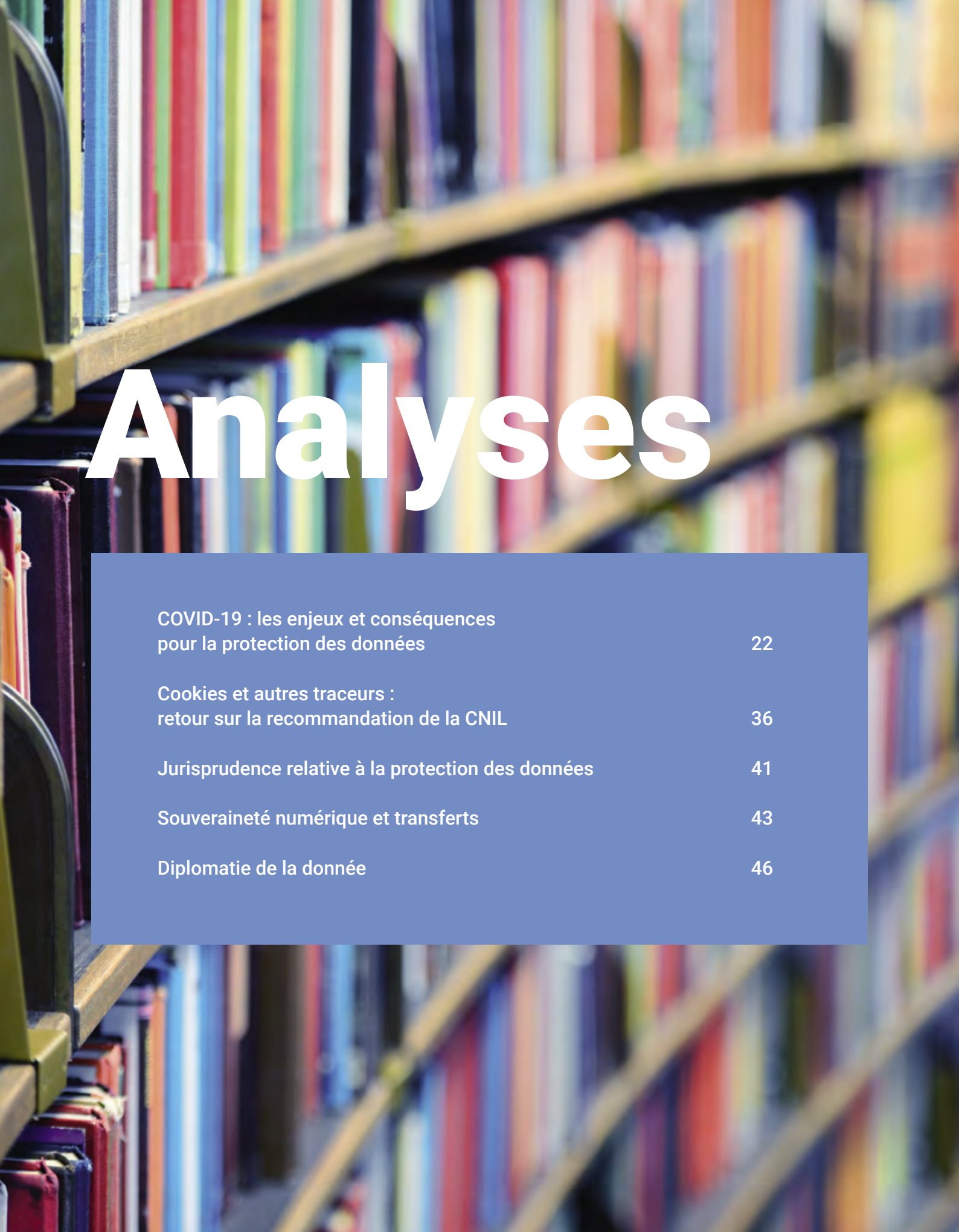
Les conséquences concrètes du RGPD restent trop souvent incertaines pour les acteurs. Il faut donc poursuivre le travail de clarification des règles et proposer des cadres sécurisants par des recommandations et des lignes directrices. C'est dans l'intérêt des responsables de traitement et c'est également la condition pour que les droits des personnes soient en pratique respectés. L'accompagnement restera ainsi une priorité pour la CNIL, sous toutes ses formes (générale sur les grandes notions, sectorielle ou individuelle avec les nouveaux outils de la conformité) et c'est pourquoi l'institution s'est récemment dotée d'une « charte d'accompagnement des professionnels ». La CNIL doit également s'inscrire dans le mouvement de développement des certifications ou autres formes de label qui permettent de transformer la contrainte réglementaire en avantage comparatif, en atout économique. Pour cela, elles doivent présenter une réelle fiabilité, ce qui ne peut se faire sans l'accompagnement du régulateur.

La CNIL est par ailleurs garante du respect des règles de sécurité informatique lorsque des données personnelles sont traitées. Elle doit continuer à agir pour une meilleure connaissance et un meilleur respect des recommandations de cybersécurité, qu'elle contribue à façonner à travers sa doctrine, l'instruction des violations de données personnelles qui lui sont signalées et ses actions répressives.

Côté face : l'effectivité des droits des personnes restera la boussole de l'action de la CNIL.

Le traitement des très nombreuses plaintes que confient les usagers à la CNIL est une mission impérieuse, afin de changer concrètement leur quotidien numérique. Une stratégie de contrôle ambitieuse y contribuera, accompagnée, le cas échéant, de mises en demeure et sanctions adaptées.

Ces deux actions se complètent et sont nécessaires l'une à l'autre : le travail de pédagogie manquera de crédibilité si les règles n'apparaissent pas effectives ; l'action correctrice et répressive de la CNIL n'est acceptable que si les obligations des responsables de traitement sont tout à fait claires.



Analyses

COVID-19 : les enjeux et conséquences pour la protection des données

Dans le contexte de la crise sanitaire, l'utilisation des technologies de communication à distance et de dispositifs de surveillance pour essayer de ralentir la propagation de la COVID-19 ou pour s'adapter aux mesures de distanciation physique n'a cessé d'augmenter. Elle a eu pour effet de placer les enjeux de protection des libertés et des données personnelles au cœur des débats publics. Face à la multitude d'initiatives, la CNIL a su mobiliser ses deux piliers, l'accompagnement et la chaîne répressive, tout en restant à l'écoute de ses publics.

L'UTILISATION DE NOUVELLES TECHNOLOGIES EN PÉRIODE DE CRISE SANITAIRE

Une intensification des pratiques numériques quotidiennes

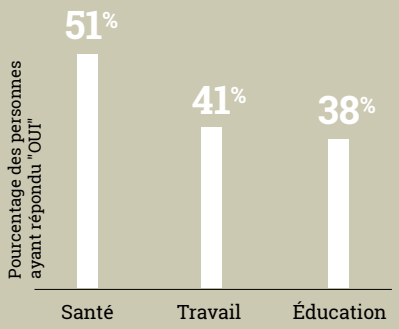
L'épidémie de la COVID-19 et les mesures de confinement et de distanciation sociale imposées à la population ont fait évoluer massivement les pratiques numériques. Certaines d'entre elles, jusqu'ici marginales ou minoritaires (télétravail, télémédecine, téléenseignement) auront connu à l'occasion du confinement une adoption et une intensification particulièrement fortes, s'introduisant ainsi dans la vie quotidienne des Français.

Par exemple, la médecine à distance a connu un essor spectaculaire. Alors que le total des téléconsultations était d'à peine 60 000 en 2019, **plus de 5,5 millions de téléconsultations ont été facturées entre mars et avril 2020 selon l'Assurance maladie**[4].

De même, le télétravail est devenu en l'espace de quelques semaines la norme pour plus d'un tiers des personnes en emploi, ainsi que l'enseignement à distance pour les élèves et les étudiants. Cette migration massive et largement non anticipée vers ces services à distance a conduit les entreprises et les institutions publiques à recourir à des solutions proposées par des acteurs de marché, sans une prise en compte systématique des enjeux de protection des données personnelles.

En effet, ce déploiement rapide vers des solutions technologiques plus ou moins maîtrisées fait craindre des défauts de conformité vis-à-vis de la collecte et du traitement des données personnelles de leurs usagers. Au-delà des problématiques en termes de sécurisation des données que le recours à de telles solutions est susceptible d'entraîner, les enjeux de surveillance ont particulièrement inquiété les personnes concernées (dispositifs de surveillance de l'activité des salariés en télétravail, télésurveillance des examens, centralisation des données de santé par des acteurs privés dans le cadre des services de médecine à distance, etc.). Afin de s'assurer du respect des droits et libertés fondamentaux des personnes, la CNIL a cherché à encadrer le recours à de telles solutions, notamment par la publication de recommandations visant à conseiller les professionnels et les particuliers dans l'utilisation de ces dispositifs.

Pendant la crise, avez-vous eu recours à des outils numériques ?[5]



L'utilisation de nouvelles technologies à des fins de gestion de l'épidémie

La gravité de la crise sanitaire a conduit tant les acteurs privés que le Gouvernement à recourir à de nombreuses solutions technologiques à des fins de gestion de l'épidémie.

L'INTRODUCTION DU « SUIVI DE CONTACTS » OU « *CONTACT TRACING* » NUMÉRIQUE

Face au déploiement mondial de dispositifs numériques de « suivi des contacts » automatisés, les autorités de protection des données européennes se sont penchées, très tôt, sur l'élaboration de recommandations communes concernant le respect, par ces solutions, des droits et libertés fondamentaux de ses utilisateurs[6].

C'est sur la base de cette grille d'analyse européenne que la CNIL a rendu plusieurs avis sur l'application TousAntiCovid (anciennement StopCovid). Elle a rappelé à plusieurs occasions la nécessité de démontrer, au cours du temps, l'utilité sanitaire du dispositif dans le cadre de la politique sanitaire globale et les garanties nécessaires à sa mise en œuvre : utilisation basée sur le volontariat des personnes, recours à la technologie Bluetooth et non à une technologie de géolocalisation, recours à des pseudonymes minimisant les possibilités d'identification des personnes concernées, etc.

La CNIL reste particulièrement attentive aux évolutions successives d'un tel dispositif qui a posé des questions inédites en matière de protection des données personnelles.

L'USAGE DES CAMÉRAS DITES « INTELLIGENTES » ET THERMIQUES

L'épidémie de la COVID-19 a conduit certains acteurs privés et publics à envisager de déployer des caméras dites « intelligentes », telles que celles destinées à **mesurer la température** ou à **détecter la présence de masques** sur la voie publique voire dans (ou aux abords) des commerces, des transports ou encore des lieux de travail.

Ces dispositifs sont susceptibles d'avoir des **conséquences importantes pour les droits et libertés des citoyens** : un développement incontrôlé présenterait le risque de généraliser un sentiment de surveillance et de créer un phénomène de banalisation de technologies intrusives susceptibles de porter atteinte au bon fonctionnement de notre société démocratique.

4 « Téléconsultation et COVID-19 : croissance spectaculaire et évolution des usages », 21 juillet 2020, ameli.fr

5 Les chiffres et graphiques présentés dans cette section sont issus d'un sondage IFOP réalisé en ligne, du 25 août au 31 août 2020, auprès d'un échantillon de 1 001 personnes, représentatif de la population française âgée de 18 ans et plus

6 « Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19 », 21 avril 2020, edpb.europa.eu

« Tous les dispositifs légalement mis en œuvre durant cette crise sanitaire doivent être considérés comme exceptionnels, temporaires, et rester proportionnés aux objectifs particuliers de cette période. »

Contrairement à certains dispositifs de captation d'images dans l'espace public, **l'usage des caméras dites « intelligentes » n'est aujourd'hui pas prévu par un texte spécifique**. La CNIL considère qu'il est nécessaire que l'utilité et l'intérêt réel de ces dispositifs soient évalués en fonction des circonstances de leur mise en œuvre et qu'un encadrement textuel adéquat est requis dès lors que des données sensibles sont traitées (la température corporelle dans le cas des caméras thermiques) ou qu'un droit d'opposition effectif ne peut pas s'appliquer, en pratique, dans l'espace public.

Ce cadre, nécessaire mais insuffisant, s'ajouterait à toutes les garanties que doivent prévoir ces éventuels dispositifs de vidéo « intelligente » au regard du RGPD : démonstration de leur nécessité et proportionnalité, durée de conservation limitée, mesures de pseudonymisation ou d'anonymisation, absence de suivi individuel, etc. Tous les dispositifs légalement mis en œuvre durant cette crise sanitaire doivent être considérés comme exceptionnels, temporaires, et rester proportionnés aux objectifs particuliers de cette période.

Face au déploiement de solutions innovantes, et sans remettre en cause les bénéfices que peut avoir l'utilisation de nouvelles technologies dans ce contexte, la CNIL rappelle que la technologie ne peut constituer la seule réponse à une crise sanitaire et que toute solution technologique pour lutter contre une épidémie doit s'inscrire dans une stratégie sanitaire globale.

FOCUS

L'avis et les contrôles de la CNIL sur les caméras thermiques

Le déploiement de caméras thermiques, qui traitent des données de santé, doit faire l'objet d'une attention toute particulière.

Leur efficacité est contestée dans la mesure où la fièvre n'est pas un symptôme systématique de la COVID-19 et peut témoigner, par exemple, d'une autre affection. Le Haut Conseil de la santé publique recommande d'ailleurs de ne pas mettre en place un dépistage de la COVID-19 par prise de température.

À moins de ne recourir à aucun traitement de données personnelles et à ne donner lieu à aucune conservation des données, un tel dispositif ne peut être mis en œuvre au regard du RGPD que s'il y a un consentement des personnes.

LES CONTRÔLES DE LA CNIL

En 2020, l'attention de la CNIL a été attirée sur l'usage par certaines sociétés de caméras thermiques aux entrées de leurs locaux. Ces caméras ont été acquises à l'issue du premier déconfinement, afin de contrôler la température des personnes lors de leur entrée sur le site.

La CNIL a procédé à un contrôle auprès d'une société visée par plusieurs plaintes et a pu constater que le dispositif était installé de telle manière que le passage dans le champ de la caméra était rendu obligatoire.

S'agissant d'un traitement de données de santé (température corporelle), la seule base légale possible est le consentement préalable des personnes concernées. Or, la configuration du dispositif ne permettant pas l'entrée dans les lieux sans passer dans le champ de la caméra, ce consentement ne pouvait être recueilli.

La mobilisation de la CNIL pour la recherche médicale

Conformément à la loi Informatique et Libertés, les recherches dans le domaine de la santé qui ne sont pas conformes à un **référentiel ou à une méthodologie de référence** (voir encadré) doivent faire l'objet d'une autorisation de la CNIL. Ainsi, toutes les recherches qui étaient conformes à un référentiel et toutes les études internes (par exemple une équipe de soin qui utilise uniquement les données de ses patients pour un projet de recherche) ont pu être mises en œuvre sans délai par les responsables de traitement.

Selon le ministère des Solidarités et de la Santé, plus de 500 recherches impliquant la personne humaine (RIPH) liées à la COVID-19 ont été mises en œuvre

après l'obtention de l'avis favorable d'un Comité de protection des personnes ainsi que, dans certains cas, de l'autorisation de l'Agence nationale de sécurité du médicament et des produits de santé. Près de 90 % d'entre elles ont pu être mises en œuvre directement, c'est-à-dire sans avoir à constituer un dossier auprès de la CNIL, grâce aux méthodologies de référence. Ce chiffre démontre l'action de la CNIL en faveur d'une simplification des procédures, effective y compris dans un contexte de crise sanitaire.

Cependant, **près d'une centaine de demandes d'autorisation « recherche » liées à la COVID-19, impliquant ou non la personne humaine, ont été déposés à la CNIL en 2020**. Ces demandes étaient souvent justifiées par l'absence de conformité aux méthodologies de référence s'agissant :

- **des modalités d'information des patients et/ou des personnes, organes ou autorités chargés de les assister, de les représenter ou d'autoriser la recherche** (inclusion de patients en urgence sans information préalable du patient ou d'un de ses proches, information d'un seul titulaire de l'autorité parentale en cas d'inclusion d'un mineur dans un projet de recherche, ou encore dans le cadre de recherches n'impliquant pas la personne humaine, demande d'exception à la fourniture d'une information individuelle des personnes concernées), ce qui représente environ 60 % des dossiers ;
- **des destinataires des données directement identifiantes** (mise en place d'un suivi centralisé par des professionnels n'ayant pas assuré la prise en charge des patients) ;
- **de la nature des données traitées** (traitement du numéro d'inscription au répertoire des personnes physiques (NIR) aux fins d'appariement avec les données du Système national des données de santé (SNDS) ; traitement des données issues du SNDS ou des données de l'« entrepôt COVID » de la Caisse nationale de l'assurance maladie et de la Plateforme des données de santé (voir encadré).

DÉFINITIONS

Référentiels

Instruments de régulation « souple », les **référentiels** ont vocation à donner davantage de sécurité juridique aux organismes.

Élaborés en concertation avec les acteurs concernés, ces référentiels peuvent notamment actualiser les anciens cadres de références adoptés avant l'entrée en vigueur du RGPD, tels que les autorisations uniques (AU) et les actes réglementaires uniques (RU).

Un référentiel répond à deux objectifs principaux :

- guider les professionnels dans leurs démarches de mise en conformité ;
- constituer une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) si celle-ci est nécessaire.

Méthodologies de référence

La CNIL adopte également des **méthodologies de référence**, qui visent à créer un cadre protecteur des personnes concernées favorable à la recherche, à l'innovation et la compétitivité.

Lorsque le responsable de traitement réalise une recherche en conformité avec une méthodologie de référence, la demande d'autorisation auprès de la CNIL n'est pas nécessaire. Ainsi :

- Dans le cadre d'une recherche impliquant la personne humaine, seul l'avis d'un comité de protection des personnes, prévu par le code de la santé publique, doit être obtenu ;
- Dans le cadre d'une recherche n'impliquant pas la personne humaine, l'avis du CESREES (Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé) n'est pas nécessaire. En revanche, le responsable de traitement devra inscrire son traitement dans le répertoire public tenu par la Plateforme des données de santé *(Health Data Hub)*.

Un accompagnement de la CNIL dès la conception du projet

Dès février 2020, date du dépôt de la première demande d'autorisation relative à une recherche liée à la COVID-19, la CNIL a fait de l'instruction de ces dossiers **une priorité absolue et a mis en place une procédure accélérée d'instruction**.

Dans ce cadre, les responsables de traitement ont été invités à adresser aux services de la CNIL leurs dossiers, même incomplets (dans l'attente, par exemple, de l'avis du comité compétent, que ce soit un comité de protection des personnes ou le CESREES, ou de la réalisation d'une analyse d'impact relative à la protection des données). Plus d'une centaine de projets de recherche ont ainsi pu bénéficier d'un accompagnement autant juridique que technique, parfois particulièrement conséquent, afin d'être autorisés dans des délais que la CNIL a souhaité réduire au strict minimum.

Dans ces délais contraints, la CNIL s'est attachée à vérifier que les traitements de données envisagés respectaient l'ensemble des obligations prévues par le RGPD, la loi Informatique et Libertés, ainsi que le Code de la santé publique. Cette vérification concerne autant les aspects juridiques (proportionnalité, minimisation des données, respect des droits des personnes) que techniques (sécurité des données, gestion des habilitations, etc.).

Cette organisation a imposé une adaptation des méthodes de travail avec les responsables de traitement : organisation de réunions très régulières afin d'anticiper les saisines, réponses à des demandes de conseil, parfois avant même le dépôt du dossier pour pré-instruction, etc.
Cette procédure, mise en place au début de l'année 2020, demeurera pendant toute la durée de la crise sanitaire afin de **permettre aux responsables de traitement de mettre en œuvre leurs projets de recherche en lien avec la COVID-19 dans les meilleurs délais**.

> « Plus d'une centaine de projets de recherche ont ainsi pu bénéficier d'un accompagnement autant juridique que technique, parfois particulièrement conséquent, afin d'être autorisés dans des délais que la CNIL a souhaité réduire au strict minimum. »

89
autorisations de recherche sur la COVID-19 délivrées en 2020

L'adaptation de la doctrine de la CNIL

Durant la crise sanitaire, l'isolement des patients dans les établissements et l'impossibilité d'organiser des visites ont fait apparaître des questions inédites qui ont conduit la CNIL à élaborer des solutions conciliant le besoin de mise en œuvre rapide des projets de recherche et la préservation des droits des personnes concernées.

QUELQUES CAS CONCRETS :

- Saisie de plusieurs projets liés à la COVID-19 visant à réutiliser les données des dossiers médicaux de patients n'étant alors pas en état d'être informés, la CNIL a admis qu'elles puissent être utilisées à des fins de recherche. En contrepartie, les responsables de traitement se sont engagés à transmettre au patient, dès que son état le permettrait, une note d'information individuelle de « poursuite de participation » faisant état de son droit d'opposition, et à effacer les données traitées si le patient ne souhaitait pas participer à l'étude.

- S'agissant de la participation de mineurs à des projets de recherche (en dehors des recherches interventionnelles comportant une intervention non justifiée par la prise en charge habituelle), la CNIL a admis, compte tenu du confinement, que l'information soit délivrée à un seul des titulaires de l'autorité parentale s'il était impossible d'informer le second titulaire ou s'il ne pouvait être consulté dans des délais compatibles avec la réalisation de la recherche, au regard de ses finalités. Les responsables de traitement concernés se sont engagés à prévoir une note d'information destinée au second titulaire de l'autorité parentale transmise par l'intermédiaire de l'autre parent ou directement envoyée par le responsable de traitement.

- Concernant les notes d'information liées aux projets de recherche, pour des questions de confidentialité, la CNIL a admis leur envoi par courriel lorsqu'elles ne révèlent aucune information sur l'état de santé, réel ou supposé, des participants à l'étude. Dans l'hypothèse où elles révéleraient de telles informations, elles peuvent être transmises aux participants de façon chiffrée ou téléchargées via un site web à condition qu'elles soient protégées par un mot de passe transmis grâce à un canal de communication distinct tel qu'un SMS.

FOCUS

L'entrepôt COVID

Les entrepôts de données sont créés principalement pour collecter et disposer de données massives (données relatives à la prise en charge médicale du patient, données socio-démographiques, données issues de précédentes recherches etc.).

Ces données sont **ensuite réutilisées**, principalement à des fins d'études, de recherches et d'évaluations dans le domaine de la santé.
Dans le cadre de la crise sanitaire, un entrepôt de données, l'« entrepôt COVID », a été créé par la CNAM et la Plateforme des données de santé, cette dernière ayant été mise en œuvre de manière anticipée (voir page 45).

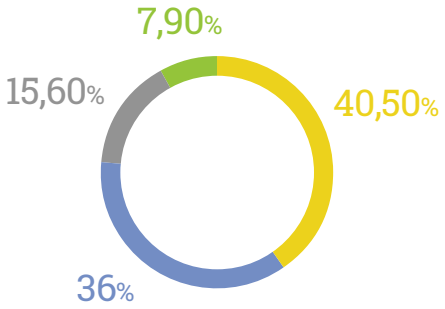
Le traitement des dossiers liés à la COVID-19

21%
DES DOSSIERS TRAITÉS LE JOUR MÊME

45%
EN MOINS DE DEUX JOURS

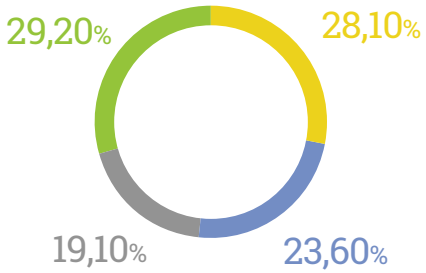
63%
EN MOINS D'UNE SEMAINE

Qui a déposé les dossiers ?



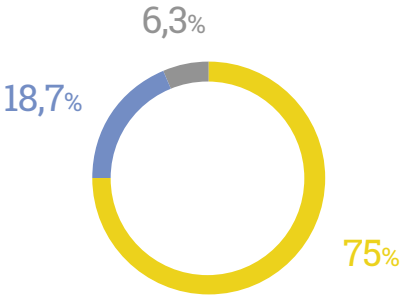
- Universités publiques et CHU (hors APHP)
- APHP
- INSERM
- Autres (organismes privés, bureaux d'études...)

Quels types d'études ont été autorisés ?



- Recherches impliquant la personne humaine de catégorie 1 (risque médical élevé)
- Recherches impliquant la personne humaine de catégorie 2 (risque médical minime)
- Recherches impliquant la personne humaine de catégorie 3 (aucun risque médical - recherches observationnelles)
- Recherches n'impliquant pas la personne humaine

Où sont hébergées les études impliquant un traitement de données du Système national des données de santé ?



- Hébergement sur le portail de la CNAM
- Hébergement via la solution technique de la Plateforme des données de santé
- Hébergement via un système fils du responsable de traitement ou du laboratoire de recherche / bureau d'études

Les mutations dans le monde du travail

Percuté par la crise sanitaire liée à la pandémie de COVID-19, le monde du travail a subi de profondes mutations dans tous les secteurs d'activités. Les entreprises et les administrations ont dû s'adapter et trouver un équilibre pour garantir la sécurité des salariés tout en assurant la continuité de leurs activités. Tout au long de l'année, la CNIL a veillé à accompagner ces acteurs en répondant à leurs sollicitations et en les informant sur leurs obligations et sur les droits des personnes.

Le renforcement des mesures de prévention et de protection du personnel

La crise sanitaire a nécessité la mise en place de mesures de sécurité renforcées au sein des entreprises pour limiter les risques de propagation du virus. Dans ce contexte, la CNIL a reçu de nombreuses sollicitations de la part des professionnels et des particuliers sur les possibilités de collecter, en dehors de toute prise en charge médicale, des données concernant des employés ou des visiteurs afin de détecter ou de retracer des cas de contamination à la COVID-19. Si l'employeur est bien soumis à une obligation de sécurité à l'égard de ses salariés, celle-ci possède ses propres limites que la CNIL a rappelées[7].

L'OBLIGATION DE SÉCURITÉ DE L'EMPLOYEUR ET DU SALARIÉ

Conformément au Code du travail, les employeurs sont responsables de la santé et de la sécurité de leurs employés. Comme l'a rappelé la Cour de cassation, il s'agit d'une **obligation de moyens renforcée** qui doit se limiter à l'élaboration et à la mise en œuvre de mesures de prévention telles que le rappel des gestes barrières, la mise à disposition de masques et de gel hydroalcoolique ou encore le traitement des signalements des cas de contamination qui sont adressés aux employeurs.

Les employés sont également soumis à une obligation de sécurité puisqu'ils doivent veiller à préserver leur propre santé ainsi que celle des personnes avec qui ils pourraient être en contact à l'occasion de leur activité professionnelle. Cette obligation est renforcée dans le contexte de la crise sanitaire : habituellement, un employé malade ne doit communiquer à son employeur que l'éventuel arrêt de maladie dont il pourrait bénéficier, sans aucune autre précision sur son état de santé ou sa pathologie. **Dans le cas précis d'une contamination ou d'une exposition à la COVID-19, un employé doit en informer son employeur à chaque fois qu'il a pu exposer une partie de ses collègues au virus**. Ces obligations ne doivent néanmoins pas être perçues comme un blanc-seing pour collecter d'autres données relatives à la santé des salariés.

LE TRAITEMENT DES DONNÉES DE SANTÉ DES SALARIÉS

De nombreux projets se sont développés au sein des entreprises pour lutter contre la propagation du virus. De la diffusion de questionnaires sur l'état de santé des salariés à la mise en place de caméras thermiques, les employeurs ont multiplié les solutions pour limiter le risque d'exposition des salariés à la COVID-19 sur leur lieu de travail.

Si les employeurs ont le droit de traiter des données personnelles pour répondre à leur obligation de sécurité, **les données collectées doivent être strictement nécessaires à la réalisation de cet objectif**. Ainsi, les employeurs ne peuvent pas prendre des mesures susceptibles de porter une atteinte disproportionnée à la vie privée de leurs salariés, notamment en collectant des données de santé, pour la gestion des suspicions d'exposition au virus. **Il n'est donc pas possible, pour l'employeur, de collecter des informations relatives à des symptômes, d'établir un diagnostic ou d'effectuer toute autre analyse médicale sur ses salariés**. L'employeur qui souhaiterait aller au-delà de ses obligations en s'assurant de l'état de santé de ses salariés **doit nécessairement s'appuyer sur le service de santé au travail, seul compétent en la matière**.

Vers une nouvelle organisation du travail

Le recours accru au télétravail illustre parfaitement les mutations subies par le monde du travail en 2020. Si la jurisprudence avait précédemment reconnu le droit à la vie privée du salarié sur son lieu de travail, le télétravail contribue à la tendance, initiée depuis quelques années, à flouter les frontières entre la vie professionnelle et la vie privée des salariés.

LE DROIT À LA VIE PRIVÉE DES SALARIÉS SUR LEUR LIEU DE TRAVAIL

Dans son arrêt fondateur de 2001, l'arrêt Nikon, la Cour de cassation avait jugé que **le salarié dispose sur son lieu de travail d'un droit au respect de sa vie privée**. Si ce droit doit, en tout état de cause, rester résiduel, la jurisprudence a progressivement dessiné les contours de cette garantie en protégeant les dossiers et les correspondances personnelles des salariés. La règle est simple : **l'employeur ne peut accéder librement aux correspondances privées du salarié dès lors qu'elles sont identifiées comme étant personnelles**. À l'inverse, cette reconnaissance du droit à la vie privée du salarié sur son lieu de travail a consacré la présence de la vie personnelle dans la vie professionnelle des salariés.

LES RISQUES D'INTRUSION DANS LA VIE PERSONNELLE DES SALARIÉS

Le confinement et le recours accru au télétravail ont entraîné une intrusion de la vie professionnelle dans la vie personnelle des salariés. Face à ce changement de modèle, de nombreuses entreprises ont sollicité la CNIL sur les modalités d'organisation du travail à distance et sur les possibilités de contrôle de l'employeur sur ses salariés.

7 « Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs », 23 septembre 2020, cnil.fr

INFOSPLUS

Les mutations dans le monde du travail dues à la pandémie de COVID-19 ne doivent pas faire perdre de vue le respect des règles de protection des données qui sont un facteur de transparence et de confiance dans les relations entre l'employeur et ses salariés.

Le télétravail constitue une modalité de l'organisation du travail. En temps normal, celui-ci doit avant tout résulter d'une négociation entre les différentes parties prenantes au sein de l'organisme. C'est cet accord collectif qui détermine les conditions de l'exercice du télétravail (et notamment la question des outils). Un nouvel « accord national interprofessionnel pour une mise en œuvre réussie du télétravail » a d'ailleurs été signé par les partenaires sociaux le 26 novembre 2020.

Concernant le pouvoir de contrôle de l'employeur, il faut rappeler que celui-ci n'est pas illégitime puisqu'il s'agit d'une contrepartie naturelle du contrat de travail. Néanmoins, **il ne peut pas être sans limites**. La mise en place de dispositifs de contrôle de l'activité des salariés doit en effet répondre à **un principe de proportionnalité**. Ainsi, l'employeur doit pouvoir justifier que les dispositifs mis en œuvre sont strictement proportionnés à l'objectif poursuivi et ne portent pas une atteinte excessive aux droits et libertés des salariés, en particulier au droit au respect de leur vie privée.

Par conséquent, **ces derniers ne peuvent être placés sous surveillance permanente**, sauf dans des cas exceptionnels qui seraient justifiés par la nature de la tâche à accomplir. Aussi, la surveillance constante aux moyens de dispositifs vidéo (tels qu'une webcam) ou audio, le partage permanent d'écran ou encore l'enregistrement de frappe (« *keyloggers* ») sont des dispositifs particulièrement excessifs et attentatoires à la vie privée : leur utilisation doit donc être, en principe, interdite.

Enfin, le Code du travail et le RGPD imposent à l'employeur **une obligation de loyauté** qui lui commande d'œuvrer avec transparence et d'informer les salariés avant la mise en place de tout dispositif de contrôle.

Ces règles impliquent une réflexion profonde sur les méthodes d'évaluation du travail des salariés et la pratique du management en télétravail. Le télétravail doit en effet être perçu comme une opportunité et non comme une technologie néfaste pour l'activité de l'entreprise.

FOCUS

Un évènement pour comprendre les mutations dans le monde du travail

À l'occasion d'**air2020**, un colloque de réflexion éthique organisé le 9 novembre 2020, la CNIL s'est penchée sur les nouveaux rapports qui lient le travail aux technologies afin d'en saisir les logiques et les enjeux.
À la croisée des expériences sur le terrain et des expertises scientifiques, l'évènement a réuni virtuellement plus de 600 participants autour de trois axes majeurs :

1. Le **rôle de l'intelligence artificielle** sur le marché de l'emploi, et ses enjeux pour le repérage des talents ou encore les biais discriminatoires à l'embauche.

2. Le **management par la donnée** en temps réel et automatisé pour mesurer et optimiser la productivité des travailleurs (ou *people analytics*), et ses limites.

3. Le **retour d'expérience sur l'essor massif du télétravail** pendant la crise sanitaire, ayant provoqué une évolution de la culture d'entreprise et de nouvelles questions sur la vie privée des salariés.

Pour en savoir plus sur cet évènement, voir page 109.

L'accompagnement de l'État et des collectivités

La CNIL a veillé à accompagner tant l'État que les collectivités territoriales dans leurs traitements de données personnelles sur des sujets aussi divers que le contrôle du respect du confinement, l'utilisation de fichiers comme les registres d'alerte des populations ou encore la continuité pédagogique. L'année aura également été marquée par un investissement important de la CNIL pour accompagner l'État dans la mise en œuvre de dispositifs de lutte contre l'épidémie.

DÉFINITIONS

SI-DEP

Le fichier SI-DEP est un système d'information national mis en œuvre par le ministère des Solidarités et de la Santé qui permet la centralisation des résultats des tests au SARS-CoV-2 réalisés par des laboratoires publics ou privés et certains professionnels de santé habilités.

Contact Covid

Le traitement Contact Covid, mis en œuvre par la Caisse nationale d'assurance maladie (CNAM), recueille des informations sur les cas contact et les chaînes de contamination. Il vise à détecter les cas contacts à trois niveaux différents, médecins de ville/établissements de santé/centres de santé (niveau 1), personnel habilité de l'assurance maladie (niveau 2), Agence régionale de santé (ARS) (niveau 3).

Les dispositifs de lutte contre l'épidémie

La CNIL s'est fortement mobilisée pour répondre aux demandes d'avis du Gouvernement. Elle a ainsi réduit ses délais d'instruction, sans pour autant faire de compromis sur ses missions, de façon à ce que les traitements déployés dans le cadre de lutte contre la COVID-19 soient bien respectueux des droits et libertés des personnes.

L'EXAMEN PAR LA CNIL DES SYSTÈMES D'INFORMATION SI-DEP ET CONTACT COVID

SI-DEP et Contact Covid ont été créés en application de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions. La CNIL s'est prononcée le 8 mai 2020 sur le projet de texte encadrant leur fonctionnement.

Compte tenu de la sensibilité des données et de l'ampleur des traitements, la CNIL a été particulièrement vigilante quant à la mise en œuvre, dans l'urgence, de ces deux systèmes d'information.

Elle a ainsi été attentive aux modalités d'information des personnes et d'exercice de leurs droits, au respect du principe de minimisation des données, à l'encadrement de la dérogation au principe du secret professionnel, en exigeant notamment une gestion particulièrement fine des habilitations des personnes amenées à accéder aux données et une sensibilisation spécifique à ces questions, et au respect de mesures de sécurité extrêmement élevées.

Le décret du 12 mai 2020 relatif à ces systèmes d'information est ensuite venu détailler leur mise en œuvre. Ce décret a été modifié à plusieurs reprises, afin d'adapter les dispositifs à l'évolution de la situation sanitaire. Chaque projet de décret modificatif a fait l'objet d'un avis de la CNIL.

STOPCOVID (TOUSANTICOVID) : LA PREMIÈRE APPLICATION DE TRAÇAGE DES CAS CONTACTS

Développée lors du premier confinement, l'application mobile StopCovid (puis TousAntiCovid) aura fait l'objet de plusieurs avis de la CNIL en 2020.

Le premier, adopté le 24 avril 2020, portait sur l'éventuelle mise en œuvre de StopCovid. À ce stade, le déploiement de cette application et ses modalités exactes de mise en œuvre n'étaient pas encore arrêtés. Dans son avis, la CNIL insistait sur la nécessité de démontrer que l'utilité de l'application pour la gestion de crise soit suffisamment avérée et que les garanties appropriées soient apportées : recours à des données pseudonymisées, sécurité, limitation du dispositif dans le temps, durée de conservation limitée des données etc. Dans ce même avis, elle accueillait favorablement le caractère volontaire de l'utilisation de StopCovid et demandait qu'aucune conséquence négative ne puisse être attachée au choix de ne pas y recourir (pas de différence pour l'accès aux tests et soins, ou pour l'accès à certains services).

Suivant la recommandation de la CNIL de disposer d'un fondement juridique explicite et précis dans le droit national, sur lequel elle serait préalablement consultée, le ministère en charge de la Santé a saisi la CNIL d'une demande d'avis concernant un projet de décret relatif à StopCovid.

Cette nouvelle saisine a permis à la CNIL de constater que les principales recommandations formulées dans son précédent avis avaient été prises en compte. Dans ce deuxième avis du 25 mai 2020, la CNIL a estimé que l'application pouvait être légalement déployée dès lors qu'elle apparaît être un instrument complémentaire du dispositif de suivi des contacts manuels et qu'elle permet des alertes plus rapides en cas de contact avec une personne contaminée, y compris pour des contacts avec des personnes inconnues. La CNIL a cependant mis en avant la nécessité d'évaluer l'impact effectif du dispositif sur la stratégie sanitaire globale afin de s'assurer de son utilité au cours du temps et a formulé plusieurs recommandations parmi lesquelles, l'opportunité de développer une technologie alternative à celle utilisée

24 avril 2020
Avis de la CNIL sur le projet d'application mobile StopCovid

25 mai 2020
Avis de la CNIL sur les conditions de mise en œuvre de StopCovid

15 juillet 2020
Mise en demeure du ministère des Solidarités et de la Santé à la suite de contrôles de la CNIL

3 septembre 2020
Clôture de la mise en demeure à la suite de la mise en conformité

23 octobre 2020
StopCovid devient TousAntiCovid

17 décembre 2020
La CNIL rend son avis sur les évolutions de TousAntiCovid et son dispositif d'enregistrement des visites dans certains établissements recevant du public (ERP)

pour vérifier que l'application est bien utilisée par une personne physique. En effet, le système de CAPTCHA initial était non seulement susceptible d'entraîner la collecte de données personnelles non prévues dans le décret, mais également le transfert de données hors de l'Union européenne ainsi que des opérations de lecture/écriture nécessitant un consentement de l'utilisateur.

Le 2 juin 2020, StopCovid a été déployée dans les magasins d'applications. Des vérifications ont alors été menées auprès du ministère des Solidarités et de la Santé et d'autres organismes impliqués dans sa mise en œuvre dont l'Institut national de recherche en sciences et technologies du numérique (INRIA), qui a conçu le protocole sur lequel repose l'application. Bien que les contrôles réalisés aient permis de constater que le fonctionnement de StopCovid respectait pour l'essentiel la protection des données, certains manquements aux dispositions du RGPD et de la loi Informatique et Libertés ont toutefois été constatés dans la première version de l'application. Concomitamment au contrôle de la CNIL, le ministère a rapidement déployé une deuxième version de l'application afin d'apporter des changements sur la manière dont les données sont traitées.

Au regard des manquements constatés, la présidente de la CNIL a donc mis en demeure le ministère de mettre StopCovid en conformité dans un délai d'un mois sur les points suivants :

- veiller à ce que la nouvelle version de l'application soit généralisée ;
- compléter l'information fournie aux utilisateurs de l'application sur les destinataires des données et les opérations de lecture des informations présentes sur les équipements terminaux (réalisées via la technologie reCAPTCHA) et le droit de refuser ces opérations de lecture ;
- compléter le contrat de sous-traitance conclu entre le ministère et INRIA ;
- compléter l'analyse d'impact relative à la protection des données (AIPD).

FOCUS

Les avis de la CNIL adressés au Parlement sur les fichiers en lien avec la COVID-19

Le législateur a prévu, pour les fichiers SI-DEP, Contact Covid, Vaccin Covid et TousAntiCovid, que le Gouvernement adresse au Parlement un rapport trimestriel détaillé de l'application de ces mesures, jusqu'à leur disparition. Il a également prévu que ces rapports soient complétés par un avis public de la CNIL.

Dans son premier avis du 10 septembre 2020, la CNIL a relevé que les dispositifs mis en place dans le cadre de la crise sanitaire (fichiers SI-DEP et Contact Covid, application Stopcovid) étaient, pour l'essentiel, respectueux des données personnelles et que la plupart des préconisations formulées dans ses avis avaient été prises en compte. Elle a toutefois constaté certaines mauvaises pratiques et s'est rapprochée des organismes concernés afin qu'ils se mettent en conformité dans les meilleurs délais. La CNIL a également demandé que des indicateurs soient mis en place afin d'évaluer plus précisément la contribution de ces dispositifs à la gestion de la crise sanitaire. Elle annonçait enfin une seconde phase de contrôles, dont les résultats ont été communiqués dans son second avis.

Dans ce second avis, daté du 14 janvier 2021, la CNIL a relevé que des modifications avaient été apportées aux dispositifs pour les mettre en conformité avec la législation sur la protection des données personnelles. Elle a toutefois constaté de nouvelles pratiques contraires au RGPD. Une mise en demeure a notamment été prise à l'encontre d'une Agence régionale de santé (ARS) en lien avec le système d'information Contact Covid. S'agissant de l'utilité et de l'efficacité de l'application TousAntiCovid sur la stratégie sanitaire globale, la CNIL a rappelé qu'il était indispensable de développer des initiatives et des indicateurs permettant d'évaluer pleinement l'effectivité sanitaire du dispositif dans le cadre de la lutte contre l'épidémie de COVID-19.
Une troisième phase de contrôles a débuté en janvier 2021.

FOCUS

Les cahiers de rappel

Lors du déconfinement, l'ouverture de certains établissements situés dans les zones d'alerte maximale a été conditionné au respect d'un protocole sanitaire renforcé. Il comprenait notamment la tenue d'un cahier de rappel des clients, conditionnant leur accès à l'établissement.

Ce « cahier » est destiné à collecter les coordonnées des clients présents dans le restaurant, la cafétéria ou l'établissement de restauration rapide, afin de les tenir à disposition des autorités sanitaires en cas de contamination de l'un des clients. Qu'il s'agisse d'un registre au format papier ou non (formulaire en ligne, QR code, etc.), ce « cahier » constitue un traitement de données personnelles soumis au RGPD et à la loi Informatique et Libertés.

LES CONTRÔLES DE LA CNIL

Au-delà des contrôles effectués sur TousAntiCovid, SI-DEP, Contact Covid et Vaccin Covid, la CNIL a également vérifié des fichiers du quotidien liés au suivi de la pandémie et notamment les cahiers de rappel.

Plusieurs manquements au RGPD ont été constatés, dont la réutilisation des données collectées à des fins de prospection. Les organismes concernés ayant indiqué avoir supprimé les données et ne pas les avoir utilisées à des fins commerciales, la CNIL a décidé de les rappeler à l'ordre tout en les invitant à se mettre en conformité à l'avenir dans l'hypothèse où la tenue de « cahiers de rappel » serait de nouveau nécessaire.

Les éléments de réponse apportés par le ministère au cours du mois d'août ayant permis de démontrer que les manquements constatés lors du contrôle avaient cessé, la présidente de la CNIL a décidé de procéder à la clôture de la procédure le 3 septembre 2020.

Le 22 octobre 2020, le Gouvernement a annoncé le déploiement de TousAntiCovid, en remplacement de StopCovid. Le déploiement de la nouvelle application ne nécessitait pas de saisine obligatoire de la CNIL, aucune modification substantielle touchant au traitement de données personnelles n'ayant été mise en œuvre.

L'AJOUT D'UN DISPOSITIF NUMÉRIQUE D'ENREGISTREMENT DES VISITES DANS CERTAINS ÉTABLISSEMENTS RECEVANT DU PUBLIC

Enfin, le 17 décembre 2020, la CNIL s'est prononcée sur un nouveau projet de décret modifiant le décret du 29 mai 2020 relatif à StopCovid.

L'évolution principale visait alors à introduire, au sein de l'application TousAntiCovid, une alternative numérique au cahier de rappel (voir encadré), dans la perspective de la réouverture de certains établissements recevant du public ou ERP (restaurants, salles de sport, salles de spectacles, etc.). Ce dispositif permet d'enregistrer les visites afin de faciliter l'alerte des personnes ayant fréquenté un même lieu sur une plage horaire similaire qu'une personne ultérieurement dépistée ou diagnostiquée positive à la COVID-19.

Si la CNIL a considéré que l'utilité d'un dispositif complémentaire était démontrée, elle a néanmoins précisé qu'elle n'était pas pleinement en mesure d'apprécier la proportionnalité de la collecte de données, certains éléments nécessaires à son analyse n'étant pas encore définis (liste précise des établissements recevant du public concernés, caractère obligatoire ou facultatif du dispositif pour les établissements notamment).

VACCIN COVID : OUTIL DE GESTION DE LA VACCINATION CONTRE LA COVID-19

Vaccin Covid est un système d'information comprenant des informations sur les personnes vaccinées ou invitées à l'être. Il permet d'organiser la campagne de vaccination, le suivi et l'approvisionnement en vaccins et consommables (seringues…), et la réalisation de recherches et du suivi de pharmacovigilance.

Mis en œuvre sous la responsabilité conjointe de la Direction générale de la santé (ministère des Solidarités et de la Santé) et de la CNAM, Vaccin Covid a été créé par le décret du 25 décembre 2020. La CNIL, qui s'est prononcée sur le projet de texte dans son avis du 10 décembre 2020, a été particulièrement vigilante sur la nécessité, pour le ministère, de faire preuve de la plus grande transparence, notamment en prévoyant une parfaite information des personnes concernées. Elle a également veillé au respect des droits des personnes, en préconisant de prévoir la possibilité de s'opposer au traitement de leurs données jusqu'à l'expression du consentement à l'acte vaccinal.

L'accompagnement des collectivités territoriales

Mobilisée pour accompagner les collectivités territoriales durant la crise sanitaire, la CNIL, en liaison continue avec les associations d'élus locaux et administrations centrales, s'est tenue à l'écoute des problématiques identifiées sur le terrain, lors d'initiatives prises par les décideurs publics aux fins de lutter le plus efficacement possible contre le développement et les effets de la pandémie.

Deux sujets ont, tout particulièrement, donné lieu à des appels à la vigilance et recommandations de la part de la CNIL.

INFOSPLUS

SI-DEP, Contact Covid, TousAntiCovid : les contrôles de la CNIL en 2020

La crise sanitaire a conduit à une réorientation des contrôles de la CNIL vers les traitements mis en œuvre pour lutter contre l'épidémie, afin d'en vérifier la conformité. Ces procédures, qui ont permis d'alimenter des avis de la CNIL et ont conduit, pour certaines, à l'adoption de mesures correctrices ont, en effet, représenté environ 20 % de l'activité de contrôle de la CNIL sur cette période.

25
opérations de contrôles au total ont été menées en lien avec la lutte contre la pandémie de COVID-19 entre mai et novembre 2020

6
contrôles du traitement SI-DEP

12
contrôles du traitement Contact Covid

7
contrôles de TousAntiCovid et StopCovid

LE PARTAGE DE DONNÉES ISSUES DE FICHIERS SOCIAUX ET MÉDICO-SOCIAUX ENTRE COLLECTIVITÉS

Lors du premier confinement, la CNIL a été interrogée sur la possibilité pour les départements de transmettre les données d'identification et de contact utilisées pour la gestion du revenu de solidarité active, de l'allocation personnalisée d'autonomie et de la prestation de compensation du handicap, à des communes, intercommunalités et centres communaux d'action sociale. L'objectif était de permettre à ces acteurs de proximité d'identifier les personnes en situation de vulnérabilité et de leur proposer une aide adaptée.

Au-delà de la réponse apportée, la CNIL a publié une nouvelle fiche pratique sur son site web sur les registres communaux d'alerte aux populations[8], en rappelant leur rôle et l'utilisation qui peut en être faite.

LES CONDITIONS DE MISE EN ŒUVRE DES TRAITEMENTS DE DONNÉES PERSONNELLES POUR LA DISTRIBUTION DES MASQUES

Fin avril 2020, les communes et leurs groupements devaient procéder, dans l'urgence et avec des stocks limités, à des distributions massives de masques. La CNIL a publié une fiche pratique supplémentaire[9] pour accompagner le déploiement de traitements de données dédiés à l'information des foyers sur le dispositif local envisagé, ainsi qu'à l'organisation, au contrôle et au suivi de ces opérations.

L'accompagnement du monde de l'éducation et de l'enseignement supérieur

La CNIL a très tôt été interrogée sur les outils que souhaitaient utiliser les établissements scolaires et d'enseignement supérieur pour assurer la continuité pédagogique et organiser les modalités d'examen. Le 8 avril 2020, la CNIL a publié, sur le site educnum.fr, des conseils à destination de la communauté enseignante, des parents et de 12 millions d'élèves sur les outils en ligne permettant la continuité pédagogique (voir page 54).

Sur des points plus précis, tels que la télésurveillance des examens ou l'activation de la caméra des élèves et étudiants, la CNIL a veillé à accompagner les responsables de traitement en leur rappelant leurs obligations, et à informer les étudiants de leurs droits[10].

Les réponses aux interrogations du grand public

Tout au long de l'année 2020, la CNIL a veillé à maintenir la plupart de ses canaux d'accès et a constitué, en interne, un groupe de travail dédié aux problématiques juridiques de la crise. Le traitement accéléré des demandes écrites dans tous les secteurs a également permis d'assurer la continuité du service aux usagers, particuliers et professionnels. Concernant les permanences téléphoniques, la répartition des appels en fonction des thématiques n'a pas été affectée par la crise, laissant à la permanence généraliste la grande majorité des appels (68,5 %).

En outre, si le nombre de plaintes est resté stable par rapport à 2019 (voir page 87), une quarantaine de plaintes en lien avec la COVID-19 a été déposée et instruite en urgence, conduisant la CNIL à rappeler leurs obligations à de nombreux organismes.

8 « Les registres communaux d'alerte et d'information des populations », 14 avril 2020, cnil.fr

9 « COVID-19 : les traitements de données associés aux opérations de distribution de masques », 1er mai 2020, cnil.fr

10 « Surveillance des examens en ligne : les rappels et conseils de la CNIL », 20 mai 2020, cnil.fr

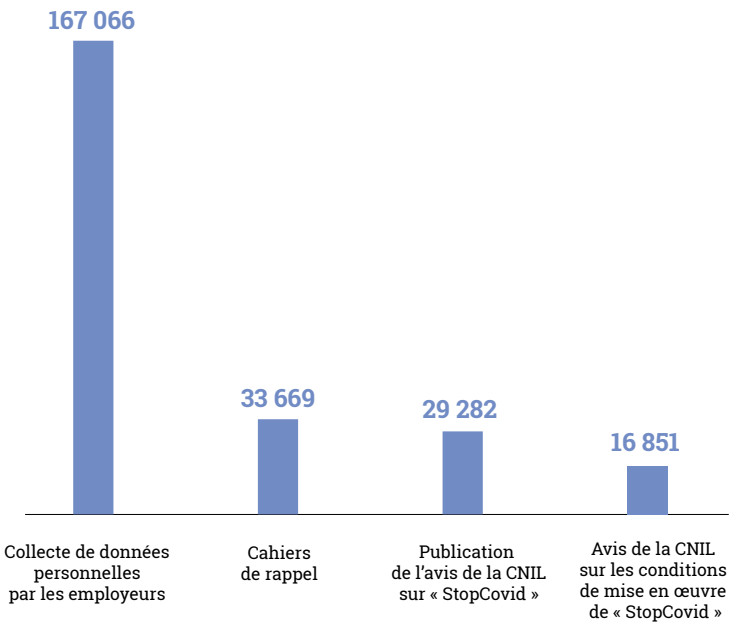
INFOSPLUS

Cnil.fr : un outil efficace pour informer et accompagner les différents publics

Tout au long de l'année, la CNIL a publié et actualisé des fiches pratiques en lien avec la COVID-19 afin de tenir compte des questions récurrentes qu'elle a reçues. Dès le début de la crise, une porte d'entrée vers ces contenus a été mise en ligne en page d'accueil cnil.fr pour en faciliter l'accès et augmenter leur visibilité.

Au total, **plus de 50 articles, communiqués et fiches pratiques ont été publiés sur cnil.fr sur de nombreux sujets en lien avec la crise**, des rappels pour les employeurs, collectivités ou chercheurs aux conseils pratiques pour le grand public (télétravail, continuité pédagogique, etc.). Ces différentes ressources ont également fait l'objet d'une communication intensive sur les réseaux sociaux.

Les 4 fiches en lien avec la COVID-19 les plus consultées en 2020



La coordination européenne

Cette année encore, le dialogue et la coordination des recommandations menés au sein du Comité européen de la protection des données (CEPD) se sont révélés extrêmement précieux pour dégager des positions communes sur des sujets aussi sensibles que les applications de suivi de contact, leur interopérabilité, le traitement des données de santé à des fins de recherche ou encore la protection des droits fondamentaux dans le cadre des mesures d'urgence prises par les États membres.

Pour faire face à la situation exceptionnelle, l'activité du CEPD s'est considérablement intensifiée, avec 27 réunions de plénières pour la seule année 2020 : habituellement mensuelles, les réunions au niveau des commissaires et présidents d'autorités sont devenues hebdomadaires au plus fort de la crise.

Cette importante mobilisation a permis au CEPD d'adopter rapidement des lignes directrices sur des sujets centraux tels que l'utilisation de données de localisation et d'outils de recherche de contact dans le contexte de la crise sanitaire ou encore sur le traitement des données de santé à des fins de recherche scientifique liée à la COVID-19. En complément de ces lignes directrices, le CEPD a également développé un guide pour fournir des orientations générales aux concepteurs et aux utilisateurs d'applications de suivi des contacts. Il a aussi fait preuve d'anticipation en adoptant une déclaration sur l'interopérabilité des applications de suivi des contacts (c'est-à-dire la capacité de ces systèmes à fonctionner entre eux), ainsi qu'une déclaration sur le traitement des données personnelles dans le cadre de la réouverture des frontières Schengen à la suite de l'épidémie. Il a invité les États membres à adopter une approche européenne commune pour décider quel traitement était nécessaire dans ce contexte et a souligné l'importance d'une consultation préalable des autorités nationales de contrôle compétentes lorsque les États membres envisageaient de traiter des données personnelles dans ces circonstances.

« La législation européenne en matière de protection des données reste d'application et permet de réagir efficacement à la pandémie, tout en protégeant les droits et libertés fondamentaux. »

À la demande de la Commission européenne, le CEPD a en outre adopté une position concernant le projet d'orientation sur les applications de soutien à la lutte contre la COVID-19. Ce document est venu compléter la recommandation de la Commission, pour la mise en place d'une boîte à outils européenne pour l'utilisation des technologies et des données dans ce contexte de crise sanitaire.

Le CEPD a également répondu à plusieurs sollicitations de députés européens qui l'interrogeaient sur ces questions.

Enfin, les autorités nationales de protection des données se sont mobilisées pour apporter une réponse coordonnée sur des questions connexes, mais qui découlaient de cette situation, comme par exemple l'organisation des processus électoraux par voie postale.

Le CEPD s'est également prononcé sur la question plus large de la protection des droits fondamentaux dans le cadre des mesures d'urgence, en adoptant une déclaration sur les droits des personnes concernées. Même en cette période exceptionnelle, il est essentiel que la protection des données personnelles soit préservée afin de contribuer au respect des valeurs fondamentales que sont la démocratie, l'état de droit et les droits fondamentaux sur lesquels l'Union est fondée.

Dans tous ses travaux, le CEPD s'est ainsi attaché à rappeler aux institutions européennes et aux États membres un élément essentiel : la législation européenne en matière de protection des données reste d'application et permet de réagir efficacement à la pandémie, tout en protégeant les droits et libertés fondamentaux.

Cookies et autres traceurs : retour sur la recommandation de la CNIL

Le 1er octobre 2020, la CNIL a adopté les lignes directrices modificatives ainsi qu'une recommandation portant sur l'usage de cookies et autres traceurs. L'évolution des règles applicables marque un tournant pour les internautes, qui pourront désormais exercer un meilleur contrôle sur les traceurs en ligne.

« Certaines fenêtres de recueil des choix actuels doivent donc être améliorées pour permettre à l'internaute de dire oui ou non, facilement et en ayant pu prendre connaissance de toutes les informations nécessaires à un choix éclairé. »

Les enjeux pour les libertés individuelles

Un sujet au cœur des usages numériques quotidiens

Chaque jour, les internautes interagissent avec une variété de sites web, d'applications et de plateformes numériques en utilisant leurs smartphones, ordinateurs, tablettes, mais également des objets connectés tels que les assistants vocaux, les jouets connectés ou encore les téléviseurs connectés. Ce faisant, leurs données personnelles peuvent être collectées grâce à des traceurs dits « cookies », mais aussi d'autres technologies similaires.

Cette collecte de données suscite de plus en plus d'inquiétudes en termes de protection des données et de la vie privée.
Tout d'abord, le profilage s'est intensifié : de nombreux acteurs sont désormais en mesure d'accumuler suffisamment d'informations pour créer des profils individuels très détaillés, en particulier grâce à la multiplication des sources de collecte. Ces profils peuvent produire, au fil du temps, une « image » complète et plus ou moins exacte des internautes, voire révéler des informations qu'ils n'auraient pas choisi d'exposer (par exemple, des données relatives aux opinions politiques inférées à partir de l'analyse de lectures sur des sites d'information).

Ensuite, ces données peuvent être traitées par un nombre considérable d'acteurs : très peu d'internautes se rendent compte que, souvent, lorsque qu'ils visitent un site web ou utilisent une application mobile, ils n'entrent pas en relation avec une seule entreprise, mais avec un grand nombre de sociétés qui vont collecter et utiliser leurs données pour des raisons dont ils ne sont pas toujours conscients (voir encadré sur l'outil Cookieviz page 39).

Donner la liberté de choix aux utilisateurs

Si la CNIL ne remet pas en cause les avantages économiques d'une telle collecte pour un nombre considérable de services en ligne, elle reste convaincue que cette pratique ne saurait exister aux dépens du droit des personnes à la protection de leurs données et de leur vie privée. **Son objectif est donc d'accroître la transparence et garantir une véritable liberté de choix aux internautes** en leur donnant davantage de contrôle sur leurs données personnelles.

Les changements pour les acteurs

Deux nouveaux outils pour accompagner les professionnels

En 2013, après concertation avec les professionnels, la CNIL adoptait une première recommandation relative aux cookies pour guider les acteurs dans la mise en œuvre des textes régissant, à l'époque, les opérations de lecture et d'écritures des cookies.

Le 25 mai 2018, l'entrée en application du RGPD est venue renforcer les exigences en matière de validité du consentement, rendant obsolète une partie de cette recommandation.

Dans le cadre de son plan d'action sur le ciblage publicitaire, la CNIL a donc entrepris d'actualiser en deux temps ses cadres de référence. Elle a ainsi publié, le 1er octobre 2020 :

- Des **lignes directrices modificatives rappelant le droit applicable**. Celles-ci ont été ajustées le 17 septembre 2020 pour tirer les conséquences de la décision rendue le 19 juin 2020 par le Conseil d'État[11].
- Une recommandation, établie à l'issue d'une concertation avec les professionnels et la société civile ainsi que d'une consultation publique. Sans être prescriptive, **la recommandation joue le rôle de guide pratique** destiné à éclairer les acteurs utilisant des traceurs sur les modalités concrètes de recueil du consentement de l'internaute.

Une évolution nécessaire des interfaces de recueil des choix de l'internaute

65 %[12]

des personnes interrogées estiment que les demandes d'autorisation de dépôt de cookies actuelles sont inefficaces

11 Conseil d'État, 10e - 9e chambres réunies, N°434684, 19 juin 2020, conseil-etat.fr

12 Enquête IFOP pour la CNIL conduite les 3 et 4 décembre 2019, « Les Français et la réglementation en matière de cookies » menée auprès d'un échantillon de 1 005 personnes représentatif de la population française âgée de 2018 ans et plus en suivant la méthode des quotas.

Il appartient aujourd'hui aux différents acteurs de faire évoluer leurs interfaces de recueil des choix de l'utilisateur en ligne avec la règlementation. Les lignes directrices et la recommandation de la CNIL ont pour ambition d'accompagner cette transition et rappellent deux règles fondamentales de protection des internautes.

La première règle est que, avant même que l'utilisateur puisse avoir l'opportunité d'accepter les cookies, le site ou l'application doit l'informer, de façon claire et synthétique, de ce à quoi ils vont servir (publicité personnalisée ou non, publicité géolocalisée, personnalisation du contenu, partage d'information avec les réseaux sociaux, etc.) et de l'ensemble des sociétés qui collectent, par ce biais, leurs données personnelles à ces fins.

La deuxième réside dans les modalités de refus offertes à l'internaute :

- La simple poursuite de la navigation n'est plus considérée comme l'expression d'un accord de l'utilisateur mais comme un refus ; aucun traceur ne pourra être déposé sur le terminal de l'utilisateur sans une action positive de sa part (case à cocher, bouton « accepter », etc.).
- L'utilisateur doit pouvoir refuser les cookies aussi facilement qu'il lui est proposé de les accepter. La CNIL estime donc que lorsqu'un seul clic est requis pour consentir au traçage tandis que plusieurs actions sont nécessaires pour « paramétrer » un refus, il y a un risque que le choix de l'internaute, désireux d'accéder rapidement au site en question, soit biaisé. Elle recommande ainsi l'utilisation d'un bouton « tout refuser » au même titre que celui permettant à l'utilisateur de « tout accepter ».

Certaines fenêtres de recueil des choix doivent donc être améliorées pour **permettre à l'internaute de dire oui ou non facilement** et en ayant pu prendre connaissance de toutes les informations nécessaires à un **choix éclairé**.

L'accompagnement de la CNIL

La CNIL a privilégié l'accompagnement des professionnels afin de permettre une mise en conformité aux règles protégeant la vie privée des internautes selon un standard robuste et durable. Ainsi, la publication des lignes directrices et de la recommandation a été accompagnée d'un dispositif comprenant la publication d'une série de contenus et d'outils pour les professionnels ainsi que l'organisation de webinaires à destination de nombreuses associations représentant une grande partie de l'économie numérique.

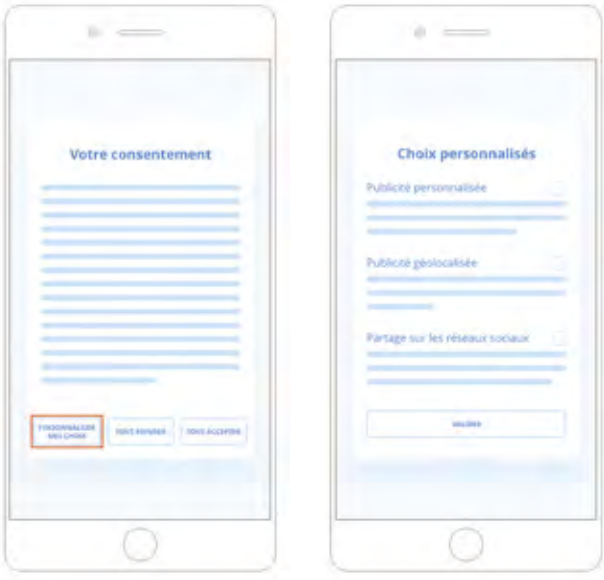
L'année 2021 permettra désormais au régulateur de contrôler le respect effectif de la règlementation applicable aux « cookies et autres traceurs ».

Des contenus pédagogiques pour le grand public

La communication autour des nouvelles lignes directrices et de la recommandation sur les cookies et autres traceurs a été, et reste aujourd'hui, un enjeu primordial pour la CNIL.

À l'instar de beaucoup de sujets traités sur son site web, la CNIL a abordé la question sous deux angles : des rap-

Exemple de fenêtre de recueil du consentement recommandée par la CNIL : le bouton « tout refuser » est au même niveau que « tout accepter », au même titre qu'un bouton permettant également de préciser ses choix.



Source : recommandation du 1er octobre 2020 sur les cookies et autres traceurs.

13 « Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation », 1er octobre 2020, cnil.fr

pels légaux aux conseils pratiques pour les professionnels – qu'ils soient responsables de traitement, DPO ou développeurs – et des contenus plus pédagogiques pour les particuliers, quel que soit leur niveau en informatique.

En ce sens, la CNIL a mis à jour de nombreuses fiches, dont certaines (« Cookies : les outils pour les maîtriser » et « Cookies et autres traceurs, que dit la loi ? ») sont les plus consultées du site web (respectivement 584 866 et 495 115 vues uniques). Au total, les fiches sur le thème des cookies cumulent environ 1 400 000 visites uniques en 2020.

Une fiche dédiée aux particuliers souhaitant comprendre les enjeux autour des cookies a également été publiée : « Évolution des règles d'utilisation des cookies : quels changements pour les internautes ? » ainsi que plusieurs vidéos :

• ***Qu'est-ce qu'un cookie ?*** donne les clés pour comprendre cette technologie.

• ***Comment j'ai attrapé un cookie ?*** présente une situation quotidienne d'achat en ligne en explicitant le rôle des traceurs.

• ***Nouvelles règles de dépôt des cookies : qu'est-ce que ça change pour vous ?*** explique, quant à elle, les changements apportés par les recommandations de la CNIL.

Toutes les fiches pratiques et vidéos de la CNIL sont disponibles sur son site web, dans la rubrique « Technologies > Site web, cookies et autres traceurs ».

Des rendez-vous réguliers ont aussi été mis en place sur les réseaux sociaux pour accompagner les acteurs qui ne seraient pas encore mis en conformité avec les nouvelles règles.

FOCUS

Cookieviz 2 : l'outil pour traquer les traceurs

La CNIL a publié la version 2.0 de son outil de visualisation qui permet de mesurer l'impact des cookies et autres traceurs lors de la navigation sur internet. Cette nouvelle version intègre de nouveaux visuels et de nouvelles fonctionnalités :

- la création d'un parcours de visite manuellement (via un navigateur intégré) ou depuis un fichier texte ;
- un support multilingue ;
- une analyse par histogramme et diagramme de Voronoï (découpage par cellules).

Disponible sur Windows, Linux et Mac, ce logiciel est également *open source* (licence GPLv3) et peut donc être enrichi par les développeurs, notamment sur GitHub : github.com/LaboCNIL/Cookieviz.
Une version 2.1 sera bientôt disponible.

Exemple d'une navigation sur quelques sites web d'information pendant une dizaine de minutes, sans accepter le dépôt de cookies.

Contrôles et mesures répressives

Les internautes sont de plus en plus attentifs aux enjeux liés à la protection de leur vie privée, notamment en raison du traçage de leurs activités et du profilage qui en résulte. Cette prise de conscience se traduit par une multiplication du nombre de plaintes adressées sur ce sujet à la CNIL. Celles-ci proviennent principalement de particuliers qui constatent, au cours de leur navigation sur le web, ne pas pouvoir exprimer correctement leurs préférences concernant le dépôt de cookies. Plusieurs associations comme None of your business (NOYB) ou Privacy International ont également saisi la CNIL.

Les problématiques soulevées par ces plaintes sont diverses : information fournie absente ou parcellaire, dépôt de cookies avant toute action sans recueil du consentement, mécanisme d'opposition insatisfaisant, etc.

Au cours de l'année 2020, sur la base des plaintes reçues et selon la nature du signalement opéré, la CNIL est intervenue de différentes manières : envoi de courriers rappelant les règles applicables et informant l'organisme de la possibilité d'un futur contrôle, questionnaire sur les faits signalés et les mesures prises pour y remédier, réalisation de contrôles (en ligne et/ou sur place) afin de constater d'éventuels manquements.

Dans certains cas particulièrement graves, lorsque des manquements à des principes en vigueur depuis la révision de la directive ePrivacy en 2009 et inchangés avec le RGPD ont été constatés, des sanctions ont été adoptées. C'est le cas des sanctions prononcées à l'encontre de Carrefour, Google et Amazon en fin d'année 2020 (voir page 100).

Si les mesures correctrices rendues publiques en 2020 ont principalement concerné deux géants du numérique, les règles sont les mêmes et s'appliquent à tous les acteurs de la même manière. Les plaintes reçues et les actions d'instruction réalisées par la CNIL au cours de l'année portent d'ailleurs sur tout type de site web et application mobile, quel que soit leur modèle économique, le volume de données traitées, ou la notoriété auprès des internautes.

En 2020, la CNIL a ainsi régulièrement pris soin d'appeler l'attention sur la nécessité, pour ceux qui ne l'auraient pas encore fait, de se mettre en conformité avec le nouveau cadre légal clarifié dans ses lignes directrices et sa recommandation publiées le 1er octobre 2020.

Une nouvelle étape, initiée le 31 mars 2021, permettra de contrôler l'application des lignes directrices modificatives et de la recommandation. En effet, la CNIL a estimé que le délai de mise en conformité aux nouvelles règles ne devait pas dépasser six mois à compter de la publication de ses nouveaux outils, soit au plus tard à la fin du premier trimestre.

INFOSPLUS

Cookies et autres traceurs : les contrôles de la CNIL en 2020

Au regard de l'évolution des recommandations de la CNIL s'agissant des « cookies et autres traceurs », **19 contrôles** sur cette thématique ont été menés en 2020, dans le cadre de **dix procédures impliquant neuf organismes différents visés par des plaintes**. Ils avaient pour périmètre : l'information des personnes, le recueil du consentement et la prise en compte de l'opposition ou du retrait du consentement.

Il a été constaté que l'information des personnes reste souvent insuffisante, la finalité des cookies n'étant souvent pas précisée. Des efforts sont néanmoins à relever, car les bandeaux d'information tendent à faire preuve de plus de transparence.

Par ailleurs, des manquements importants persistent s'agissant du recueil du consentement et de l'exercice du droit d'opposition. En effet, dans plusieurs contrôles, il a été constaté que des cookies ayant pour finalité l'affichage de publicités ciblées sont déposés dès l'arrivée de l'internaute sur le site, et ce, avant toute action de sa part. Par ailleurs, le plus souvent, les interfaces ne facilitent pas, voire ne permettent pas, de s'opposer au dépôt des cookies. Et quand tel est le cas, l'expression de la volonté de la personne n'est pas toujours suivie d'effet.

Certains de ces dossiers ont d'ores et déjà abouti à une sanction : en particulier, les sociétés Amazon et Google ont été condamnées à des sanctions respectivement de 35 et 100 millions d'euros. D'autres procédures sont en cours.

Jurisprudence relative à la protection des données

Certaines juridictions peuvent rendre des décisions qui permettent de préciser un point de droit : l'ensemble de ces décisions constitue la jurisprudence. Cette frise chronologique revient sur les principales décisions des juridictions nationales et européennes relatives à la protection des données personnelles en 2020.

13 février 2020

COUR EUROPÉENNE DES DROITS DE L'HOMME
La conservation indéfinie du profil ADN, des empreintes digitales et de la photographie d'un homme condamné pour conduite en état d'ivresse enfreint son droit au respect de la vie privée.

27 mars 2020

CONSEIL D'ÉTAT
Précisions sur la portée géographique du déréférencement des moteurs de recherche que peut ordonner la CNIL.

27 mars 2020

CONSEIL D'ÉTAT
Rejet du recours pour excès de pouvoir à l'encontre du décret « HOPSYWEB » (décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement).

11 mai 2020

CONSEIL CONSTITUTIONNEL
Censure partielle et réserves d'interprétation concernant les dispositions de la loi de prorogation de l'état d'urgence sanitaire relatives aux traitements de données de nature médicale mis en œuvre aux fins de traçage des personnes atteintes par la COVID-19 et leurs contacts.

18 mai 2020

CONSEIL D'ÉTAT
Le juge des référés ordonne à l'État de cesser immédiatement la surveillance par drone du respect des règles sanitaires.

20 mai 2020

CONSEIL CONSTITUTIONNEL
Censure partielle des dispositions organisant l'exercice du droit de communication de la HADOPI, et notamment l'accès à des données de connexion des internautes.

19 juin 2020

CONSEIL D'ÉTAT
Validation de la sanction de 50 millions d'euros infligée à Google par la CNIL.

19 juin 2020

CONSEIL D'ÉTAT
Annulation partielle des lignes directrices de la CNIL relatives aux cookies et autres traceurs (annulation de l'interdiction générale et absolue des *« cookies walls »* et validation des autres dispositions des lignes directrices).

16 juillet 2020

COUR DE JUSTICE DE L'UNION EUROPÉENNE
Invalidation de la décision d'adéquation du niveau de protection assurée par le bouclier de protection des données UE-États-Unis.

6 octobre 2020

COUR DE JUSTICE DE L'UNION EUROPÉENNE
Dans deux décisions jointes, la Cour précise sa jurisprudence relative à la conservation et à la transmission des données relatives au trafic et à la localisation à des fins de lutte contre les infractions ou de sauvegarde de la sécurité nationale.

13 octobre 2020

COUR DE CASSATION
Le code de déverrouillage d'un téléphone portable peut constituer, sous certaines conditions, une convention secrète de déchiffrement d'un moyen de cryptologie au sens des dispositions légales.

14 octobre 2020

CONSEIL D'ÉTAT
Le juge des référés ordonne à l'État de mettre en œuvre des précautions supplémentaires dans la mise en œuvre du *Health Data Hub*, dans l'attente d'une solution pérenne permettant d'éliminer tout risque d'accès aux données qui y figurent par les autorités américaines.

28 octobre 2020

COUR DE CASSATION
Les prélèvements génétiques et prises d'empreintes digitales prévus par le code de procédure pénale, ainsi que les sanctions prévues en cas de refus, ne constituent pas une ingérence excessive dans le droit au respect de la vie privée ; la relaxe de l'infraction à l'occasion de laquelle le prélèvement ou relevé a été effectué n'est pas contradictoire avec la condamnation pour refus de se soumettre à ces opérations.

4 novembre 2020

CONSEIL D'ÉTAT
Validation du décret « ALICEM » à la suite du rejet du recours pour excès de pouvoir (décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile »).

8 décembre 2020

COUR DE CASSATION
Le procureur de la République peut légalement faire procéder à une vidéosurveillance sur la voie publique, sous son contrôle effectif et selon les modalités qu'il autorise, aux fins de rechercher la preuve des infractions à la loi pénale.

10 décembre 2020

CONSEIL D'ÉTAT
Validation de la recommandation de la CNIL concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance.

22 décembre 2020

CONSEIL D'ÉTAT
Interdiction d'utiliser les drones pour la surveillance de manifestations sur la voie publique par la préfecture de police de Paris.

Souveraineté numérique et transferts

L'année 2020 a été marquée par des décisions d'envergure et une réémergence des questions de transferts de données, mais aussi de souveraineté numérique et de condition d'accès aux données.

Transfert de données vers les États-Unis : retour sur l'invalidation du *Privacy Shield*

Le *Privacy Shield* (« bouclier de protection des données » en français) était une décision d'adéquation adoptée par la Commission européenne en 2016 qui reconnaissait un dispositif américain institué pour les entreprises américaines volontaires comme fournissant un niveau de protection adéquat aux données transférées aux États-Unis ; il permettait le transfert de données entre l'Union européenne et les opérateurs américains adhérant à ses principes de protection des données, sans formalités supplémentaires. Le *Privacy Shield* avait été adopté à la suite de l'invalidation, par la Cour de justice de l'Union européenne en 2015, d'une décision qui reconnaissait un mécanisme à l'objectif similaire, le *Safe Harbor*.

Le *Privacy Shield* reposait sur un mécanisme d'auto-certification : pour bénéficier du bouclier et ainsi recevoir des données provenant de l'Union européenne, les opérateurs américains devaient d'abord adhérer à ce système auprès du ministère américain du commerce et accepter de se soumettre à diverses obligations. La certification était accordée par le ministère pour une durée d'un an, renouvelable.

La décision d'adéquation reconnaissant ce mécanisme comme assurant un niveau de protection adéquat a été invalidée le 16 juillet 2020 par la CJUE (affaire dite « Schrems II »), mettant par conséquent fin aux transferts fondés sur cette décision. La Cour s'est également prononcée sur les clauses contractuelles types (CCT) développées par la Commission européenne pour encadrer les transferts vers des pays hors de l'UE. Elle les a considérés valides d'une manière générale mais a exigé que des garanties supplémentaires soient mises en place dans le cadre de leur utilisation concrète lorsqu'il apparaît, au terme d'une évaluation, que le niveau de protection garanti par le pays tiers pour le transfert en cause ne permet pas de respecter les engagements des CCT. Il s'agit d'une décision majeure sur la question des transferts dont les autorités européennes de protection des données et la CNIL se sont emparées afin d'en tirer toutes les conséquences.

Cet arrêt a constitué un véritable tournant pour la question des transferts de données.

Cette décision est la conséquence des plaintes déposées par Maximillian Schrems, auprès de l'autorité de protection des données irlandaise, à l'encontre du réseau social Facebook et visant à faire interdire les transferts de données de l'Europe vers les États-Unis.

L'invalidation résulte des exigences du droit américain, en particulier dans le cadre de programmes de renseignement permettant l'accès des autorités américaines aux données personnelles transférées de l'UE, y compris lors du transit de ces données entre l'UE et les États-Unis. La CJUE a également mis en évidence que les conditions d'accès à ces données ont lieu sans limitation suffisante et que les personnes concernées ne se voient pas accorder des droits de recours devant les juridictions contre les autorités américaines.

L'ensemble formé par les mesures supplémentaires et les CCT, après une analyse au cas par cas des circonstances entourant le transfert, devra garantir que la législation du pays tiers applicable au transfert (par exemple de la législation américaine) ne compromet pas le niveau de protection adéquat que les clauses et ces mesures garantissent.

Les actions du Comité européen de la protection des données (CEPD)

Face à l'ampleur des conséquences d'une telle décision, qui concerne toutes les situations de transfert en dehors des dérogations, qu'ils soient vers les États-Unis ou vers un autre pays tiers à l'Union, le CEPD a adopté dès le mois de juillet une déclaration sur l'arrêt, puis offert des premiers éléments de réponse dans une FAQ publiée sur son site.

Le CEPD a ensuite adopté une recommandation sur les mesures supplémentaires destinées à compléter les outils de transfert lorsque cela est nécessaire pour assurer le respect du niveau de protection des données personnelles dans l'UE. La recommandation a été soumise à la consultation publique en vue de l'adoption d'une version finale en 2021.

Enfin, le CEPD a mis à jour son document sur les quatre garanties européennes essentielles en matière de surveillance[14]. L'objectif est de guider les acteurs, avant d'envisager des transferts de données, dans leur analyse de la législation du pays tiers en cas de risque d'accès par un gouvernement étranger aux fins de surveillance.

Une *task force* dédiée au sein de la CNIL

Pour mener l'analyse concrète et détaillée des conséquences de l'arrêt Schrems II, la CNIL a également institué une *task force* interne qui se réunit très régulièrement pour élaborer différents outils à destination du public ou à usage interne.

Ainsi, des éléments pratiques sont en cours d'élaboration et ont vocation à être publiés prochainement sur le site de la CNIL. Cette *task force* a également pour objectif de préparer les travaux européens sur le sujet, notamment dans le cadre de l'examen des 101 plaintes déposées par l'association None of your business (NOYB) à la suite de l'arrêt de la CJUE et qui concernent les transferts réalisés par diverses entreprises en Europe vers les États-Unis dans le cadre du recours aux solutions de Google et Facebook.

14 Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance adoptées le 10 novembre 2020, edpb.europa.eu

Plateforme des données de santé : entre nécessité sanitaire et risques pour les personnes

Le contexte

La Plateforme des données de santé (PDS), ou *Health Data Hub (HDH)* en anglais, est une infrastructure officiellement créée le 30 novembre 2019 destinée à **faciliter le partage des données de santé** issues de sources très variées afin de favoriser la recherche. Elle a été mise en œuvre de façon anticipée en avril 2020 pour les besoins de la gestion de l'urgence sanitaire et l'amélioration des connaissances sur la COVID-19.

Dans ce cadre, la Caisse nationale de l'assurance maladie et la PDS ont été autorisées à regrouper, au sein d'un « entrepôt COVID », certaines données personnelles comprenant des données de santé. Cet entrepôt permet l'utilisation de ces données pour suivre et projeter les évolutions de l'épidémie, prévenir, diagnostiquer et traiter au mieux la pathologie, et organiser le système de santé en conséquence.

Dans son avis sur l'arrêté créant cet « entrepôt COVID », la CNIL avait notamment attiré l'attention sur :

- les risques liés à un démarrage anticipé dans un contexte où le HDH a dû accomplir en quelques semaines des opérations structurantes pour garantir la sécurité des données traitées ;
- les éventuels risques matériels et juridiques en matière d'accès direct par les autorités de pays tiers.

Les risques liés au transfert de données de santé aux États-Unis

En effet, la PDS a décidé de recourir aux services de Microsoft, dont le siège est situé aux États-Unis, afin d'héberger les données de santé (service AZURE dit de *cloud computing*). Ce choix appelle cependant une vigilance particulière à la suite de l'arrêt dit « Schrems II » (voir pages précédentes).

Concrètement, en raison de la sensibilité et du volume des données ayant vocation à être hébergées au sein de la PDS, pour lesquelles les niveaux élevés de protection technique mais aussi juridique sont requis, la CNIL a fait part de son souhait que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne.

Dans ce contexte, la CNIL a également accueilli favorablement les déclarations du secrétaire d'État au numérique qui a indiqué, le 8 octobre 2020 devant le Sénat, la volonté du Gouvernement d'héberger la Plateforme des données de santé dans des infrastructures françaises ou européennes.

Si des garanties permettant de conclure à l'absence de transferts de données hors UE dans le cadre du fonctionnement courant de la solution technique ont bien été apportées, le Conseil d'État a cependant reconnu, le 13 octobre 2020, l'existence d'un risque de transfert vers les États-Unis du fait même de la soumission de Microsoft au droit étatsunien. Il a ainsi demandé des garanties supplémentaires.

Partageant cette inquiétude, la CNIL a réclamé et obtenu de nouvelles garanties du ministère des Solidarités et de la Santé quant à un changement de solution technique dans un délai déterminé. Le ministère s'est engagé à recourir à une solution permettant de ne pas exposer les données hébergées par le HDH à d'éventuelles demandes d'accès illégales au regard du RGPD dans un délai compris entre 12 et 18 mois et, en tout état de cause, ne dépassant pas deux ans.

Pour la CNIL, ce délai permet un juste équilibre entre la préservation du droit à la protection des données personnelles et l'objectif de favoriser la recherche et l'innovation dans le domaine de la santé. Elle estime que le risque inhérent au recours à un hébergeur soumis au droit étatsunien est admissible pendant cette période transitoire, en tenant compte des objectifs d'intérêt général poursuivis par le développement du HDH.

Dans ce contexte, quatre nouveaux projets pilotes ont été autorisés ainsi que trois projets liés à la COVID-19.

Ces enjeux mettent en lumière des problématiques de plus en plus prégnantes relatives au contrôle des flux de données au niveau international, à l'accès aux données sensibles ou stratégiques par les autorités de pays tiers, mais aussi à l'autonomie et la souveraineté numérique de l'Union européenne et de ses États membres.

Diplomatie de la donnée

La CNIL est pleinement investie dans les procédures de coopération européenne. Du point de vue de la diplomatie de la donnée, l'année 2020 aura été marquée par deux évènements inédits : le premier recours au mécanisme de résolution des différends par le CEPD et la gestion des relations avec l'autorité britannique de protection des données dans le cadre du Brexit.

La coopération européenne sur les plaintes, contrôles et sanctions

Cette année encore, la coopération européenne s'est amplifiée et les mécanismes de coopération européens font désormais partie intégrante de l'activité de la CNIL. Ces échanges permettent d'aboutir à des clarifications et harmonisations de positions entre autorités de protection des données au sein de l'UE mais aussi à la résolution de centaines de situations individuelles faisant l'objet de plaintes.

En pratique, lorsque la CNIL reçoit une plainte qui porte sur un traitement transfrontalier (mis en œuvre par un organisme établi dans plusieurs États membres ou ayant des conséquences sur des personnes dans plusieurs États membres), elle peut prendre contact avec l'organisme concerné pour s'assurer du caractère transfrontalier, identifier l'établissement principal au sein de l'Union européenne et demander davantage d'informations sur le cas en cause (procédure dite de « *preliminary vetting* » ou « vérification préliminaire »). Selon la problématique signalée ou d'initiative, la CNIL peut également décider d'initier directement une procédure de contrôle des traitements de données mis en œuvre en France.

Lorsqu'elle est l'autorité chef de file, la CNIL informe les autorités concernées des éléments recueillis au cours de ses investigations et de son analyse. Elle peut également les solliciter pour obtenir leur avis ou assistance. À l'issue de ses investigations, la CNIL soumet à leur approbation un projet de décision. Il peut s'agir d'un rejet de la plainte si elle s'est finalement avérée infondée, d'une clôture du dossier en cas de résolution du problème soulevé (mise en conformité de l'organisme) ou de l'adoption d'une mesure correctrice à l'encontre de l'organisme mis en cause. Les autorités concernées disposent alors d'un délai de quatre semaines pour émettre des objections si elles sont en désaccord avec le projet de décision soumis.

Lorsque la CNIL est autorité concernée par un traitement transfrontalier, elle transmet les plaintes à l'autorité chef de file qui se charge de l'instruction du dossier. La CNIL reste le point de contact du plaignant français et le tient informé de l'état d'avancement du dossier. Elle participe à l'élaboration de la décision de l'autorité chef de file en émettant des objections si elle n'est pas d'accord avec l'analyse et/ou la mesure envisagée.

Si l'autorité chef de file suit les objections formulées, elle soumet une nouvelle décision révisée qui deviendra finale après un nouveau délai de deux semaines.
Si l'autorité chef de file n'entend pas suivre les objections émises par une ou plusieurs autorités concernées, elle saisit le Comité européen de la protection des données (CEPD) pour ouvrir la procédure de règlement des litiges prévue par l'article 65 du RGPD.

Le CEPD dispose alors d'un délai d'un mois, pouvant être prolongé d'un mois supplémentaire, pour se prononcer et adopter une décision. Celle-ci s'impose à l'autorité chef de file et est rendue publique.

INFOSPLUS

Le guichet unique et l'autorité chef de file

Le guichet unique est une procédure mise en place par le RGPD. Il a vocation à harmoniser au niveau européen les décisions des autorités de protection des données concernant les traitements transfrontaliers. Ces autorités doivent désormais se coordonner sur l'ensemble de ces décisions.

Avant l'entrée en application du RGPD, les entreprises établies dans plusieurs États membres de l'Union européenne (UE) devaient s'adresser à l'autorité de chacun des États membres dans lesquels elles avaient un établissement. Chacune de ces autorités de protection des données décidait seule, ce qui ne permettait pas de garantir une application uniforme des règles européennes.

Pour résoudre ces difficultés, le RGPD institue le mécanisme de « guichet unique », qui repose sur les trois principes suivants :

- un mécanisme de contrôle ouvert aux seules entreprises établies en UE ;
- un interlocuteur unique pour les responsables de ces traitements (l'autorité chef de file, c'est-à-dire l'autorité du pays où se trouve l'établissement principal de l'entreprise) ;
- une seule décision valable dans toute l'UE.

En 2020, plus de **1 000 dossiers** de coopération européenne concernaient des plaintes ou des contrôles.

La CNIL a été autorité « chef de file » (l'établissement principal de l'organisme visé se situe en France) dans une centaine de cas et « autorité concernée » (l'établissement principal de l'organisme visé se situe dans un autre pays de l'Union, mais des résidents français sont concernés) dans près de 400 cas.

La première décision contraignante adoptée par le CEPD

L'année 2020 a été marquée, au niveau européen, par l'adoption de la première décision du CEPD, à la majorité des deux tiers, dans le cadre du dispositif prévu par l'article 65 du RGPD. Cette décision, contraignante vis-à-vis de l'autorité chef de file irlandaise, a pour objet de régler les différends survenus entre cette autorité et les autorités de contrôle concernées à propos d'un projet de décision portant sur la Twitter International Company. Ce mécanisme a permis de répondre aux objections formulées par plusieurs autorités de protection des données concernées, et que l'autorité chef de file avait choisi d'écarter.

Dans ce dossier, l'autorité irlandaise avait adopté un projet de décision de sanction à la suite d'une enquête menée sur sa propre initiative, en l'absence de plaintes et après que la société Twitter l'avait informée d'une violation de données personnelles. L'autorité irlandaise a partagé son projet de décision avec les autres autorités concernées en mai 2020, conformément au mécanisme du « guichet unique » prévu par le RGPD. Les autorités concernées disposaient alors de quatre semaines pour présenter leurs objections pertinentes et motivées.

L'autorité irlandaise a rejeté l'ensemble des objections (pour désaccord sur le fond et/ou en les considérant comme non « pertinentes et motivées »). Elle a ensuite renvoyé l'affaire devant le CEPD, conformément à l'article 65 du RGPD, ouvrant ainsi la procédure de règlement des différends.

La procédure a été lancée officiellement le 8 septembre 2020. Le délai d'adoption par défaut d'un mois a été prolongé d'un mois supplémentaire en raison de la complexité de l'affaire.

Le 9 novembre 2020, le CEPD a adopté sa décision contraignante. L'autorité irlandaise a ensuite adopté sa décision finale sur la base de la décision du comité, qui a été transmise au responsable de traitement. Une fois le responsable de traitement notifié, le CEPD a pu rendre publique sa décision.

Cette première procédure « article 65 » a permis d'éprouver le mécanisme prévu par le RGPD et d'approfondir certaines notions clés, telle que « l'objection pertinente et motivée ».

Brexit : quelles conséquences ?

Le Royaume-Uni a quitté l'Union européenne le 31 janvier 2020 à minuit et, depuis cette date, il n'est plus considéré comme un État membre de l'UE.

Dans le cadre de l'accord de retrait entre l'Union européenne et le Royaume-Uni, une période transitoire a été convenue durant laquelle le droit de l'Union a continué de s'appliquer au Royaume-Uni. Pendant cette période, que ce soit en matière d'application du RGPD ou de transferts, la situation pour les organismes ou les personnes concernées est restée inchangée. La période transitoire ayant été prévue pour une durée d'un an, jusqu'au 31 décembre 2020, l'année a permis aux autorités de protection des données de l'EEE et du Royaume-Uni d'anticiper sur le futur de leurs relations.

En prévision de la fin de la période de transition du Brexit, le Comité européen de la protection des données (CEPD) a adopté dès juillet 2020 une note d'information qui soulignait les mesures devant être prises par les autorités de protection des données, les détenteurs de règles d'entreprise contraignantes (BCR) approuvées et les organisations dont les BCR étaient en cours d'examen par l'autorité de contrôle du Royaume-Uni, de façon à garantir que ces BCR puissent servir d'instruments de transfert valides fin 2020.

Le CEPD a par ailleurs adopté en décembre 2020 une déclaration relative à la fin de la période transitoire dans laquelle il décrit les principales implications pour les responsables de traitement et les sous-traitants. En particulier, il est abordé la question des transferts de données vers un pays tiers et les conséquences de la fin de la période transitoire pour le mécanisme de guichet unique (la période transitoire permettait à l'autorité de protection des données britannique de rester impliquée sur les procédures de coopération). Il était notamment rappelé aux responsables de traitement établis au Royaume-Uni qui ne disposeraient plus d'établissement dans l'Union la nécessité de désigner un représentant au sein de l'Union. En outre, le CEPD a adopté une note d'information sur les transferts de données dans le cadre du RGPD après la fin de la période de transition du Brexit, dans l'éventualité d'une sortie définitive sans accord.

Depuis le 1er janvier 2021, le mécanisme du « guichet unique » n'est plus applicable au Royaume-Uni.

Concernant les transferts de données vers le Royaume-Uni, l'accord de commerce et de coopération a été conclu entre l'Union européenne et le Royaume-Uni à la toute fin de l'année 2020. Une clause provisoire permet la poursuite de flux de données de façon temporaire sans encadrement particulier pour une durée maximale de 6 mois. Au 1er juillet 2021, à défaut d'une décision de la Commission européenne autorisant de façon générale les transferts de données personnelles vers le Royaume-Uni dite « décision d'adéquation », toute communication de données personnelles vers le Royaume-Uni sera considérée comme un transfert de données vers un pays tiers. De tels transferts ne pourront s'effectuer qu'avec la mise en place de garanties appropriées, telles que prévues par le RGPD.

La Commission européenne a de son côté annoncé qu'elle saisirait le CEPD de ses deux projets de décision d'adéquation concernant le Royaume-Uni en début d'année 2021, afin qu'il puisse se prononcer sur cette option. L'adoption de ces décisions d'adéquation aurait pour conséquence la possibilité de transferts avec le Royaume-Uni sans autorisation spécifique, sur la base de la décision d'adéquation.

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 les médias, sur internet et sur les réseaux sociaux, où elle met à disposition des outils pédagogiques et pratiques adaptés à ses différents publics.**

Anne-Charlotte
Juriste au service des relations avec les publics

Jean
Juriste au service des relations avec les publics

La fonction de juriste, au sein du service des relations avec les publics (SRP), a été créée pour répondre à la complexification des questions des usagers depuis l'entrée en application du RGPD en 2018. Nous accompagnons les téléconseillers dans l'élaboration des réponses, effectuons des recherches sur le droit et l'actualité, rédigeons des analyses et des synthèses juridiques, élaborons des outils pratiques de réponse pour les conseillers et des outils pédagogiques à destination des particuliers et professionnels.

Notre mission consiste ainsi à assurer la qualité des réponses apportées en concertation avec les services de l'institution.

Nous apprécions à la fois la transversalité des échanges avec les experts de la CNIL et le fait que nos activités font appel à l'esprit d'équipe ainsi qu'à des connaissances juridiques pluridisciplinaires. Être juriste au SRP permet à la fois d'être en contact direct avec les usagers et d'apporter un appui aux collègues conseillers.

LE SITE DE LA CNIL ET LES RÉSEAUX SOCIAUX

9 677 000

visites en 2020 sur les sites de la CNIL (cnil.fr, linc.cnil.fr, educnum.fr, services en ligne)

+ 21 % par rapport à 2019

120

actualités et communiqués publiés

964

contributions aux 6 consultations publiques

Un nombre record de visites sur le site de la CNIL

La crise sanitaire de 2020 a apporté de nouveaux enjeux pour les droits et libertés des personnes et, en conséquence, autant de demandes de professionnels et du grand public. L'augmentation considérable des visites des sites web de la CNIL (+ 21 % en un an sur l'ensemble des sites) est un indice particulièrement fort de l'intérêt du public pour la protection des données, notamment au regard de l'actualité récente.

Ainsi, la CNIL a publié de nombreuses fiches pratiques ou des communiqués, souvent en réponse à l'actualité, **cumulant plus de 430 000 visites pour le seul sujet « COVID-19 »**. Ces articles permettent de dessiner un panorama complet des enjeux Informatique et Libertés liés à la crise et au confinement : recommandations pour élaborer des projets de recherche en santé, conseils pour le télétravail, analyses relatives à l'application TousAntiCovid, caméras dites « intelligentes » et thermiques, continuité pédagogique, etc. La fiche « Les rappels de la CNIL sur la collecte des données par l'employeur » est **l'un des contenus les plus consultés de l'année 2020** avec 167 000 visites.

Outre les nombreux contenus publiés sur le sujet des cookies et autres traceurs (voir page 38), la CNIL a également publié de nouveaux guides et fiches pratiques à l'intention des responsables de traitement, comme le guide des durées de conservation ou de la fiche « Comment répondre à une demande de droit d'accès ? ». Des six bons réflexes de conformité à adopter aux outils les plus pointus, en passant par les cadres de référence, les professionnels disposent aujourd'hui d'une boîte à outils complète pour répondre au mieux aux droits des personnes dans leur activité.

Le grand public, au cœur des préoccupations de la CNIL, a également accès à de nombreuses fiches, que ce soit pour comprendre ses droits, maîtriser son navigateur ou ses réseaux sociaux. Ces contenus sont régulièrement mis en avant selon l'actualité : départs en vacances, achats lors des fêtes de fin d'année, outils de visioconférence, etc.

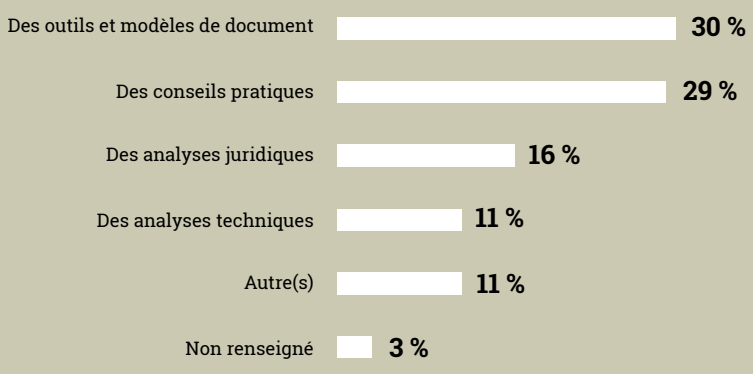
FOCUS

Votre avis sur le site web de la CNIL

La CNIL a conduit, de décembre 2020 à janvier 2021, une première enquête de satisfaction sur son site web.

Près de 200 personnes y ont répondu, en grande majorité des professionnels (85 %). Les résultats de cette consultation, qui sera reconduite annuellement, permettront à la CNIL d'orienter plus précisément son approche éditoriale et d'apporter des améliorations fonctionnelles pour faciliter la navigation sur son site web.

Quel(s) type(s) de contenu(s) souhaiteriez-vous voir davantage sur le site ?



Cette double communication, vers le grand public et les professionnels, continuera d'être au cœur des enjeux éditoriaux pour 2021 et au-delà, par une meilleure coexistence sur une thématique donnée des conseils pour les premiers et des réponses concrètes pour les seconds, notamment sur la – déjà riche – base de données « Besoin d'aide ».

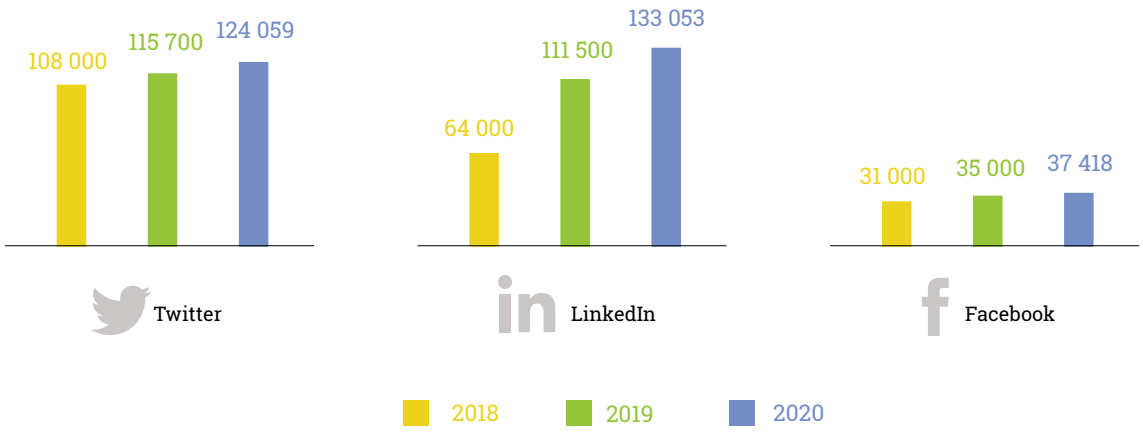
Top 3 des fiches pour les professionnels les plus lues	
Cookies : les outils pour les maîtriser	584 866 vues uniques
Cookies & traceurs : que dit la loi ?	495 115 vues uniques
Le règlement général sur la protection des données - RGPD	303 453 vues uniques

Top 3 des communiqués les plus lus	
Sanctions contre GOOGLE et AMAZON	51 000 vues uniques
Sanctions contre CARREFOUR FRANCE et CARREFOUR BANQUE	33 740 vues uniques
Mises en demeure contre EDF et ENGIE	30 804 vues uniques

Top 3 des fiches pour les particuliers les plus lues	
Générer un mot de passe solide	179 500 vues uniques
Les droits pour maîtriser vos données personnelles !	121 937 vues uniques
Faites régulièrement le ménage dans l'historique de navigation	97 934 vues uniques

Les réseaux sociaux, un vecteur d'information complémentaire

Les internautes sont, depuis l'entrée en application du RGPD et au regard de l'actualité, de plus en plus nombreux à se saisir du sujet de la protection des données : ainsi, fin 2020, tous les réseaux sociaux sur lesquels la CNIL communique enregistrent une nette progression du nombre d'abonnés.



Prédominants en cette année inédite, les sujets liés à la COVID-19 reviennent parmi les publications les plus partagées par les communautés de la CNIL, au regard notamment de ses avis et contrôles sur les fichiers tenus pour la gestion de la crise sanitaire. Les sanctions en fin d'année 2020 de Google, Amazon et Carrefour, remarquables par le montant inédit, ont également été très commentées et relayées par les internautes.

La publicité des sanctions, décidée au cas par cas par la formation restreinte de la CNIL, permet de communiquer efficacement sur les bonnes pratiques à adopter pour respecter les droits des personnes, mais également les risques en cas de manquements au RGPD et à la loi.

LinkedIn s'inscrit comme le réseau privilégié des délégués à la protection des données. Les internautes apprécient et partagent les contenus pédagogiques comme l'infographie consacrée à la réponse au droit d'accès. C'est aussi le réseau social de la CNIL qui enregistre la plus grande hausse d'abonnés entre 2019 et 2020 (+ 19 %).

Cette année, la CNIL a également enrichi sa chaîne YouTube (voir encadré) de nouvelles vidéos sur les cookies et sur les évènements qu'elle a organisés : air2020 (sur les mutations dans le monde du travail), la présentation du livre blanc sur les assistants vocaux ainsi que les tables rondes sur la portabilité.

LES RÉPONSES AU PUBLIC

La CNIL informe et conseille les particuliers ainsi que 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. Le public contacte la CNIL par téléphone lors des permanences juridiques (4 jours par semaine), par les services en ligne sur le site de la CNIL ou par courrier postal.

En 2020, la CNIL a reçu 121 439 appels, soit 17 % de moins que l'année précédente, notamment en raison de la crise sanitaire et de la fermeture partielle de l'accueil téléphonique durant le premier confinement.

24 045 appels ont été traités par les différentes permanences juridiques.

Avec 20 452 requêtes écrites reçues, l'année 2020 marque en revanche une augmentation de 18 % du nombre de demandes écrites d'information et de conseil, principalement adressées par les canaux électroniques (75 % par le formulaire « Nous contacter ») et en majorité par les particuliers (77 %).

Les principales thématiques de ces demandes, de plus en plus complexes, concernent :

- L'usage personnel des outils numériques du quotidien (questions sur les réglages de confidentialité des smartphones et des applications, sur les cookies et autres traceurs, sur les démarches à accomplir pour se faire déréférencer des moteurs de recherche).
- L'utilisation des données des salariés par les employeurs (principalement des questions sur le télétravail, la vidéosurveillance et la géolocalisation au travail).
- Les données traitées par le secteur bancaire, des organismes de crédit d'assurance.
- Enfin, la diffamation, l'usurpation d'identité, le piratage, et le cyberharcèlement, pour lesquels la CNIL réoriente l'usager.

La tendance à une plus grande prise de conscience par les usagers de leurs droits, déjà relevée en 2019, se caractérise également de plus en plus par leur volonté de les exercer et les faire respecter.

Le nombre de consultations de la rubrique « Besoin d'aide » dépasse cette année la barre du million (1 108 100 consultations).

> BESOIN D'AIDE

Les 2 thématiques les plus consultées parmi les 524 FAQ de « Besoin d'aide » portent sur la présentation de la CNIL et les explications sur les données personnelles, avec respectivement 154 292 et 48 215 consultations, soit 94 % de consultations de plus qu'en 2018 (année d'entrée en application du RGPD) pour les FAQ portant sur la CNIL et ses missions.

FOCUS

Les vidéos de la CNIL, un vecteur d'information pédagogique privilégié en 2020

Top 5 des vidéos les plus consultées :

1 - Tutoriel | Masquer ses amis sur Facebook (41k vues)

2 - Comment effacer ses cookies ? (38k vues)

3 - Tutoriel | Keepass (22k vues)

4 - La CNIL, 40 ans et toujours dans l'air du temps ! (13k vues)

5 - Comment j'ai attrapé un cookie ? (12k vues)

121 439
appels reçus au 01 53 73 22 22

1 108 100
consultations de la rubrique Besoin d'aide (FAQ questions/réponses)

24 045
appels aux permanences juridiques de la CNIL

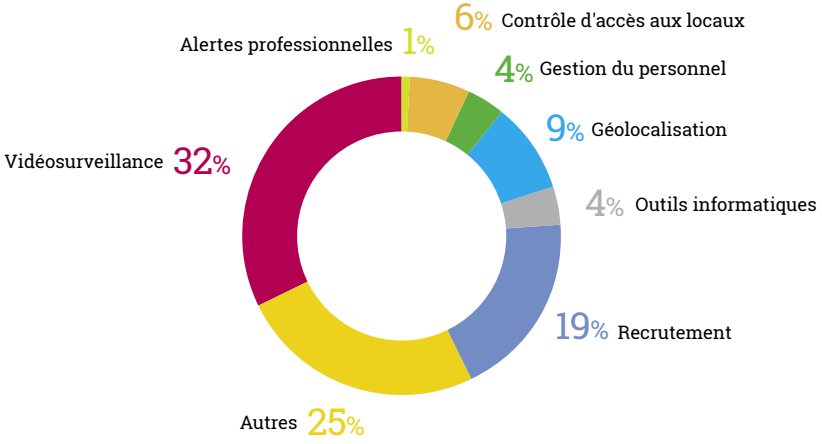
+ 18%
de requêtes écrites reçues (20 452)

Des demandes concentrées sur trois thématiques

Aux côtés de la thématique Travail-RH, commune aux particuliers et aux professionnels, le thème Internet-Téléphonie concentre près de 20 % des demandes d'information et de conseil des particuliers, tandis que le thème Santé-Social fait principalement l'objet de questions écrites des professionnels.

« La thématique « Travail-RH » est au cœur des demandes d'information et de conseil des particuliers et des professionnels.

Les contenus les plus consultés pour la thématique « Travail-RH »



L'ÉDUCATION AU NUMÉRIQUE

Le contexte de crise sanitaire lié à la COVID-19 a eu des conséquences directes sur les actions menées par la CNIL en matière d'éducation au numérique. Afin de poursuivre sa mission d'accompagnement, la CNIL s'est adaptée en proposant des webinaires et des formations de formateurs en ligne.

Un accompagnement dans le quotidien éducatif numérique

Pendant la crise sanitaire, les enseignants ont eu massivement recours aux outils numériques avec leurs élèves. En réponse à la multiplication des services disponibles sur le marché, la CNIL a accompagné les enseignants, les chefs d'établissements et les parents dans le choix d'outils respectueux des données personnelles. Elle s'est ainsi associée aux recommandations du ministère de l'Éducation nationale[15] incitant les enseignants à utiliser prioritairement les supports d'enseignement usuels, qui constituent un bouquet d'outils sécurisés pour les données personnelles de tous les acteurs, notamment celles des élèves.

La CNIL a participé activement à des webinaires thématiques pour les acteurs de l'éducation ainsi qu'aux États Généraux du numérique pour l'éducation, organisés en novembre 2020 par le ministère de l'Éducation nationale. Cet évènement a été l'occasion de valoriser ses actions d'éducation au numérique menées tant au niveau national qu'à l'échelle internationale, ainsi que les principes de protection des données et de souveraineté numérique.

Enfin, le site du collectif Educnum a été enrichi de manière régulière avec des actualités et des ressources destinées aux enseignants et aux éducateurs, ce qui a eu un impact positif sur son audience (+ 25 % de visites en 2020). Cela a également permis de valoriser les diverses actions et ressources des membres du collectif, ainsi que celles de la CNIL. Les thèmes liés à la protection des données, à la citoyenneté numérique et à l'éducation aux médias et à l'information ont été particulièrement mis en avant pendant cette période.

Les droits des mineurs à l'ère numérique : une priorité d'action pour la CNIL

En 2020, la CNIL s'est saisie d'un sujet d'ampleur : les droits des mineurs dans l'environnement numérique. En effet, si le RGPD et la loi prévoient un encadrement particulier pour le consentement des mineurs de moins de 15 ans, ces dispositions ne sont pas encore suffisamment prises en compte par les responsables de traitement. Afin d'informer de façon satisfaisante les mineurs et de renforcer les actions pédagogiques proposées par les personnels éducatifs et les parents, la CNIL a conduit deux études préalables.

15 « Plan de continuité pédagogique », page mise à jour en janvier 2021, eduscol.education.fr

INFOSPLUS

Outils de continuité pédagogique, Incollables®, conférences... Pour permettre aux professionnels de l'éducation et aux parents de suivre au mieux l'actualité éducative numérique, la CNIL communique régulièrement sur les contenus publiés sur son site web Educnum sur les réseaux sociaux Facebook et Twitter (@EDUCNUM).

UN SONDAGE SUR LES PRATIQUES NUMÉRIQUES DES MINEURS

La CNIL et l'IFOP ont conduit un sondage en décembre 2019[16] sur les pratiques numériques des mineurs et la perception qu'en ont leurs parents. Les résultats montrent non seulement qu'un fort pourcentage de mineurs navigue sur internet, joue en ligne, regarde des vidéos et ouvre des comptes sur les réseaux sociaux, mais surtout qu'ils le font seuls et de plus en plus tôt. De même, il existe un décalage entre les pratiques constatées par les parents et celles réelles de leurs enfants.

UNE CONSULTATION PUBLIQUE SUR LES ENJEUX POUR LA PROTECTION DES DONNÉES DES MINEURS

La CNIL a également organisé une consultation publique entre avril et juin 2020 sur son site web. Cette consultation portait sur les conditions dans lesquelles un mineur devrait pouvoir accomplir seul certains actes sur internet, les modalités de vérification de l'âge et de recueil du consentement des parents et enfants à privilégier, ou encore les conditions d'exercice des droits. La majorité des personnes interrogées (éducateurs, acteurs associatifs, professionnels du numérique et du droit, parents, enfants) ont indiqué souhaiter que les mineurs puissent gagner en autonomie, tout en demandant un renforcement de leur protection en ligne. Les résultats complets du sondage et de la consultation sont disponibles sur le site de la CNIL[17].Ces deux études seront prises en compte par la CNIL, qui adoptera des recommandations en 2021 à destination des différents acteurs de l'éducation.

Un kit du citoyen numérique proposé par quatre autorités indépendantes

La CNIL, le CSA, le Défenseur des droits et la Hadopi ont décidé de regrouper leurs ressources pédagogiques au sein d'un kit du citoyen numérique.

Destiné aux enseignants, aux parents et aux jeunes adultes, ce kit permet de sensibiliser les jeunes publics aux enjeux de la citoyenneté numérique, sur quatre grands thèmes : les droits sur internet, la protection de la vie privée en ligne, le respect de la création, l'utilisation raisonnée et citoyenne des écrans. Le kit est disponible sur les sites de chacune des autorités[18].

Le collectif Educnum

La CNIL a initié, en mai 2013, un collectif d'acteurs très divers – issus du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, de fondations d'entreprises et d'autres institutions – pour porter et soutenir des actions visant à promouvoir une véritable « culture citoyenne du numérique ». Il regroupe aujourd'hui près de 70 structures.

SES MISSIONS

- Initier et promouvoir des actions visant à sensibiliser et à former tous les publics, et notamment les plus jeunes, à un usage responsable et éclairé des technologies numériques.
- Encourager les échanges d'expériences entre les différents acteurs impliqués dans l'éducation au numérique, en favorisant le dialogue entre générations.
- Informer la communauté éducative (enseignants, associations, acteurs du périscolaire, parents) sur les ressources et les actions du collectif en matière d'éducation au numérique.
- Relayer et contribuer à assurer la visibilité des actions engagées par les membres du collectif, tant au niveau national qu'international.
- Communiquer sur les actions menées par des prises de parole publiques et faire des propositions et des recommandations aux pouvoirs publics.
- Associer les acteurs économiques à l'importance de développer une culture générale du numérique.

16 Sondage IFOP conduit du 2 au 10 décembre 2019 auprès d'un échantillon de 1000 personnes représentatif des parents français dont au moins un enfant de 8 à 17 ans réside dans le foyer et d'un échantillon de 502 personnes représentatif des jeunes français âgés de 10 à 17 ans selon la méthode des quotas.

17 « Droits numériques des mineurs : la CNIL publie les résultats du sondage et de la consultation publique », 11 janvier 2021, cnil.fr

18 « Kit pédagogique du citoyen numérique : retrouvez toutes les ressources », 18 janvier 2021, educnum.fr

CONSEILLER
les pouvoirs publics et le Parlement

La CNIL peut formuler des avis sur des projets de textes du Parlement ou du Gouvernement afin de souligner les enjeux pour les droits des personnes et proposer des solutions. Elle participe également à des auditions parlementaires pour expliciter certains points techniques.

Marion
Juriste au service des affaires régaliennes et des collectivités territoriales

La sphère régalienne (« Police-Justice ») constitue l'un des secteurs au sein desquels il subsiste encore un grand nombre de formalités à accomplir auprès de la CNIL. Dès lors, une partie des missions du service des affaires régaliennes et des collectivités territoriales consiste en l'instruction de demandes d'avis, aussi bien sur des projets de loi et de décrets que sur des analyses d'impact relative à la protection des données (AIPD).

Dans ce cadre, j'instruis très régulièrement des dossiers sur lesquels le Collège de la CNIL est amené à se prononcer et rendre un avis. Cela est particulièrement intéressant puisque les traitements mis en œuvre dans cette sphère impliquent nécessairement de devoir concilier des impératifs de sécurité et de liberté, afin d'assurer la stricte proportionnalité des dispositifs de collecte de données personnelles. L'année 2020 a notamment été marquée par la modification de certains fichiers de renseignement à forts enjeux (traitements PASP, GIPASP et EASP). J'ai également pu réaliser des interventions extérieures, avec certains aménagements dus au contexte sanitaire, visant à assurer une sensibilisation sur ces enjeux et plus largement à ceux de la protection des données.

L'année 2021 sera en partie consacrée à assurer une plus grande visibilité des avis rendus par la CNIL sur ces sujets en les rendant facilement accessibles au grand public. À cet égard, un article visant à expliquer le déroulement ainsi que les grandes étapes propres à cette formalité a fait l'objet d'une publication sur le site de la CNIL.

LES ACTIVITÉS AU PARLEMENT

L'année 2020 se caractérise par des liens intenses avec le Parlement, notamment à travers une vingtaine d'auditions et huit questionnaires écrits. Trois facteurs y ont contribué :

- la fréquence des demandes adressées à la CNIL, en provenance de tous les acteurs de la vie parlementaire, élus, collaborateurs et personnels des assemblées ;
- l'augmentation du nombre de propositions et projets de loi comportant des enjeux Informatique et Libertés, du fait de la numérisation croissante de la société ;
- la capacité de la CNIL à répondre à des demandes de plus en plus techniques dans des délais très restreints en raison du rythme parlementaire. Ces demandes régulières témoignent de l'expertise solide de la CNIL dans ses champs de compétences.

Les auditions par les rapporteurs des projets et propositions de loi constituent des temps forts dans l'année parlementaire.

En 2020, en dehors des projets de textes liés à la crise sanitaire (voir page 31), la CNIL a été entendue sur le projet de loi organique relatif au CESE (Conseil économique, social et environnemental), la proposition de loi relative à la sécurité globale, déposée le 20 octobre 2020 et suivie d'un avis le 26 janvier 2021[19] ou encore la proposition de loi interopérabilité.

Les thèmes traités dans le cadre des missions de contrôle occupent également une part non négligeable de l'action de la CNIL au Parlement avec une très grande variété de thèmes abordés, en particulier lors des auditions devant les missions d'information. En 2020, la CNIL a ainsi répondu aux demandes des missions consacrées à l'identité numérique, l'évaluation de la loi renforçant la lutte contre les violences sexuelles et sexistes, les géants du numérique, l'émergence et l'évolution des différentes formes de racisme.

FOCUS

Les auditions de la CNIL liées à la crise sanitaire

3 avril 2020 : entretien avec M. Cédric Villani, 1er vice-président de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) pour la préparation d'une note relative aux technologies de l'information utilisées pour limiter la propagation de l'épidémie de COVID-19.

8 avril 2020 : audition devant la Commission des lois de l'Assemblée nationale sur l'utilisation des nouvelles technologies en matière épidémiologique face à la crise sanitaire actuelle et dans la perspective du déconfinement.

8 avril 2020 : audition devant Mme Laure de La Raudière et M. Éric Bothorel, co-rapporteurs du groupe de travail mis en place par la Commission des affaires économiques sur l'impact, la gestion et les conséquences de l'épidémie de COVID-19 dans le domaine des communications électroniques, des postes et de l'économie numérique. Thème de l'audition : les technologies numériques et lutte contre la COVID-19.

15 avril 2020 : audition devant la Commission des lois du Sénat sur le projet d'application StopCovid.

1er mai 2020 : audition devant M. Alain Milon, rapporteur pour avis de la Commission des affaires sociales du Sénat sur le projet de loi prorogeant l'état d'urgence sanitaire.

5 mai 2020 : audition devant la Commission des lois de l'Assemblée nationale sur le projet de loi prorogeant l'état d'urgence sanitaire.

8 octobre 2020 : audition devant Mme Claudine Lepage, sénatrice, vice-présidente de la commission des affaires parlementaires de l'Assemblée parlementaire de la francophonie, dans le cadre de la préparation d'un rapport sur « l'utilisation de la géolocalisation en temps de pandémie dans l'espace francophone ».

25 novembre 2020 : audition devant MM. Philippe Gosselin et Sacha Houlié, co-présidents de la mission d'information de l'Assemblée nationale sur le régime juridique de l'état d'urgence sanitaire.

19 « La CNIL rend son avis sur la proposition de loi sécurité globale », 3 février 2021, cnil.fr

FOCUS

L'avis de la CNIL sur le projet de loi confortant le respect des principes de la République

La CNIL, saisie en urgence le 16 novembre 2020, a rendu **un avis le 24 novembre 2020 sur l'article 3 du projet de loi confortant le respect des principes de la République**. Cet article vise à modifier certaines des conditions de mise en œuvre du fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT), dont les principales caractéristiques ont été fixées par le législateur.

La CNIL a relevé dans son avis que ce projet d'article visait à étendre le périmètre de ce fichier en y intégrant de nouvelles infractions liées au terrorisme, à modifier les conditions d'inscription dans ce fichier ainsi qu'à introduire un régime différencié dans le traitement des personnes inscrites dans ce fichier.

La CNIL s'est montrée réservée sur certaines évolutions envisagées du FIJAIT et a considéré qu'une vigilance accrue devait être portée aux modalités et conditions d'application de ces nouvelles dispositions, déterminées par décret en Conseil d'État, et sur lesquelles elle devrait également se prononcer.

En dehors de la saisine, la CNIL a également tenu à souligner, dans le même avis, que la lecture dans son ensemble du projet de loi faisait apparaître d'autres dispositions de nature à avoir un impact sur la réglementation relative à la protection des données personnelles et pour lesquelles sa saisine apparaissait, selon les cas, justifiée ou opportune. L'avis de la CNIL, public, détaille les articles à propos desquels il faudra, le cas échéant, tirer toutes les conséquences des modifications envisagées.

La CNIL a par ailleurs constaté une augmentation des demandes de contribution sous la forme du questionnaire écrit, sans doute pour compenser l'impossibilité de réaliser une audition sur place : elle a ainsi répondu à des questionnaires rendus à l'Assemblée nationale à la mission d'information sur le Défenseur des droits, à la mission d'information sur l'évaluation de la loi Renseignement ou bien à la commission des affaires européennes du Sénat à l'appui des travaux relatifs à la proposition de résolution européenne sur la localisation des données.

L'année restera également marquée par des échanges fréquents et nourris qui ont pu se déployer entre la CNIL et les commissions du Parlement pour assurer le suivi et l'information de la représentation nationale sur les différents outils déployés dans le cadre de la crise sanitaire.

Enfin, la CNIL a rencontré à deux reprises les membres de la mission confiée par le Premier ministre au député Éric Bothorel, associant Stéphanie Combes, directrice du *Health Data Hub* et Renaud Vedel, coordonnateur national pour la stratégie en IA, sur l'ouverture des données et codes sources publics et les données d'intérêt général. Un questionnaire écrit a également été rendu à la mission.

Outre les avis qu'elle rend (voir page 9), les auditions de la CNIL devant les rapporteurs des textes dans les assemblées donnent l'opportunité d'exposer les détails juridiques et technologiques ayant motivé les avis rendus.

LE RÔLE DE LA CNIL DANS LE CADRE DES CAMPAGNES ÉLECTORALES

L'accompagnement des acteurs de la vie politique

La CNIL accompagne toutes les parties prenantes du processus électoral, qu'il s'agisse des candidats aux élections et de leur parti, des élus ou des électeurs qui la sollicitent. Elle accomplit cette mission dans le cadre de la mise en conformité des traitements mis en œuvre et pour permettre l'exercice des droits des personnes concernées.

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

De plus, plusieurs scandales, en particulier l'affaire « Cambridge Analytica », ont permis au grand public de prendre conscience des enjeux liés à l'utilisation de leurs données personnelles. Se sont révélés en particulier des enjeux juridiques complexes autour de la notion de profilage, de sécurité et de localisation des données. Enfin, au-delà des seuls enjeux juridiques, cette affaire soulève des questions éthiques importantes en touchant notamment à la sincérité du scrutin réalisé.

Dans ce contexte, le rôle de **la CNIL consiste à accompagner l'innovation tout en garantissant le respect des libertés individuelles,** comme en témoigne son activité dans le secteur de la communication politique.

Retour sur les élections municipales 2020

ACCOMPAGNEMENT : LE PLAN D'ACTION DE LA CNIL EN PRÉVISION DES ÉCHÉANCES ÉLECTORALES

La CNIL a présenté un plan d'action en amont des élections municipales de 2020 afin de s'assurer du respect des dispositions RGPD tout au long du processus électoral. Ce plan s'articulait autour de plusieurs initiatives, parmi lesquelles :

- la mise à jour des contenus disponibles sur le site web de la CNIL, notamment sur le cadre juridique applicable ;
- des conseils pratiques pour les candidats et partis, en particulier sur les fichiers pouvant être utilisés et méthodes de prospection (SMS, courriel, etc.) ;
- une actualité lors de l'entre-deux-tours pour rappeler quelques règles à la suite de signalements ;
- la mise à disposition d'une plateforme de signalement sur le site de la CNIL qui permet à toute personne de signaler une pratique qu'elle estimerait non conforme, ce qui peut donner lieu à des contrôles et, si nécessaire, de mesures correctrices.

De plus, des contrôles ont été réalisés auprès de prestataires de service de prospection politique et de stratégie électorale afin de prendre connaissance des conditions dans lesquelles les données personnelles étaient utilisées.

LES PRATIQUES CONSTATÉES

Ces élections ont mis en lumière le recours de plus en plus fréquent à des logiciels de prospection politique ou de stratégie électorale. Ces outils permettent d'identifier, à partir de données sociodémographiques et des résultats électoraux précédents, les secteurs géographiques les plus intéressants en termes de prospection politique. Ils peuvent ainsi préparer l'organisation d'opérations de porte-à-porte ou la collecte des coordonnées des personnes démarchées afin de leur adresser par la suite des communications d'un candidat.

La CNIL a pu constater un manque de transparence de certains candidats et partis en matière de démarchage et un mécontentement chez les personnes contactées. Outre le rappel des règles à suivre sur son site web, la CNIL a signalé aux candidats mis en cause les points suivants :

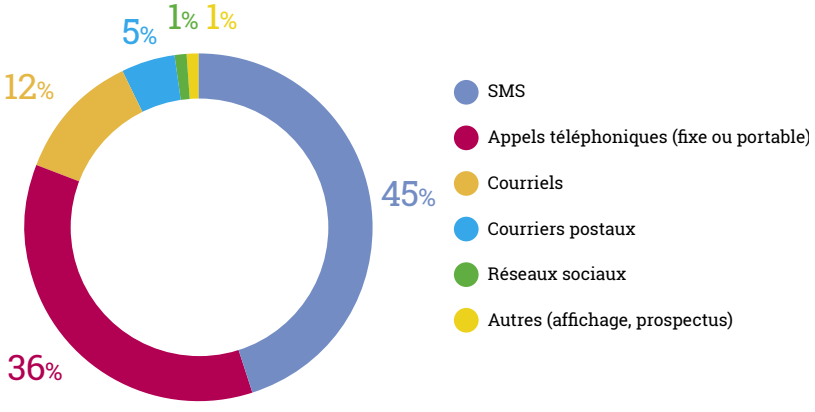
- Les candidats sont tenus d'**informer correctement les destinataires** de leurs messages de prospection politique. Ainsi, l'origine des données utilisées pour démarcher un électeur doit lui être précisée.
- Il est formellement interdit pour un candidat d'utiliser le fichier des clients de sa société commerciale ou des adhérents de l'association qu'il préside, par exemple. Les fichiers tenus par les mairies (fichiers scolaires ou périscolaires, fichiers « évènements météorologiques », etc.) ne doivent pas non plus être utilisés pour adresser des messages en lien avec la campagne électorale, à l'exception de la liste électorale.
- Les moyens de communication utilisés doivent **permettre aux personnes contactées de faire valoir leurs droits** aisément et ces demandes doivent être traitées dans les meilleurs délais, et au plus tard dans un délai d'un mois.

Ainsi, cinq missions de contrôle ont été ouvertes sur les cas les plus graves et la présidente de la CNIL a formellement rappelé à leurs obligations quatre candidats.

En dehors de ces cas, la CNIL a constaté que **ses précédentes recommandations en matière électorale avaient, en règle générale, été prises en compte par les candidats et leurs prestataires**. Par ailleurs, ces contrôles ont fait apparaitre que les solutions proposées aux

Affiche réalisée dans le cadre du plan d'action pour les élections municipales 2020

Les modes de prospection électorale les plus souvent mis en cause dans les signalements



candidats n'offrent pas de possibilités de ciblage des électeurs aussi fines que ce qui a parfois pu être évoqué dans les médias.

L'absence de recours aux données issues des réseaux sociaux chez les prestataires contrôlés, l'utilisation d'outils statistiques en *open data*, ainsi que l'hébergement des données en France, sont autant de points positifs qui doivent être soulignés et être conservés lors des prochaines élections.

SIGNALEMENTS : LE BILAN CHIFFRÉ

Comme à chaque élection, la CNIL a ouvert une **plateforme de signalement** sur son site web afin de permettre à toute personne de signaler une pratique qu'elle estime non conforme.

À l'occasion des élections municipales, la CNIL a enregistré un total de **3 948 signalements**, concernant 329 communes, dont 3 034 signalements reçus au 1er tour et 914 signalements reçus au 2nd tour. Elle a également enregistré plus d'une centaine de plaintes.

Les principaux motifs de sollicitation, qu'il s'agisse de signalements ou de plaintes, ont concerné :

- le détournement de finalité ;
- l'origine des données ;
- la dénonciation de l'absence de réponse ou la réponse insatisfaisante à une demande d'accès ;
- l'opposition et effacement (par exemple l'absence de prise en compte de l'exercice du droit d'opposition, l'absence de modalités facilitant la désinscription ou encore un lien de désinscription non valide) ;
- la sécurité ;
- l'obligation d'information.

Histoire vécue...

« J'ai reçu 3 appels téléphoniques aujourd'hui me délivrant un message de Y m'incitant à voter pour X. Comment ont-ils eu mes coordonnées ? Je suis sur liste rouge ! J'ai toujours voté et choisi seule mon candidat sans que l'on cherche à me forcer la main. Honte à vous X, et par extension à tous vos communicants. À quel niveau vous vous rabaissez pour collecter quelques voix que vous n'aurez jamais. Il faut être digne d'une mairie. »

Histoire vécue...

« Bonjour, je reçois des mails concernant les réunions du candidat X. Cependant il utilise les adresses mail via le portail famille avec lequel j'inscris mes enfants à la cantine... C'est scandaleux d'utiliser les données personnelles pour ça. »

ACCOMPAGNER
la conformité

L'accompagnement des organismes dans leur conformité est une mission fondamentale de la CNIL. Celle-ci adopte et publie régulièrement de nombreux outils pour les responsables de traitement, les délégués à la protection des données et l'ensemble des acteurs concernés par les enjeux de protection des données.

Marie
Juriste au service des affaires économiques

Le service des affaires économiques, composé de 9 juristes, d'une cheffe de service et d'une adjointe, est notamment chargé de l'accompagnement des acteurs publics et privés, en particulier dans les secteurs du commerce/marketing, des télécoms, des services internet (plateformes/réseaux sociaux), de la banque, de l'énergie, des assurances, et du transport.

Dans ce cadre, l'une de nos missions consiste à instruire et répondre aux demandes de conseil sur des projets impliquant des traitements de données personnelles et des problématiques de conformité au regard de la réglementation relative à la protection des données et, le cas échéant, un intérêt particulier d'un point de vue juridique, sociétal, économique ou encore technologique.

L'accompagnement des professionnels, premiers acteurs de la conformité, est en effet l'une des missions essentielles de la CNIL. À cet égard, le service a été particulièrement impliqué en 2020 sur la rédaction et la publication des lignes directrices et des recommandations relatives aux cookies et autres traceurs, qui ont également fait l'objet d'une large consultation des différents acteurs du secteur et des membres de la société civile.

En 2020, nous avons également été particulièrement sollicités sur diverses demandes d'avis concernant des projets de textes réglementaires pris par les pouvoirs publics ou des demandes de conseil de professionnels liées à l'épidémie de COVID-19 (applications de suivi des contacts, utilisation de caméras dites « intelligentes » ou caméras thermiques pour gérer la crise sanitaire, etc.).

Pour accompagner les organismes dans leurs démarches de mise en conformité, la CNIL produit un grand nombre d'outils destinés à l'ensemble des professionnels ou à certains secteurs : il peut s'agir de référentiels, de lignes directrices, de recommandations, de guides pratiques ou, plus simplement, de fiches pratiques sur son site web.

Ces outils n'ont pas de valeur contraignante et sont dits de « droit souple » : ils visent à donner à ces professionnels des clés afin d'assurer leur conformité dans les meilleures conditions.

En dehors de ces outils, la CNIL a poursuivi, en 2020, sa stratégie d'accompagnement spécifique des délégués à la protection des données.

LES OUTILS D'ACCOMPAGNEMENT GÉNÉRAUX

« Cookies et autres traceurs » : les nouveaux outils

Dans la continuité de ses travaux sur le ciblage publicitaire, dont le plan d'action a été rendu public en 2019, la CNIL a publié des lignes directrices modificatives et une recommandation concernant l'usage des « cookies et autres traceurs » le 1er octobre 2020. Ces outils, adoptés à la suite d'une concertation avec le secteur de la publicité numérique et la société civile, après une consultation publique, visent à aider les professionnels à se conformer aux règles protégeant les données personnelles et la vie privée des internautes, selon un standard robuste et durable.

Afin de permettre aux professionnels de comprendre et d'appliquer l'évolution des règles applicables, un dispositif d'accompagnement renforcé a été initié. Des contenus complémentaires ont été publiés, tels qu'une **foire aux questions et des exemples d'interfaces de recueil des choix**. La CNIL a également proposé des **webinaires** à destination des associations représentatives des professionnels concernés et du secteur public.

Un guide pratique sur les « tiers autorisés »

Un certain nombre d'autorités ont également le pouvoir d'exiger la transmission, par des organismes publics, de documents ou de renseignements : ces organismes sont appelés les « tiers autorisés ».

Cela implique fréquemment la communication de données personnelles par un responsable de traitement. Les organismes concernés par une demande d'un tiers autorisé peuvent alors rencontrer des difficultés pour concilier l'obligation d'y répondre tout en veillant au respect des règles de protection des données personnelles, en particulier sur l'exigence de confidentialité.

INFOSPLUS

Les consultations publiques

Afin de répondre aux besoins des professionnels sur les secteurs concernés et aux interrogations des personnes (employés, internautes, etc.), la CNIL propose régulièrement des consultations publiques sur son site web avant de publier les versions définitives de ses outils.

Ces consultations, parfois ouvertes à tous, sont essentielles : elles permettent d'ajuster les recommandations de la CNIL en fonction des retours du terrain.

FOCUS

Lignes directrices sur les traceurs : une publication en deux étapes

Le 4 juillet 2019, la CNIL a adopté des lignes directrices rappelant le droit applicable aux « cookies et autres traceurs ».

Celles-ci ont été ajustées le 17 septembre 2020 pour tirer les conséquences de la décision rendue le 19 juin 2020 par le Conseil d'État.

Afin de les accompagner dans ces démarches, la CNIL a publié[20] :

- **un guide pratique**, qui présente les problématiques que peut rencontrer le responsable de traitement et les points de vigilance lors du traitement de telles demandes ;
- **un recueil des principales procédures** listant les acteurs susceptibles de demander la communication de données personnelles.

Un guide et des référentiels pour aider les professionnels à définir les durées de conservation

Les données personnelles ne peuvent être conservées indéfiniment : une durée de conservation doit être déterminée par le responsable de traitement en fonction de l'objectif ayant conduit à la collecte de ces données. Ce principe, essentiel, d'une conservation limitée des données personnelles est consacré par le RGPD et la loi Informatique et Libertés.

La CNIL a ainsi élaboré **un dispositif complet, composé :**

1. d'un **guide pratique** qui répond aux questions que se posent fréquemment les professionnels, tant sur le principe de la limitation de la conservation des durées que sur sa mise en pratique. Élaboré en partenariat avec le service interministériel des Archives de France (SIAF), ce guide explicite :
   - l'articulation entre les obligations du RGPD et celles imposées par le Code du patrimoine ;
   - l'utilisation des référentiels de durées de conservation.
2. de **référentiels sectoriels** pour faciliter la recherche de la durée pertinente. Sous forme de tableaux, ils présentent, pour les traitements les plus récurrents dans le secteur concerné, les étapes de la vie des données (base active, voire archivage intermédiaire). **Cet outil a été conçu comme une base de travail, à partir de laquelle le responsable du traitement peut mener sa propre analyse**, selon les spécificités du traitement et de la structure concernés.

Les premiers référentiels adoptés concernent le domaine de la santé (hors recherche) et celui de la recherche en santé.

L'ACCOMPAGNEMENT SECTORIEL

Santé

UN RÉFÉRENTIEL RELATIF À LA GESTION DES CABINETS MÉDICAUX ET PARAMÉDICAUX

Le 18 juin 2020, la CNIL a adopté un référentiel relatif aux traitements de données personnelles pour la gestion des cabinets médicaux et paramédicaux. En effet, les professionnels de santé exerçant à titre libéral sont responsables de plusieurs traitements générés à l'occasion de la gestion médicale et administrative de leurs cabinets.

Ce référentiel décrit tout d'abord les finalités que pourraient poursuivre des traitements mis en œuvre dans le cadre d'une activité médicale ou paramédicale libérale. Ce référentiel souligne notamment :

- les bases légales, les données qui peuvent être considérées comme pertinentes ou les destinataires de données possibles ;
- les points de vigilance en cas de recours à un prestataire tels qu'un service de maintenance du logiciel et des postes de travail gérant les « dossiers patients », ou une plateforme de prise de rendez-vous en ligne.
- les durées de conservation des données, qui peuvent différer selon la finalité du traitement.
- l'information qui doit être donnée aux personnes (patients, salariés…), notamment sur leurs droits ;
- des mesures de sécurité utiles notamment pour les postes de travail, l'archivage, la protection des locaux ou le réseau informatique interne, etc.

Gestion des ressources humaines

UN RÉFÉRENTIEL ET DES QUESTIONS-RÉPONSES

La CNIL a également adopté un référentiel relatif aux traitements de données

20 « Tiers autorisés : la CNIL publie un guide pratique et un recueil de procédures », 10 juillet 2020, cnil.fr

personnelles mis en œuvre aux fins de gestion des ressources humaines et l'a rendu public en avril 2020. Il s'inscrit dans la continuité de la norme simplifiée n°46 qui n'a plus de valeur juridique depuis l'entrée en application du RGPD.

Outil d'aide à la mise en conformité, il applique les règles de protection des données aux traitements courants de gestion du personnel, tels que le recrutement, la gestion administrative du personnel, la rémunération, ou encore la mise à disposition des salariés d'outils de travail. Une FAQ accompagne la publication du référentiel pour répondre aux questions les plus fréquentes.

Gestion locative

Une consultation sur le projet de référentiel

Afin d'actualiser le cadre juridique des traitements de données relatifs à la gestion locative, la CNIL a lancé fin 2020 une consultation publique sur son projet de référentiel. **Le référentiel s'adresse aux personnes physiques ou morales qui, à titre professionnel, mettent en location un local d'habitation constituant une résidence principale, à l'exclusion du secteur du logement social.**

Reprenant certains éléments de l'ancienne norme simplifiée n° 21 (qui n'a plus de valeur juridique aujourd'hui), ce référentiel a pour vocation de couvrir l'ensemble des étapes d'une location immobilière, de la recherche à la résiliation du bail.

Pour chacune de ces étapes, le référentiel fournira des indications aux particuliers et professionnels afin de les aider à mettre en œuvre leurs traitements de données en conformité avec les principes Informatique et Libertés. Cette consultation permettra également, par la suite, la publication de fiches pratiques sur le site de la CNIL.

Secteur social et médico-social

La CNIL a également lancé fin 2020 une consultation publique sur un projet de référentiel relatif aux traitements de données personnelles mis en œuvre dans le cadre de l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes âgées, en situation de handicap et en difficulté.

Le référentiel définitif, publié en mars 2021, s'inscrit dans la démarche d'actualisation du patrimoine normatif de la CNIL.

LES AUTRES OUTILS PRÉVUS PAR LE RGPD

Le RGPD offre une boîte à outils diversifiée pour permettre aux organismes de gérer leur conformité d'une façon dynamique et vérifier qu'ils respectent la règlementation : certains de ces outils sont nouveaux comme la certification ou les codes de conduite d'autres, comme les règles d'entreprise contraignantes, existaient depuis longtemps mais leur procédure d'approbation a été révisée.

La certification

La certification permet de **répondre aux besoins des professionnels qui souhaitent démontrer et communiquer sur le niveau de protection des données offert par leurs produits, services, processus ou systèmes de données.**

En décembre 2020, la CNIL a adopté les critères de certification que les prestataires de formation à la protection des données devront respecter pour pouvoir être certifiés. Cette adoption s'inscrit dans la continuité d'une consultation publique organisée en mars 2020 et pour laquelle une centaine de contributions ont été reçues. Ces critères ont été publiés en février 2021 sur le site web de la CNIL.
Ce mécanisme de certification s'ajoute à la certification des compétences du délégué à la protection des données qui peut être demandée auprès des 9 organismes de certification agréés par la CNIL le 31 décembre 2020.

À NOTER : La CNIL a publié, en février 2021, un dossier complet dédié à la certification sur son site web. Elle en explique le fonctionnement pour les organismes certificateurs et professionnels souhaitant être certifiés, et propose également un nouveau service en ligne pour soumettre un mécanisme de certification national[21].nant les traitements de données personnelles effectués par ses filiales dans le monde entier.

21 Dossier « La certification », février 2021, cnil.fr

FOCUS

Des ressources sectorielles sur le site de la CNIL

En 2020, de nouvelles thématiques dédiées ont été créées pour le profil « je suis un professionnel » comme par exemple les thématiques « social » et « logement ».

La CNIL y propose des fiches pratiques pour aider à comprendre les enjeux liés à la protection des données personnelles dans ces secteurs ainsi que des outils d'accompagnement à la mise en conformité.

INFOSPLUS

Au niveau européen, plusieurs projets de certification font l'objet d'échanges entre la CNIL et ses homologues en vue d'aboutir à l'approbation en 2021 d'une première certification européenne par le Comité européen de la protection des données (CEPD). Dans le cadre de ces travaux préparatoires, la CNIL a participé en 2020 à l'élaboration de **10 avis relatifs aux exigences d'agrément des organismes certificateurs adoptés par le CEPD.**

Les codes de conduite

Cet outil de conformité, créé par le RGPD, permet **d'harmoniser les pratiques de tout un secteur d'activité**. Les porteurs de code sont souvent des fédérations ou des associations professionnelles qui souhaitent proposer à leurs adhérents un instrument de mise en conformité opérationnel.

UNE ORGANISATION RIGOUREUSE NÉCESSAIRE

L'instrument code de conduite, dont la rédaction par un porteur nécessite un bon niveau de maturité et une bonne organisation, a reçu de nombreuses manifestations d'intérêt. À ce jour, la CNIL accompagne 3 porteurs qui travaillent à l'élaboration de codes de conduite européens et 5 porteurs sur des projets de codes nationaux dans des secteurs d'activités très variés. Certains projets, très avancés, devraient faire l'objet d'une approbation en 2021.

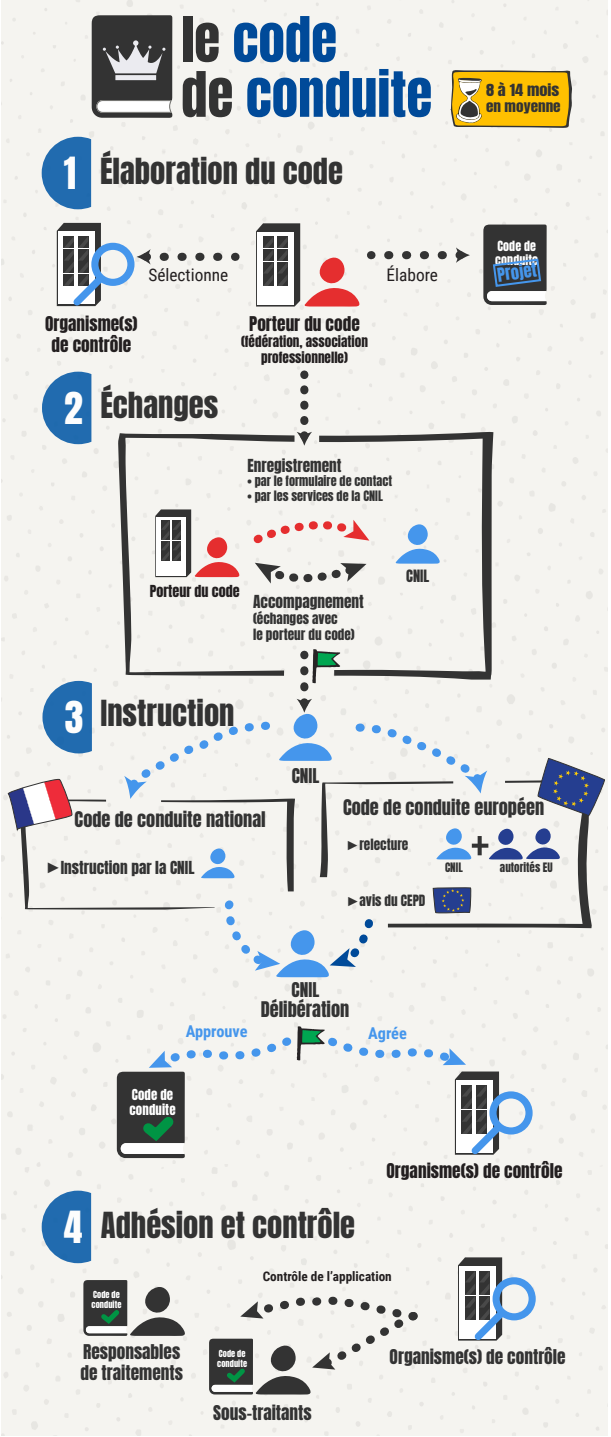
LE CONTRÔLE DU CODE DE LA CONDUITE

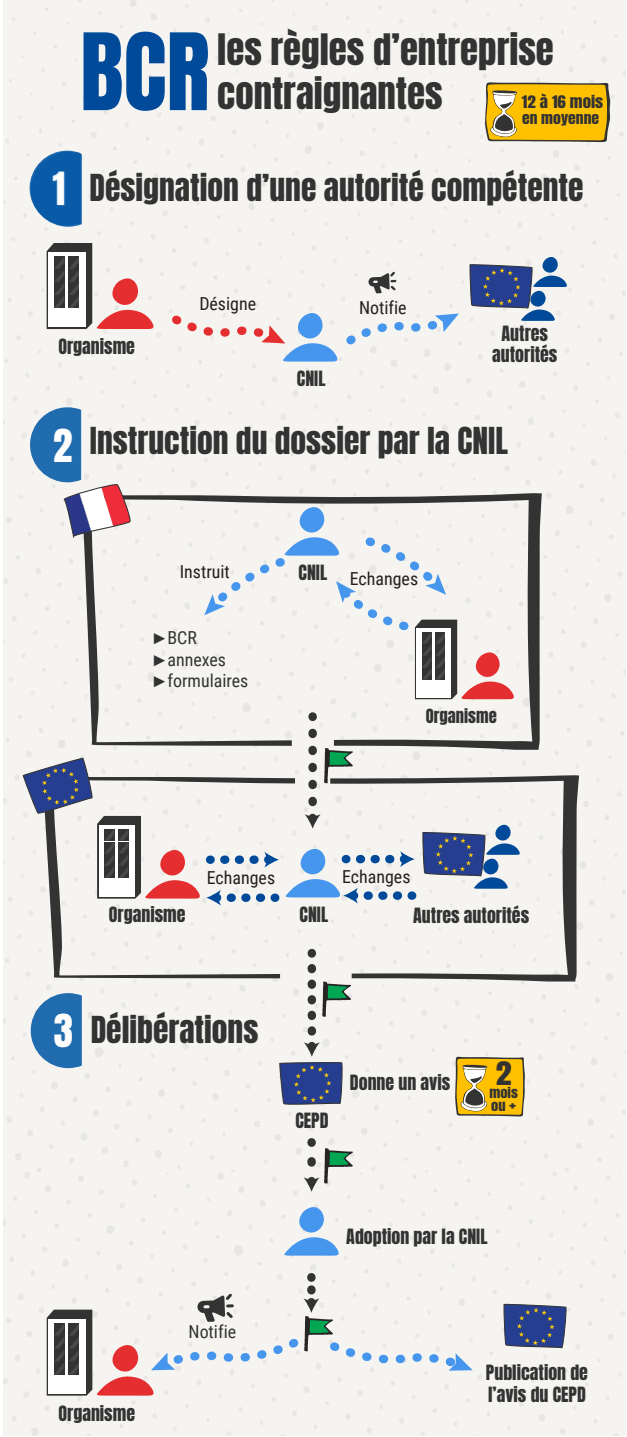
Lorsqu'un code est approuvé, des organismes tiers, dits de contrôle, sont chargés de veiller à sa bonne application par les adhérents. Chaque code peut désigner un ou plusieurs de ces organismes qui, avant d'exercer ce contrôle, doivent solliciter un agrément auprès de l'autorité de protection qui a approuvé le code.

Ainsi, en 2020, de nombreuses autorités ont travaillé à l'élaboration de leurs référentiels nationaux qui seront utlisés pour agréer les organismes de contrôle. Le projet de référentiel de la CNIL a fait l'objet d'une consultation publique avant d'être soumis à l'avis du CEPD, puis adopté définitivement par la CNIL le 24 juillet 2020. En outre, dans le cadre du mécanisme de contrôle de cohérence prévu par le RGPD, la CNIL a participé à l'analyse de 11 projets de référentiels soumis à l'avis CEPD par ses homologues européens.

En complément des travaux menés au niveau européen et national, la CNIL a enrichi son site web d'un dossier complet sur le code de conduite[22]. Elle a également mis en ligne des téléservices dédiés permettant de demander l'approbation d'un code de conduite ou de soumettre une demande d'agrément.

22 Dossier « Les règles d'entreprise contraignantes (BCR) », février 2020, cnil.fr


le code de conduite
8 à 14 mois en moyenne
1 Élaboration du code
Sélectionne
Élabore
Code de conduite Projet
Organisme(s) de contrôle
Porteur du code (fédération, association professionnelle)
2 Échanges
Enregistrement
• par le formulaire de contact
• par les services de la CNIL
Porteur du code
CNIL
Accompagnement (échanges avec le porteur du code)
3 Instruction
CNIL
Code de conduite national
►Instruction par la CNIL
Code de conduite européen
►relecture
CNIL
autorités EU
►avis du CEPD
CNIL Délibération
Approuve
Agrée
Code de conduite
Organisme(s) de contrôle
4 Adhésion et contrôle
Code de conduite
Responsables de traitements
Contrôle de l'application
Code de conduite
Sous-traitants
Organisme(s) de contrôle


BCR les règles d'entreprise contraignantes
12 à 16 mois en moyenne
1 Désignation d'une autorité compétente
Organisme
Désigne
CNIL
Notifie
Autres autorités
2 Instruction du dossier par la CNIL
Instruit
CNIL
Echanges
►BCR
►annexes
►formulaires
Organisme
Organisme
Echanges
CNIL
Echanges
Autres autorités
3 Délibérations
CEPD
Donne un avis
2 mois ou +
Adoption par la CNIL
Notifie
Organisme
Publication de l'avis du CEPD

Les règles d'entreprise contraignantes

Appelées aussi *Binding Corporate Rules (BCR)* en anglais, ces règles désignent une politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne. Les entreprises concernées sont essentiellement des multinationales. Cet outil permet à un groupe **d'unifier les garanties mises en place** concernant les traitements de données personnelles effectués par ses filiales dans le monde entier.

Cet outil de conformité existait avant le RGPD mais celui-ci a modifié la procédure d'approbation des BCR en ajoutant l'obligation de solliciter l'avis du CEPD avant d'approuver le dossier au niveau national. La CNIL a contribué à la refonte opérationnelle et à la mise en application de cette nouvelle procédure d'instruction au niveau européen qui implique, pour chaque dossier, un examen conjoint par les autorités. Ainsi, 9 dossiers d'homologues européens ont été approuvés par le CEPD en 2020 et ont fait l'objet d'une analyse approfondie par la CNIL et de ses homologues.

L'entrée en application du RGPD a conduit à un accroissement significatif du nombre de dossiers BCR : la CNIL gère actuellement 36 dossiers de demandes de BCR pour lesquels elle est autorité compétente.

Comme pour les codes de conduite et la certification, des contenus complets à l'attention des demandeurs ont été publiés sur le site web de la CNIL et un téléservice a été mis en place pour faciliter le dépôt des dossiers[23].

À SUIVRE

Une mise à jour à venir des référentiels d'instruction

La CNIL contribue aux travaux européens de mise à jour des référentiels afin d'en faciliter la lecture pour les demandeurs, de préciser les attentes des autorités et de faire bénéficier les entreprises d'un premier retour d'expérience sur l'instruction des dossiers depuis l'entrée en application du RGPD.

Une fois mis à jour, les référentiels seront directement applicables aussi bien aux groupes détenteurs de BCR qu'à ceux dont les BCR ne sont pas encore approuvés.

L'ACCOMPAGNEMENT DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Placés au cœur du RGPD, les délégués à la protection des données (*DPO pour Data protection officer*) jouent un rôle essentiel dans la mise en conformité opérationnelle des organismes. La CNIL poursuit sa stratégie d'accompagnement spécifique de ces professionnels.

En 2020, cet accompagnement a notamment permis la production de fiches pratiques dont les besoins ont été identifiés par les DPO **sur des sujets d'actualités en lien avec la situation sanitaire ou sur des sujets transversaux**.

En effet, le soutien direct apporté aux DPO par la CNIL (permanence téléphonique et adresse électronique dédiée) a rapidement permis de mettre en évidence l'urgence de répondre à des questions en cours de réflexion notamment au sein des collectivités (par exemple la distribution de masques), d'entreprises (par exemple la prise de température des employés) ou au sein d'établissements d'enseignement (par exemple les modalités de passage des examens à distance).

En outre, la CNIL a souhaité nouer un nouveau partenariat à destination des régions qui, comme toutes les collectivités, traitent de nombreuses données personnelles (gestion de services publics, des ressources humaines, sécurisation des locaux, sites web, etc.).

L'accélération de leur transformation numérique (e-administration, téléservices, *open data*, vidéosurveillance, plateformes en ligne participatives, mobilité intelligente, etc.) s'accompagne d'une prise de conscience croissante des citoyens vis-à-vis de la protection des données.

Dans le même temps, les cyber attaques de nature à porter atteinte à l'intégrité, à la confidentialité et à la disponibilité de ces données, se multiplient.

Dans ce contexte, la CNIL et Régions de France ont souhaité unir leurs efforts pour soutenir ces collectivités dans leurs démarches de mise en conformité en signant une convention de partenariat le 16 septembre 2020.

Dans la même optique, la CNIL a renouvelé cette année son partenariat avec l'ADF, l'Assemblée des Départements de France, dans le prolongement d'une première convention signée en 2017.

23 Dossier « Les règles d'entreprise contraignantes (BCR) », février 2020, cnil.fr

FOCUS

Suites de l'étude sur le métier des DPO

Pour la deuxième année consécutive, la CNIL a participé à une étude menée par la délégation générale à l'emploi et à la formation professionnelle (DGEFP) du ministère du Travail **sur les délégués à la protection des données**.[24]

Les principales conclusions de ces travaux sont les suivantes :

- La compréhension des enjeux liés au RGPD et au rôle du DPO progresse.
- **Les DPO sont souvent confrontés à un manque de moyens**.
- **Les DPO sont mieux positionnés et identifiés au sein des organisations**. Plus de la moitié des DPO internes et mutualisés est rattachée à la Direction Générale.

Un positionnement hiérarchique des DPO (46 %) éloigné du responsable de traitement peut entraîner des difficultés pour rendre compte au responsable de traitement.

- 75 % des DPO n'ont pas d'équipe pour les épauler dans leur mission. Toutefois, 31 % des DPO bénéficient d'un réseau de référents Informatique et Libertés.
- 75 % des DPO exercent leurs missions à temps partiel, et **près de 43 % consacrent moins d'un quart de leur temps de travail à leur mission de DPO**.

FOCUS

La désignation d'un délégué sur le site de la CNIL via un téléservice dédié

Avant de désigner en ligne un délégué à la protection des données, il est important de vérifier et de s'assurer qu'il dispose du **statut**, des **compétences** et des **moyens nécessaires** à l'exercice de ses missions comme prévu par le RGPD.

Pour les DPO mutualisés par des organismes (par exemple auprès de petites collectivités territoriales), une procédure spécifique existe : la permanence téléphonique du service des DPO propose un accompagnement dans cette procédure.

Enfin, pour mettre fin aux missions de votre délégué ou modifier une désignation, envoyez un courriel au service des délégués à l'adresse électronique indiquée dans l'accusé réception de la désignation. Pour toutes vos demandes, n'oubliez pas de préciser le numéro de désignation (DPO-XXX°) ou le numéro SIREN de l'organisme désignant.

Le MOOC « atelier RGPD » dépasse les 100 000 comptes

Depuis le 11 mars 2019, la formation en ligne ouverte à tous (MOOC) intitulée « L'atelier RGPD » propose une initiation au RGPD pour permettre aux professionnels de débuter la mise en conformité de leur organisme.

La CNIL proposera prochainement de nouveaux chapitres dont des contenus dédiés aux **secteurs des collectivités territoriales, de la santé et des ressources humaines**. Ce dispositif d'autoformation en ligne sera complété d'ateliers en ligne (webinaires) et, si possible, en présentiel.

73 331
organismes ont désigné un DPO

1/3
sont issus du secteur public

25 494
DPO désignés (dont 24 451 personnes physiques parfois mutualisées)

42 %
sont des DPO sont des femmes

2 853
appels reçus pendant la permanence juridique dédiée aux DPO

24 « Le délégué à la protection des données (DPD/DPO) : une fonction qui se développe, un métier qui se structure », mis à jour le 21 octobre 2020, travail-emploi.gouv.fr

109 472

comptes créés sur le MOOC de la CNIL

35 110

attestations de suivi délivrées

Une révision à venir du référentiel de certification des compétences du DPO ?

Depuis le 20 septembre 2018, la CNIL peut agréer des organismes en vue de délivrer la certification des compétences du délégué à la protection des données (DPO). **Au 31 décembre 2020, 9 organismes de certification sont agréés par la CNIL.**

Ce dispositif repose sur deux référentiels complémentaires :

- un référentiel de certification qui fixe les conditions de recevabilité des candidatures et la liste des 17 compétences et savoir-faire attendus pour être certifié en tant que DPO ;
- un référentiel d'agrément qui fixe les critères applicables aux organismes qui souhaitent être habilités par la CNIL à certifier les compétences du DPO sur la base du premier référentiel.

Ces deux référentiels prévoient une évaluation dans les deux ans après leur entrée en vigueur. La consultation publique organisée fin 2020 contribue au processus d'évaluation pour décider s'il est nécessaire d'adapter les exigences des référentiels.

UN ACCOMPAGNEMENT SPÉCIFIQUE DES TPE/PME

Les besoins spécifiques des TPE/PME ont été soulignés par le législateur dans le RGPD. En outre, la nécessité d'un accompagnement et d'outils dédiés aux TPE/PME a été rappelée lors d'un bilan réalisé à l'occasion des deux ans d'application du RGPD, en mai 2020. Enfin, la situation sanitaire, doublée d'une crise économique fragilisant particulièrement la situation des TPE/PME, a montré tout l'intérêt de cet accompagnement spécifique et de l'ingénierie mise en place par la CNIL.

La conformité au RGPD doit être prévue lors de la conception et du déploiement de nouveaux outils numériques (par exemple le *click & collect*, qui a connu une forte croissance en 2020), en apportant des garanties en matière d'information des personnes concernées sur l'usage de leurs données, de possibilité d'en contrôler la diffusion et d'en assurer la sécurité : il s'agit d'un vecteur fondamental de confiance pour les utilisateurs.

Si la CNIL accompagne déjà les TPE/PME en mettant à leur disposition différents outils, tels que le guide de vulgarisation du RGPD co-édité avec BpiFrance, des référentiels, le guide des durées de conservation des données, un modèle simplifié de registre ou encore des exemples de mentions d'information, **la stratégie dite « des têtes de réseaux » est indispensable** et complémentaire pour accompagner indirectement l'ensemble des acteurs.

En effet, les TPE et PME forment 95 % du tissu économique français avec 4 millions d'entreprises et le plus souvent, elles ne disposent pas des ressources humaines et économiques nécessaires pour se conformer au RGPD. La CNIL, qui ne peut les accompagner individuellement, a donc mis en œuvre un plan d'action prenant appui sur diverses composantes « têtes de réseaux » (associations, réseaux, fédérations, etc.).

Histoire vécue...

« Je dirige une entreprise de peinture en bâtiment et ne comprenais pas les appels d'offre prévoyant que je devais respecter l'article 28 du RGPD sur les sous-traitants alors que les seules informations dont je dispose sont les coordonnées des architectes. La CNIL m'a précisé que les prestataires ne sont pas tous des sous-traitants au sens du RGPD. Comme ma prestation ne concerne qu'à titre accessoire, sinon accidentel, un traitement de données personnelles, je suis seulement destinataire et non sous-traitant. Bien sûr, je ne laisse pas traîner cette liste et par ailleurs j'ai mon fichier de clients et salariés pour lequel je suis responsable de traitement. »

Des conventions de partenariat

L'identification et le rapprochement de la CNIL avec les relais naturels des entreprises a conduit à la signature de deux nouvelles conventions de partenariat en 2020 au bénéfice des TPE/PME : avec le médiateur des entreprises à Bercy, le 16 septembre, et avec le Conseil supérieur de l'ordre des experts-comptables, le 29 septembre.

Le constat est partagé par la CNIL et ces structures de conseil : les dirigeants de TPE/PME ont besoin d'un accompagnement en matière de conformité au RGPD, accru avec la crise sanitaire du fait d'une accélération de la transformation numérique des entreprises, d'une expansion du télétravail et du développement de la vente en ligne.

Des guides et outils d'évaluation réalisés avec le soutien de la CNIL

Les associations professionnelles développent des guides pratiques et des outils d'évaluation réalisés sur la base des activités spécifiques de leurs adhérents, avec le soutien de la CNIL.

La démarche d'accompagnement mise en place consiste à **identifier, structurer et animer les têtes de réseaux**, tant dans leur production de guides pratiques qu'en répondant aux demandes de conseil spécifiques à leur secteur d'activité. La CNIL participe ainsi à des réunions, des conférences et propose, depuis l'entrée en application du RGPD, des contenus pour les publications professionnelles (elle a participé, par exemple, à un guide et un outil d'autoévaluation (EvalRGPD) publiés par la CPME en 2018).

Ce réseau comprend, en 2020, une centaine de fédérations et associations professionnelles, soit le double de 2019.

FOCUS

La CNIL, partenaire de France Num

La CNIL est partenaire de France Num, piloté par la direction générale des entreprises du ministère de l'économie. Cette initiative vise l'accompagnement des TPE/PME dans leur transformation numérique. Dans ce cadre, la CNIL coordonnera ses actions avec celles des partenaires publics et réseaux privés ainsi qu'avec celle des « activateurs », experts du numérique.

RENFORCER
la sécurité

La sécurité des données personnelles est, au-delà d'une obligation légale, un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. Tous les organismes sont aujourd'hui touchés par les attaques, quels que soient leur taille et leur secteur. La CNIL reçoit, chaque année, de nombreuses notifications de violations de données qui peuvent avoir de lourdes conséquences. Elle offre, en coopération avec d'autres parties prenantes de la cybersécurité, de nombreuses ressources et conseils pour accompagner tous les acteurs.

Christophe
Adjoint au chef du service de l'expertise technologique

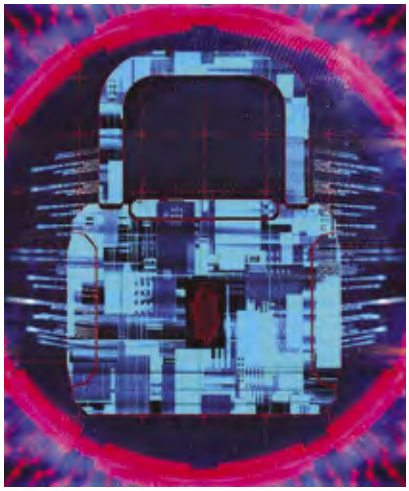
Nous sommes 13 experts au sein du service (ingénieurs, chercheurs, consultants, designers), chacun avec ses domaines de prédilection, comme la cybersécurité, la biométrie, les objets connectés, le big data, la cryptographie, le cloud ou encore la normalisation.

Notre rôle est, d'une part, d'épauler les autres services, sur les aspects techniques des demandes soumises à la CNIL, qu'il s'agisse de demandes de conseil, de demandes d'avis sur un projet de texte, ou lors des phases contentieuses lorsqu'une expertise particulière est nécessaire ; d'autre part, de détecter, en avance de phase, quelles vont être les tendances et nouveautés technologiques afin de les appréhender et de les confronter à la loi avec l'objectif final de permettre une vraie innovation technologique, efficace et respectueuse de la règlementation relative à la protection des données.

Nous disposons également de notre « Labo », où nous effectuons des expérimentations, pour identifier les usages émergents et nouvelles problématiques, vérifier la conformité des équipements ou développer des preuves de concept, par exemple pour essayer de suivre les flux d'information entre les assistants connectés et les opérateurs de ces derniers.

Enfin, nous sommes en interaction avec les différents publics de la CNIL et les acteurs du paysage français de la cybersécurité, notamment par le biais de nos interventions au FIC ou aux Assises de la sécurité, par le traitement des notifications de violations de données et des échanges générés par ces dernières avec les autres autorités, aussi bien européennes, en charge de la protection des données, que françaises en charge de la cyberdéfense/sécurité.

UNE PARTICIPATION CONSTANTE À L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ



Au-delà de l'accompagnement des responsables de traitement dans le déploiement de traitements sécurisés et des contrôles amenant à constater les défauts préjudiciables, la CNIL doit avoir **connaissance des enjeux liés à la cybersécurité**. Cela passe notamment par le partage de connaissances entre chacune des parties prenantes.

INFOSPLUS

Les obligations prévues par les articles 32 (sur la sécurité du traitement), 33 et 34 (sur les violations de données), et 35 (sur les analyses d'impact) du règlement général sur la protection des données (RGPD) sont les seules dispositions légales relatives à la cybersécurité qui s'imposent à l'ensemble des entreprises et des administrations.

Les bouleversements des usages du numérique, notamment dus au confinement de 2020, ont conduit à une évolution importante des menaces. La CNIL participe activement aux échanges avec les professionnels du secteur de la cybersécurité pour permettre **une maîtrise des menaces, des risques** et des solutions en usage dans les organismes.

Ces échanges avec les responsables de traitement, sous-traitants, éditeurs ou associations, publics comme privés, réunissant les personnes compétentes sur les sujets de la cybersécurité et de la maîtrise des risques numériques, ont pour objectif une meilleure prise en compte de solutions de sécurité efficientes pour améliorer la protection des données et de la vie privée de chacun.

Les forums et conférences

La CNIL, partie prenante de l'écosystème cybersécurité a participé en 2020 :

- au **Forum international de la cybersécurité** (FIC) organisé les 28, 29 et 30 janvier 2020 à Lille. Cet évènement annuel, qui a réuni plus de 12 500 participants, est l'opportunité pour la CNIL d'un partage d'expérience autour des enjeux de protection des données personnelles et de cybersécurité.

- aux **Assises de la sécurité,** du 14 au 17 octobre 2020 à Monaco, l'occasion d'échanger avec les décideurs du marché de la cybersécurité sur l'évolution des solutions technologiques.

La CNIL est également membre du **Club EBIOS** (expression des besoins et identification des objectifs de sécurité) qui fédère des organismes et des experts individuels du secteur public et du secteur privé, français et étrangers concernés par la gestion des risques autour cette méthode. La CNIL siège au sein de son conseil d'administration, ce qui lui permet notamment d'échanger sur les pratiques d'analyse de risques mises en œuvre par les organismes pour répondre aux obligations du RGPD.

Elle a également eu l'opportunité d'échanger avec le GIP ACYMA (groupement d'intérêt public action contre la cybermalveillance) qui a lancé en février 2020 la nouvelle version de sa plateforme d'assistance aux victimes. Destinée aux particuliers, aux entreprises et aux collectivités, cette plateforme propose des conseils ainsi que des contenus de prévention et de sensibilisation à la sécurité numérique. La CNIL a notamment suggéré des contenus et des liens vers son site web pour les cas où les actes de cybermalveillance donnent lieu à des compromissions de données personnelles.

Cette implication dans l'écosystème cyber se poursuivra dans les années à venir, avec de nouvelles perspectives offertes par le futur **Campus Cyber**, dont l'ouverture est prévue en octobre 2021.

INFOSPLUS

La CNIL poursuit sa participation active au sein des instances internationales de normalisation, notamment auprès de l'ISO qui a publié l'an dernier la norme 27701 sur la protection des données personnelles.

L'ISO vient de compléter ce dispositif avec la norme 27006-2 destinée à encadrer les organismes certificateurs délivrant des certificats ISO 27701, ce qui constitue un jalon important dans l'adoption et la reconnaissance de cette norme par les professionnels.

UNE PRISE DE CONSCIENCE CROISSANTE DES ORGANISMES

La CNIL constate **une réelle prise de conscience liée aux enjeux de cybersécurité** au sein des organismes. Celle-ci passe par le développement des échanges entre les responsables des métiers, les responsables de la protection des données, les responsables des risques et de la sécurité et la direction des systèmes d'information. Cette pluridisciplinarité est une nécessité : **il ne peut, en effet, y avoir de protection des données sans sécurité.**

Néanmoins, si cette évolution se traduit par une meilleure anticipation dans les projets liés aux systèmes d'information, les règles de base en sécurité ne sont pas toujours respectées. En particulier, les organismes de taille moyenne, souvent insuffisamment équipés en matière de sécurité informatique ont été particulièrement touchés par la vague de rançongiciels qui frappe l'ensemble des entreprises et administrations depuis quelques années et notoirement en 2020 et début 2021.
Aujourd'hui encore, de nombreux manquements relevés par la CNIL concernent des règles élémentaires de protection et de sécurité. Elles devraient pouvoir être prises en compte plus largement dans le socle de sécurité comme pour le chiffrement des échanges sur supports numériques amovibles, la mise en œuvre d'un chiffrement de surface des disques des ordinateurs portables, qui font souvent défaut, ou encore l'utilisation de fonctions cryptographiques à l'état de l'art.

Le CLUSIF (Club de la sécurité de l'information français) note dans son dernier rapport MIPS (Menaces informatiques et pratiques de sécurité en France) publié en 2020, le fait que « le chiffrement continue sa (trop lente ?) progression à 59 % (vs 40 % en 2018) sur les PC portables et 59 % (vs 42 % en 2018) pour le chiffrement des échanges »[25].

INFOSPLUS

À la suite d'une vague de cyberattaques visant des établissements de santé, le président de la République a annoncé, le 18 février 2021, affecter un milliard d'euros, dont 720 millions d'euros de fonds publics, pour renforcer la filière de la cybersécurité en France.

La CNIL a également pu constater des manquements liés à ce défaut de déploiement de solutions de chiffrement adéquates, tant lors de ses contrôles que dans le cadre des notifications de violations de données qui lui ont été adressées. **La mise en place de ces solutions doit devenir un réflexe.**

25 « MIPS 2020 – Menaces Informatiques et Pratiques de Sécurité en France – Édition 2020 (Rapport global) », 10 juillet 2020, clusif.fr

LES VIOLATIONS DE DONNÉES PERSONNELLES

2 825

Notifications reçues en 2020

+ 24 %

Un nombre record de notifications

L'année 2020 a vu le nombre de violations de données notifiées à la CNIL **en progression de 24 %** par rapport à l'année précédente. En effet, la CNIL a reçu **2 825 notifications de violations de données personnelles**, contre 2 287 en 2019. En moyenne, plus de 11 notifications ont été reçues par jour ouvré et plus de **265 notifications sont reçues par mois**. Par ailleurs, des « pics » de notifications sont parfois observés, notamment lorsqu'un sous-traitant informe ses nombreux clients, responsables de traitement, d'une violation de données les concernant. Ceux-ci étant tenus de notifier la CNIL sous 72 heures, comme prévu par l'article 33 du RGPD, jusqu'à 62 notifications ont ainsi été reçues sur un seul jour.

Environ **27 % des notifications** reçues en 2020 concernent des violations concernant **plus de 1 000 personnes**, un chiffre stable par rapport à 2019.

17 % des notifications concernaient des **données sensibles**, chiffre en hausse par rapport à 2019 (14 %).

Ces notifications ont été à la source de 56 procédures de contrôle.

Les secteurs d'activité les plus concernés

L'administration publique est à l'origine d'un peu plus de **16 % des notifications reçues** cette année, avec une progression de 28 % par rapport à l'année dernière. Le **secteur de la santé et de l'action sociale** est, quant à lui, celui pour lequel le nombre de notifications a le plus progressé par rapport à 2019 (**+ 83 %**). En effet, cette année encore, de nombreuses collectivités territoriales (telles que les communes ou les métropoles) et des organismes de santé (en particulier les établissements poursuivant des activités hospitalières) ont subi des incidents de sécurité souvent liés à des attaques par rançongiciel (voir encadré). Cette progression peut également s'expliquer par une autre obligation de ces organismes, désigner un délégué à la protection des données, ainsi que par une meilleure maturité sur les questions relatives à la cybersécurité, notamment une meilleure considération de tous les enjeux liés aux violations de données, dans le tissu économique.

Tous les organismes sont concernés par des incidents de sécurité, des multinationales aux très petites entreprises.

Natures et causes des violations notifiées

Comme en 2019, la majorité **(69 %)** des notifications de violations reçues par la CNIL concerne une **perte de confidentialité**. Bien que le RGPD considère qu'une violation de données personnelles peut aussi résulter d'un incident de sécurité engendrant une perte d'intégrité et de disponibilité, les statistiques démontrent que ce type de violation de données reste encore trop méconnu des responsables de traitement. Toutefois, la CNIL constate **une nette progression des notifications liées à une perte d'intégrité et de disponibilité** comparée à l'année précédente, notamment due à la progression des violations résultant d'une attaque par rançongiciel (voir l'encadré page 78).

INFOSPLUS

Les données sensibles forment une catégorie particulière de données. Leur traitement est, sauf exceptions particulières, interdit par le RGPD.

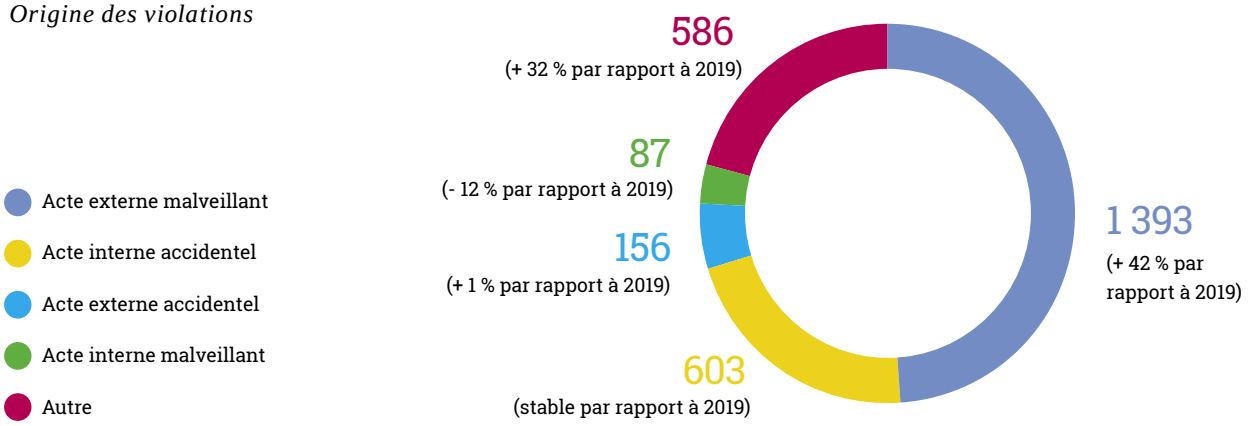
Ces données comprennent notamment les informations relatives à la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses, les données biométriques, ou encore les données de santé.

> **« Tous les organismes sont concernés par des incidents de sécurité, des multinationales aux très petites entreprises.**

Secteurs d'activité	2020	%	Progression
Administration publique, dont les administrations centrales et déconcentrées, les collectivités et leurs opérateurs (Code NAF O)	459	16 %	+ 28 %
Activités spécialisées, scientifiques et techniques (Code NAF M)	364	13 %	+ 11 %
Commerce ; réparation d'automobiles et de motocycles (Code NAF G)	339	12 %	+ 55 %
Santé humaine et action sociale (Code NAF Q)	319	11 %	+ 83 %
Activités financières et d'assurance (Code NAF K)	311	11 %	+ 5 %
Information et communication (Code NAF J)	216	8 %	+ 7 %
Industrie manufacturière (Code NAF C)	173	6 %	+ 38 %
Autres activités de services (Code NAF S)	132	5 %	+ 21 %
Activités de services administratifs et de soutien (Code NAF N)	108	4 %	- 4 %
Enseignement (Code NAF P)	97	3 %	+ 3 %
Transports et entreposage (Code NAF H)	90	3 %	- 5 %
Activités immobilières (Code NAF L)	72	3 %	+ 36 %
Autres	145	5 %	+ 21 %
TOTAL	**2 825**	**100%**	**+24%**

Nature de la violation	Nombre	Proportion	Progression par rapport à 2019
Perte de la confidentialité (données rendues accessibles à une personne non autorisée)	1 938	69 %	+ 10 %
Perte de la disponibilité (données inaccessibles pendant un certain temps)	243	9 %	+ 59 %
Perte de l'intégrité (données modifiées illégitimement)	25	1 %	- 34 %
Perte de la confidentialité, Perte de l'intégrité, Perte de la disponibilité	192	7 %	+ 140 %
Perte de la confidentialité, Perte de la disponibilité	191	7 %	+ 40 %
Perte de la confidentialité, Perte de l'intégrité	142	5 %	+ 56 %
Perte de l'intégrité, Perte de la disponibilité	94	3 %	+ 224 %
TOTAL	**2 825**	**100 %**	**+ 24 %**

Origine des violations



La majorité des notifications reçues par la CNIL en 2020 concerne une violation de données ayant pour origine un acte externe malveillant (piratage, vol d'un support physique ou les arnaques aux faux supports techniques), même si l'obligation de notification à l'autorité de contrôle d'une violation de données concerne aussi les violations d'origine accidentelle ou illicite. En 2020, **le piratage informatique a ainsi représenté 47 % du total des notifications et 94 % des actes externes malveillants notifiés à la CNIL**, soit **1 315 notifications** contre 772 en 2019 (**+ 70 %**).

L'attaque la plus répandue reste le **rançongiciel**. Sur l'année 2020, la CNIL a reçu **plus de 500 notifications** résultant d'un rançongiciel.
Ce nombre représente un peu moins de **20 % du volume total des notifications** reçues sur la période et un peu plus de 40 % des violations liées à une attaque informatique.

+ de 500

Notifications de violations résultant d'une attaque par rançongiciel reçues en 2020

Soit 20 %

du volume total

FOCUS

Le télétravail : un nouveau vecteur de violations de données

De nombreuses notifications de violations de données, reçues durant le premier confinement, sont directement liées à une mauvaise gestion des outils permettant le télétravail. Le recours massif au télétravail a en effet engendré des mauvaises pratiques qui ont favorisé les attaques par rançongiciels et par hameçonnage du fait :

- de mauvaises configurations des outils de sécurité (réseau privé virtuel (VPN) non sécurisé, correctifs de sécurité mal ou non appliqués, mauvais paramétrage des contrôles d'accès, etc.) ;
- d'un assouplissement non maîtrisé des mesures de sécurité (politique de changement de mots de passe affaiblie, contournement de la restriction des adresses IP pour permettre le travail à distance, etc.) ;
- d'une explosion de transmissions de données par courriel, entrainant une augmentation significative de divulgations non autorisées de données.

De même, la situation a facilité les tentatives d'attaque au cours desquelles un tiers non autorisé contacte un organisme en se faisant passer pour un collaborateur distant ayant besoin d'accéder à une ressource de l'entreprise.

Enfin, le télétravail a pu complexifier la fluidité des échanges entre collaborateurs en cas de violation de données pour identifier l'origine de l'incident de sécurité, pour documenter de façon adéquate la violation, pour restaurer rapidement les systèmes compromis et pour notifier la violation à la CNIL dans les délais impartis.

Dans ce contexte, la CNIL a publié en mai 2020 une série de conseils pour mettre en place le télétravail dans des bonnes conditions de sécurité.[26]

26 « Les conseils de la CNIL pour mettre en place le télétravail », 12 mai 2020, cnil.fr

FOCUS

Les attaques par rançongiciel

Le rançongiciel (*ransomware* ou *cryptolocker* en anglais) est un programme malveillant qui empêche l'accès de la victime à ses données, en les chiffrant avec une clé connue uniquement de l'attaquant, qui va ensuite demander une rançon à la victime en échange de la clé de déchiffrement.

Ce programme malveillant se transmet souvent par une pièce jointe de courriel ou des liens permettant le téléchargement de logiciels ou de contenus. Une fois présent sur son « hôte », le terminal cible, ce programme va progressivement chiffrer tous les fichiers qui lui sont accessibles afin de les rendre illisibles par les utilisateurs. Dans le cas d'un réseau d'entreprise, le logiciel va chercher à se propager sur toutes les ressources accessibles.

L'attaquant demande alors une rançon, payable en cryptomonnaie, à la personne ou à l'organisme victime en échange de la clé permettant de déchiffrer les fichiers. Si ce type d'attaque est parfois opportuniste, pour des rançons correspondant généralement à quelques centaines d'euros, de plus en plus d'entités de tailles importantes (grandes entreprises, collectivités locales, établissements de santé) sont ciblées par les attaquants pour des montants pouvant atteindre plusieurs millions d'euros. En outre, **le paiement de la rançon ne garantit pas que l'ensemble des données sera bien restitué et naturellement, il n'immunise pas les organismes contre une nouvelle attaque du même type**. Il est donc essentiel de correctement **sécuriser son réseau** et en particulier de disposer de **sauvegardes à jour** et testées, permettant de reconstruire rapidement les systèmes d'information en cas de destruction par un rançongiciel.

Certains rançongiciels utilisent des failles de sécurité connues afin de se propager via le réseau des organismes touchés et de multiplier les dommages. En particulier, en rendant inaccessibles les serveurs, logiciels et données de leurs victimes, les rançongiciels entraînent une indisponibilité de services critiques (le site web d'un organisme, les services destinés aux utilisateurs ou les moyens de communication interne à l'organisme) et très souvent une altération et/ou une perte de disponibilité des données personnelles, ce qui constitue alors une violation de données personnelles.

Les recommandations de la CNIL

La CNIL recommande aux organismes de mettre en œuvre des mesures de sécurité pour réduire le risque d'attaque par rançongiciel ou en limiter les conséquences, notamment :

- faire des sauvegardes régulières des données, les tester régulièrement et en conserver au moins une copie hors du réseau de l'organisme ;
- maintenir à jour ses systèmes et logiciels (antivirus, équipements pare-feu...) ;
- ne pas utiliser de compte ayant des droits « administrateur » pour l'usage quotidien (le recours aux droits « administrateur » doit être limité aux seules actions le nécessitant) ;
- ne pas installer de logiciels piratés ou issus de sources non fiables ;
- utiliser un proxy web permettant de bloquer les sites pouvant diffuser de tels logiciels.

Il est également essentiel de sensibiliser tous les utilisateurs internes, via, par exemple, des communications régulières par courriel :

- ne pas ouvrir les pièces jointes, ni cliquer sur les liens présents dans les courriels dont la provenance n'est pas fiable (surtout lorsque les pièces jointes ont une extension suspecte (.scr, .cab, etc.)) ;
- ne pas installer d'application ou de programme dont l'origine n'est pas sûre ;
- éviter les sites non sûrs ou illicites.

INFOSPLUS

Les ressources utiles pour comprendre les attaques et s'y préparer

La CNIL propose de nombreux conseils pratiques sur son site web (notamment dans son dossier thématique « Cybersécurité » et communique très régulièrement sur des problématiques liées à la cybersécurité.

En particulier, elle propose depuis octobre un nouveau format de publication, « la violation du trimestre », qui revient sur les attaques les plus fréquentes et donne quelques bonnes pratiques pour les éviter ou en limiter les conséquences. Les deux premières « violations du trimestre » explorent ainsi les attaques par injection SQL et *credential stuffing*.

La CNIL a également publié, en janvier 2020, un guide pour les développeurs, offrant ainsi une première approche des grands principes du RGPD et des différents points d'attention à prendre en compte dans le déploiement d'applications respectueuses de la vie privée des utilisateurs.

De plus, elle a contribué à un guide de sensibilisation aux cyberattaques de l'ANSSI et du ministère de la Justice : « Attaques par rançongiciels, tous concernés », publié en septembre.

En outre, elle a publié une fiche de bonnes pratiques sur le moteur de recherche et d'analyse Elasticsearch, largement utilisé aujourd'hui, souvent visé par des attaques, et sur lequel de nombreux déploiements ne prennent pas en compte les règles élémentaires de sécurité.

Enfin, la CNIL a participé au « Baromètre *Data Breach* » sur la gestion du risque de violation de données, publié par PwC et Bessé à l'occasion du Forum international de la cybersécurité 2020. Ce baromètre a exploité des données issues des publications de la CNIL sur la plateforme data.gouv.fr et permet de connaître les tendances en termes d'atteintes aux données personnelles.

PARTICIPER
à la régulation internationale

La CNIL est membre de plusieurs instances européennes et internationales, notamment du Comité européen de la protection des données (CEPD). Elle participe également à de nombreuses conférences sur le thème de la protection des données personnelles dans le monde afin d'apporter des réponses homogènes à des enjeux de plus en plus généralisés pour les droits des personnes.

Florence
Cheffe du service des affaires européennes et internationales

Le service des affaires européennes et internationales coordonne et défend les positions de la CNIL dans les enceintes européennes et internationales. Ainsi, nous participons activement aux travaux du Comité européen de la protection des données (CEPD), du Conseil de l'Europe, de l'OCDE et de l'Assemblée mondiale des commissaires à la protection des données (Global Privacy Assembly). Grâce à une équipe engagée et motivée, nous sommes moteurs sur un grand nombre d'initiatives discutées dans ces instances. Nous sommes aussi présents aux côtés des autres services de la CNIL pour renforcer la coopération avec nos homologues.

Cette année a été fortement marquée par des situations extraordinaires comme l'impact de la pandémie sur la protection des données ou encore la décision de la Cour de justice de l'Union européenne sur les transferts de données hors Union européenne. Nous avons vécu une année intense autour de nouveaux enjeux. Dans ce cadre, je suis profondément fière de pouvoir promouvoir, à l'étranger, les valeurs fondamentales du pays des libertés individuelles et d'agir pour toujours plus de convergence au plan mondial.

Alors que les initiatives numériques pour contribuer à la lutte contre la propagation du virus se sont multipliées partout en Europe, les autorités européennes et le CEPD ont été, plus que jamais, sollicités. Cette année a également permis de recourir aux mécanismes et procédures de coopération européenne, des outils précieux et essentiels.

DEUX ANS DU RGPD : UN BILAN POSITIF POUR L'EUROPE

L'année 2020 s'est ouverte au niveau européen avec la contribution du Comité européen à la protection des données (CEPD) à la revue du RGPD.

La Commission européenne a présenté au Parlement européen et au Conseil de l'UE un rapport sur l'évaluation et le réexamen de ce règlement : le CEPD a contribué à cet exercice et a fait son bilan, positif, des deux premières années d'application du RGPD.

Ainsi, parmi les réalisations du CEPD, 1 392 cas ont été soumis sur la plateforme de coopération IMI (voir encadré) et 168 décisions finales ont été adoptées.

Bien que le besoin de ressources pour toutes les autorités soit toujours une préoccupation et que certains défis subsistent, liés par exemple aux différentes procédures nationales, le CEPD est convaincu que la coopération entre les autorités renforcera la culture commune de protection des données.

Dans son évaluation, le CEPD a également abordé des questions sur lesquelles il est très impliqué, telles que les transferts internationaux de données, l'impact du RGPD sur les PME, ou le développement de nouvelles technologies. Il conclut sur le fait qu'**il serait prématuré d'envisager une révision du RGPD à ce stade.**

INFOSPLUS

Le CEPD

Le Comité européen de la protection des données (CEPD ou EDPB en anglais) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données.

Il est composé, entre autres, des différentes CNIL européennes et du Contrôleur européen de la protection des données (la CNIL des institutions européennes).

UNE COORDINATION EUROPÉENNE DE PLUS EN PLUS HARMONISÉE

La CNIL est particulièrement active dans les travaux du CEPD, à travers sa participation aux séances plénières, aux sous-groupes (elle coordonne plusieurs d'entre eux) ou encore aux équipes de rédaction des différents documents produits.

Thème fort de cette année 2020, la coordination des autorités de contrôle a constitué un axe important de travail au niveau européen. Le CEPD a en effet entamé une réflexion sur l'amélioration continue des procédures de coopération existantes et sur son plan stratégique.
Le CEPD a ainsi établi ses priorités et orientations stratégiques pour les trois années à venir. L'adoption de la stratégie européenne 2021-2023[27] en fin d'année a représenté l'aboutissement de ce travail et s'articule autour de 3 piliers :

1. la poursuite de l'harmonisation de la conformité ;
2. le soutien à une application effective de la législation et une coopération efficace entre les autorités nationales de contrôle ;
3. et enfin une approche des nouvelles technologies fondée sur les droits fondamentaux.

Les programmes de travail détaillés des sous-groupes, reflétant la stratégie du CEPD, seront publiés début 2021.

Les questions de la coordination et de la coopération ont également irrigué les travaux : des lignes directrices sur des notions clés ont été adoptées, par exemple sur la notion d'objection pertinente et motivée, ou sur le consentement. Des travaux sont actuellement menés sur la coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle (article 60 du RGPD).

Établi fin 2019, le comité de la supervision coordonnée au sein du CEPD a entamé ses travaux afin d'assurer la coordination entre autorités dans la supervision des systèmes d'information de l'Union européenne. Les groupes de

27 « EDPB Strategy 2021-2023 » (en anglais), 15 décembre 2020, edpb.europa.eu

supervision coordonnée existants en dehors du cadre du CEPD, notamment ceux consacrés aux systèmes d'information Schengen (signalements concernant des objets ou des personnes dans l'UE), à Eurodac (empreintes digitales des demandeurs d'asile) ou Europol (lutte transfrontalière contre le terrorisme, le trafic de drogues et autres crimes graves), ont également poursuivi leurs travaux en portant une attention particulière aux questions d'interopérabilité.

DÉFINITION

La plateforme IMI

La plateforme IMI (Internal Market Information System) est une solution mise à disposition par la Commission européenne pour les autorités de contrôles de l'UE.

Cette plateforme permet l'échange sécurisé d'informations dans le cadre des différentes procédures de coopération prévues par le RGPD.

Enfin, les communications entre les autorités de protection des données via la plateforme informatique de coopération « IMI » ont encore augmenté, que ce soit dans le cadre du mécanisme dit du « guichet unique » ou de la coopération informelle. Dans ce contexte, cette année 2020 a été marquée par la première décision du CEPD sur le fondement de l'article 65 du RGPD ; il a ainsi pu se prononcer pour la première fois pour arbitrer un désaccord entre une autorité chef de file et des autorités concernées (voir la partie « La coopération européenne sur les plaintes, contrôles et sanctions », page 47).

28 « EDPB Strategy 2021-2023 » (en anglais), 15 décembre 2020, edpb.europa.eu

Le dialogue européen face à la crise sanitaire

Le dialogue mené au sein du CEPD s'est révélé extrêmement précieux pour **apporter des positions européennes communes** face à la crise, sur des sujets aussi centraux que les applications de suivi de contact ou le traitement des données de santé à des fins de recherche scientifique dans le cadre de la lutte contre le virus.

Plus que jamais sollicité dans le cadre de la pandémie (voir page 33) mais également du fait de l'invalidation par la Cour de justice de l'Union européenne (CJUE) du bouclier de protection de la vie privée, le *Privacy Shield* (voir page 44), le CEPD n'en a pas moins continué son activité sur tous les autres sujets sur lesquels il est appelé à se prononcer.

Les outils de conformité pour les transferts

Indépendamment des questions directement liées à l'invalidation de la décision d'adéquation du Privacy Shield (arrêt Schrems II), le CEPD a poursuivi ses travaux en matière de transferts de données : les premières lignes directrices sur ces transferts entre les autorités et organes publics de l'Espace économique européen (EEE) et les pays tiers ont été adoptées.

Le CEPD a continué ses travaux sur les codes de conduites et les règles d'entreprises contraignantes (ou BCR - voir page 67), en recourant à des procédures simplifiées d'adoption par procédure écrite dès lors que les autorités étaient parvenues à un consensus. Ainsi, le CEPD a approuvé 14 BCR depuis l'entrée en application du RGPD, dont 9 en 2020. En ce qui concerne les nouvelles clauses contractuelles types (les modèles de contrat de transfert de données personnelles), le CEPD a préparé un avis conjoint avec le Contrôleur européen de la protection des données sur les nouveaux jeux de clauses proposés par la Commission européenne, adopté tout début 2021.

Le CEPD a également entamé une réflexion sur les garanties contractuelles à mettre en place dans l'hypothèse d'un transfert depuis un sous-traitant présent dans l'Union vers un responsable de traitement hors UE soumis au RGPD. Enfin, dans le contexte du Brexit et en prévision de la fin de la période transitoire, le CEPD devra se prononcer sur la nouvelle situation du transfert de données vers le Royaume-Uni ; il sera consulté par la Commission européenne sur la future adéquation du Royaume-Uni (voir page 48).

Vers une homogénéisation des différents textes

Le CEPD continue de suivre les travaux menés par les institutions européennes. Il a ainsi adopté une lettre à destination du Conseil de l'Europe sur la révision de la Convention de Budapest (sur la cybercriminalité), soulignant la nécessité d'intégrer de solides garanties en matière de protection des données dans le futur protocole additionnel à la Convention et de veiller à sa cohérence avec la Convention 108 (du Conseil de l'Europe), ainsi qu'avec les traités de l'UE et la Charte des droits fondamentaux.

Il a en outre adopté une déclaration relative au futur règlement ePrivacy dans laquelle il fait part de ses inquiétudes relatives à certaines nouvelles orientations des discussions au Conseil, notamment quant au rôle futur des autorités et du CEPD.

Il travaille aussi actuellement et sur demande de la Commission européenne à un avis conjoint avec le Contrôleur européen à la protection des données sur le futur *Data Governance Act*.

Le CEPD a également mené des travaux en matière de reconnaissance faciale. Dans sa réponse aux députés du Parlement européen en ce qui concerne l'entreprise Clearview AI, il a fait part de ses préoccupations au sujet de certaines évolutions dans le domaine des technologies de reconnaissance faciale et de leur utilisation par les services répressifs. Il a décidé d'approfondir le sujet dans le cadre de la rédaction de lignes directrices sur l'utilisation de la reconnaissance faciale par les services répressifs, qui viendront utilement compléter les travaux déjà menés par la CNIL en 2019[28].

INFOSPLUS

La Convention 108

La Convention 108 du Conseil de l'Europe, ouverte à la signature en 1981, est le premier instrument international juridique dans le domaine de la protection des données, et porte notamment sur la protection de la vie privée des citoyens.

Ce texte est contraignant : les signataires, parmi lesquels figure la France, doivent prendre les mesures nécessaires dans leur droit national, pour en appliquer les principes.

Le CEPD a par ailleurs publié des lignes directrices sur le consentement, la deuxième directive sur les services de paiement (DSP2), des lignes directrices sur le ciblage publicitaire des utilisateurs des médias sociaux, des lignes directrices sur la protection des données dès la conception et par défaut, et sur les notions de responsables de traitement et sous-traitants.

Il a également initié de nouvelles modalités de communication avec le public et les parties prenantes. Dans le cadre de l'adoption des lignes directrices sur la notion d'intérêt légitime, un évènement en ligne a ainsi été organisé afin de recueillir les avis et positions des acteurs concernés. D'autres évènements de ce type seront proposés à l'avenir.

LES TRAVAUX DE LA CNIL EN DEHORS DE L'UNION EUROPÉENNE

En dehors de l'Union européenne, la CNIL a participé à la première réunion de l'Assemblée mondiale de la vie privée (Global Privacy Assembly), qui rassemble plus de 120 autorités issues de tous les continents. Sous la présidence de l'ICO, l'autorité de protection des données britannique, l'Assemblée développe sa stratégie d'influence en matière de politique numérique ainsi que des initiatives de dimension internationale, comme la mise en place d'un panel de référence composé de personnalités venues de différents horizons (académiques, société civile, entreprises).

La CNIL continue de participer activement à l'animation du réseau en assurant la coprésidence de deux groupes de travail (éducation au numérique et éthique et protection des données dans l'intelligence artificielle) et en contribuant de manière substantielle aux différents travaux menés dans les autres sous-groupes de l'Assemblée, en particulier celui consacré à la comparaison des standards internationaux en matière de protection des données. Ce dernier a accompli un important travail afin de mettre en lumière les principes clés de la protection des données partagés dans le monde. Ce travail se poursuivra en 2021, en se concentrant plus particulièrement sur les outils de transferts et sur les principes relatifs à l'accès par les gouvernements aux données.

Réunies virtuellement en octobre, les autorités ont adopté plusieurs résolutions :

- Deux résolutions ont porté sur la technologie de reconnaissance faciale : une sur ce sujet proprement dit et l'autre sur la responsabilité dans le développement et l'utilisation de la reconnaissance faciale.
- Une résolution a été adoptée sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise.
- Une autre, sur les déclarations conjointes sur les questions internationales émergentes.

L'ensemble des documents (rapports et résolutions) est disponible sur le site web de l'Assemblée[29]. Les résolutions ont été traduites en français.

DÉFINITION

Le **Conseil de l'Europe** est une organisation intergouvernementale créée en 1949 par le traité de Londres et qui compte 47 États membres. Il n'est pas organiquement lié à l'Union européenne bien qu'il participe avec elle, comme avec d'autres entités, à la mise en place de différents programmes.

Il produit des normes, chartes et conventions parfois contraignantes (par exemple la Convention 108).

Il ne doit pas être confondu avec le **Conseil de l'Union européenne**, qui est une des principales institutions de l'UE, au même titre que le Parlement européen (avec qui il négocie et adopte la législation de l'UE) et la Commission européenne (qui propose des textes).

29 « Adopted resolutions » (page en anglais), globalprivacyassembly.org

Le point sur les lignes directrices RGPD adoptées en 2020	
Consentement	Adoption définitive
Deuxième directive sur les services de paiement (DSP 2)	Adoption définitive
Traitement des données personnelles au moyen d'appareils vidéo	Adoption définitive
Traitement de données de santé à des fins de recherche scientifique dans le contexte de la COVID-19	Adoption définitive
Utilisation de données de localisation et d'outils de recherche de contact dans le contexte de la COVID-19	Adoption définitive
Transferts de données personnelles entre les autorités et organes publics de l'Espace économique européen (EEE) et de pays tiers	Adoption définitive
Protection des données dès la conception et par défaut	Adoption définitive
Véhicules connectés	Consultation publique
Notions de responsable du traitement et de sous-traitant dans le RGPD	Consultation publique
Ciblage des utilisateurs des réseaux sociaux	Consultation publique
Notion d'objection pertinente et motivée	Consultation publique
Restrictions des droits des personnes concernées (article 23 du RGPD)	Consultation publique

L'Assemblée a également pris la décision de monter un groupe de travail consacré à l'utilisation des outils numériques dans le cadre de la lutte contre la COVID-19. Elle a notamment organisé, avec l'OCDE, un évènement commun sur les enjeux en matière de gouvernance des données et de protection de la vie privée dans le cadre de la lutte contre la pandémie. Elle a, par ailleurs, adopté une résolution sur le sujet.

La CNIL s'est également impliquée dans les travaux au sein du groupe de travail sur la gouvernance des données et la vie privée de l'OCDE, assurant la représentation des autorités françaises au sein de cet organe. Les discussions en 2020 se sont concentrées sur la finalisation du processus de revue des lignes directrices de l'OCDE sur la vie privée, mais aussi sur des problématiques connexes émergentes comme l'accès des gouvernements aux données détenues par le secteur privé.

Par ailleurs, au sein du Conseil de l'Europe, la CNIL a continué à participer, aux côtés des autorités françaises, aux travaux du Comité de la Convention 108 sur la protection des données personnelles. Ils ont notamment donné lieu en 2020 à l'adoption de lignes directrices sur la protection des données des enfants dans un cadre éducatif.

FOCUS

Francophonie

La CNIL héberge le Secrétariat général de l'Association francophone des autorités de protection des données personnelles (AFAPDP) depuis sa création en 2007. L'AFAPDP rassemble les autorités francophones de protection des données personnelles et les gouvernements intéressés par une telle loi qui partagent, au-delà de la langue, une tradition juridique et des valeurs communes.

En 2020, les activités de l'association ont été fortement touchées par la situation sanitaire. Les autorités membres ont néanmoins adopté une déclaration à propos de la protection des données personnelles dans le contexte de la crise sanitaire, en réaffirmant le caractère strictement nécessaire, proportionné et limité en droit, dans l'espace et le temps de toute mesure attentatoire aux libertés fondamentales et aux droits humains, qui serait envisagée.

Dans le cadre de la 42e Assemblée mondiale pour la protection de la vie privée (GPA), qui s'est déroulée en ligne en octobre 2020, l'AFAPDP a contribué à faire respecter la diversité linguistique dans cette instance, en assurant l'intégralité des traductions en français des documents de la réunion.

Enfin, le secrétariat a répondu aux sollicitations spécifiques de ses membres afin de favoriser le partage d'informations et de bonnes pratiques dans un contexte sanitaire qui a mis les autorités de protection des données personnelles de l'espace francophone face à de nouvelles problématiques.

Pour finir, si la CNIL a pu accueillir au tout début de l'année quelques délégations étrangères, du fait du contexte sanitaire ces rencontres n'ont plus été possibles à partir du printemps. Les contacts bilatéraux ont toutefois pu être maintenus, en attente d'une situation plus favorable qui permettra la reprise de ces échanges si importants.

1 392

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

512

procédures de guichet unique.

168

décisions finales adoptées (la CNIL a été autorité chef de file pour 11 décisions et autorité concernée pour 47 décisions).

FOCUS

Une coopération internationale soutenue sur l'éducation au numérique et les droits des enfants

Depuis 2013, la CNIL pilote un groupe de travail sur l'éducation au numérique au sein de l'Assemblée mondiale pour la protection de la vie privée. Cette implication a permis plusieurs actions :

- En 2019, le Comité des droits de l'enfant de l'ONU a rédigé un projet d'Observation générale sur les droits de l'enfant en relation avec l'environnement numérique. En concertation avec les 74 autorités membres du groupe de travail, la CNIL a favorisé l'adoption d'une contribution pour soutenir les orientations du projet publié en mars 2020 et émettre des propositions, notamment sur l'exercice des droits des enfants sur internet et l'exploitation commerciale de ces données[1].
- La CNIL a publié, en septembre 2020[2], une étude internationale concernant les cadres juridiques applicables aux enfants et l'exercice des droits des mineurs. Celle-ci a été conduite auprès des membres du groupe de travail et a permis une mise en perspective des diverses initiatives nationales et internationales sur le sujet, en cours ou en projet.

La CNIL a également proposé des contributions et éclairages spécifiques :

- En juillet 2020, elle a proposé une réponse à l'appel à contributions du Rapporteur spécial sur le droit à la vie privée de l'ONU qui s'attachait à examiner les droits des enfants à la vie privée et à la protection de leurs données. Le rapport final sera publié en mars 2021 sur le site du Conseil des droits de l'Homme des Nations Unies.
- En décembre 2020, la CNIL a répondu à la consultation publique de la Commission européenne pour sa nouvelle Stratégie 2021-2024 relative aux droits de l'enfant, qui proposera un cadre politique global de l'UE en faveur des droits de l'enfant couvrant notamment, la protection de leurs droits en ligne.
- Enfin, la CNIL a contribué à l'organisation d'une vidéoconférence internationale conduite par le Conseil de l'Europe, « Les Journées de l'éducation à la citoyenneté numérique », les 3 et 4 novembre 2020. Des experts internationaux ont débattu sur la manière dont la crise de la COVID-19 a pu être transformée en une opportunité pour permettre aux éducateurs d'améliorer leurs compétences numériques, dans le cadre de politiques éducatives innovantes.

(1) : « General Comment on children's rights in relation to the digital environment » (en anglais), novembre 2020, ohchr.org

(2) : « Cadre légal et pratiques des autorités de protection des données relatifs à l'exercice des droits des mineurs », décembre 2020, globalprivacyassembly.org

PROTÉGER
les citoyens

En cas de plainte, la CNIL informe généralement 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. En 2020, la CNIL a reçu de nombreuses plaintes en lien avec la crise sanitaire, notamment concernant des pratiques constatées en entreprise.

Paul
Juriste au service des plaintes

J'ai rejoint le service des plaintes en 2019, au sein du pôle en charge des questions sur les ressources humaines, le secteur social, la santé et l'éducation. Cette pluralité de secteurs conduit à recevoir des réclamations hétéroclites, mêlant la protection des données personnelles à d'autres législations, telles que le droit du travail, le droit social, le droit de la santé, etc.

La préoccupation croissante pour la protection de la vie privée nous amène à être fortement sollicités, imposant une organisation méticuleuse dans la gestion des dossiers. Afin d'assurer un traitement efficace des réclamations, je suis amené à collaborer étroitement avec d'autres services de la CNIL, et notamment ceux chargés des contrôles et des sanctions. Par ailleurs, la complexification des sujets que nous traitons m'amène à travailler de manière transversale avec mes collègues ingénieurs ou juristes spécialisés sur certains sujets.

La singularité de l'année 2020 a eu des conséquences sur les thématiques traitées. La CNIL a ainsi reçu des réclamations en lien avec la crise sanitaire : développement du télétravail au sein des entreprises et des administrations, opérations de dépistages menées directement par les employeurs, émergence de nouvelles applications liées à la COVID-19 et enseignement à distance. Mes missions impliquent ainsi une vigilance sur l'actualité et participent activement à la délivrance d'un service au bénéfice de la protection des droits des personnes. Cet engagement pour le public, que je partage avec chaque agent de mon service, me permet d'être acteur de la préservation d'un principe fondateur de notre institution : « L'informatique doit être au service de chaque citoyen ».

LES PLAINTES

Un nombre élevé et constant de plaintes

13 585

PLAINTES

- 3,9 %

PAR RAPPORT À 2019

95 %

DES PLAINTES SONT EFFECTUÉES SUR LE SERVICE EN LIGNE

4 528 plaintes ont fait l'objet d'une réponse rapide (ou « de premier niveau ») sur :

- les droits applicables 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.

La CNIL a également reçu et traité rapidement 150 plaintes concernant la vidéosurveillance mise en œuvre par des particuliers. En effet, des personnes ont constaté l'installation, par un voisin, d'une caméra sur un mur, toit ou balcon de sa résidence, qui aurait pour objectif de filmer au-delà du domicile de l'installateur. La CNIL rappelle dans ces cas, par courrier, la règlementation applicable à la vidéosurveillance au domicile[30].

9 057 plaintes (+ 6,3 %) 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, la CNIL intervient auprès du responsable du fichier mis en cause selon le mode d'action le plus approprié.

INFOSPLUS

Pour exercer ses droits, obtenir accès à ses données ou la suppression de contenu en ligne, 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.

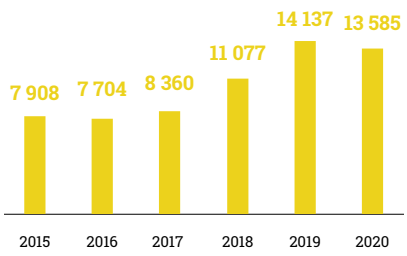
La CNIL intervient, toujours par écrit, pour :

- lui rappeler ses obligations et l'inviter à prendre les mesures nécessaires ;
- l'interroger sur les conditions de mise en œuvre de son traitement de données personnelles (par exemple, les conditions de collecte des données, leur durée de conservation, etc.) et/ou demander des précisions sur la réponse apportée à la demande du plaignant ;
- obtenir tout justificatif utile.

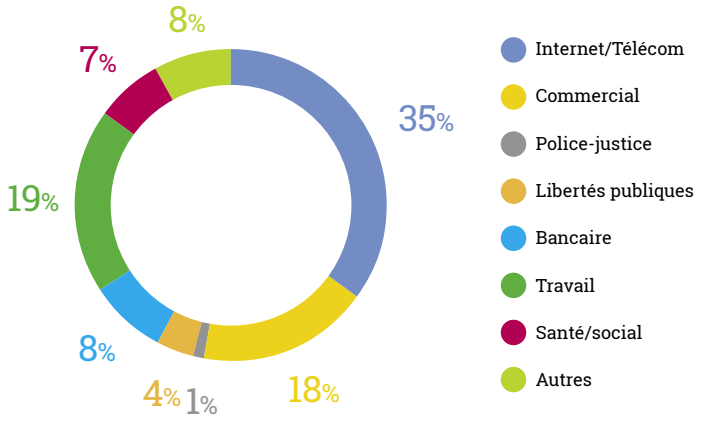
Une réponse adaptée, individuelle ou collective

La très grande majorité des plaintes reçues par la CNIL concerne un individu qui rencontre une difficulté lors de l'exercice de ses droits ou du traitement des données le concernant. Au-delà de cette plainte individuelle, l'intervention de la CNIL est également susceptible d'avoir des répercussions positives pour l'ensemble des personnes concernées par le dispositif visé par cette plainte.
Le nombre élevé et constant de plaintes reçues a conduit la CNIL à s'adapter afin de mieux identifier les plaintes similaires reçues et renforcer les actions auprès des organismes concernés.

Nombre de plaintes par année



Répartition des plaintes par secteur en 2020



30 « La vidéosurveillance, vidéoprotection – chez soi », mis à jour le 13 décembre 2019, cnil.fr

Ainsi, lorsqu'elle identifie plusieurs plaintes contre un même acteur, un même secteur et concernant une même pratique dénoncée, **la CNIL peut les regrouper en une même instruction** et approfondir ses vérifications au-delà de la situation individuelle des plaignants.

Ces vérifications des mesures techniques et organisationnelles mises en place pour se conformer aux règles en matière de protection des données peuvent notamment conduire à initier une procédure de contrôle (40 % des contrôles ont ainsi pour origine des plaintes ou des signalements) voire à l'adoption de mesures correctrices (rappel à l'ordre, mise en demeure, sanction financière, injonction, etc.). Les plaintes constituent ainsi un levier important dans la mise en conformité des organismes publics comme privés.

Au titre de l'année 2020, on peut ainsi citer les sanctions publiques à l'encontre des sociétés Carrefour France et Carrefour Banque prononcées après de nombreuses plaintes ayant donné lieu à une procédure de contrôle.

> **Les problématiques soulevées illustrent la place désormais dévolue et les enjeux soulevés par la protection des données dans le quotidien des Français.**

Les plaintes européennes

Si l'objet de la plainte est transfrontalier, soit parce que le responsable du fichier est établi dans plusieurs États membres de l'Union, soit parce qu'il est établi dans un seul État membre mais que son fichier vise des personnes dans plusieurs pays européens, elle doit être traitée en coopération avec les autorités de protection de données concernées.

Les sujets de ces plaintes européennes sont variés, allant de difficultés individuelles à des préoccupations plus larges et complexes, relayées notamment par des associations de défense des libertés numériques à l'encontre des grands acteurs mondiaux de l'internet.

En 2020, plus de 1 000 dossiers de coopération concernaient des plaintes, la CNIL étant « chef de file » dans 75 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 françaises ayant fait l'objet de plaintes ont été réglées. La présidente de la CNIL a également adopté 7 rappels aux obligations à l'encontre d'organismes français visés par des plaignants européens.

Une action sur les irritants du quotidien

Bien que les plaintes reçues soient de plus en plus complexes et techniques, les problématiques soulevées illustrent la place désormais dévolue et les enjeux soulevés par la protection des données dans le quotidien des Français.

Conserver la maîtrise de ses données

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

La CNIL a reçu près de 150 plaintes relatives à des demandes d'effacement de contenus concernant des articles de presse publiés en ligne (retrait de l'article, anonymisation, désindexation).

FOCUS

Mise en demeure de fournir la transcription écrite d'une conversation téléphonique

La CNIL a été saisie de plusieurs plaintes de personnes ayant sollicité de leur employeur la copie d'une conversation téléphonique qu'ils avaient eue avec l'un de leurs collègues et qui avait été enregistrée.

L'employeur a refusé de fournir cette copie au motif que cela porterait atteinte aux droits des tiers.

Face au refus réitéré de l'employeur, la présidente de la CNIL lui a adressé une mise en demeure rappelant que si les droits des tiers doivent être protégés, en préservant notamment leur anonymat, cette protection ne s'applique que lorsque l'identité du tiers est inconnue du demandeur. Dans ce cas, cette identité peut être supprimée, plutôt que la suppression des propos qu'il aurait tenus.

Il a ainsi rappelé à cet employeur qu'il était tenu de fournir les transcriptions complètes dans les cas d'espèce et à l'avenir. L'employeur s'est, depuis, conformé à cette décision.

En 2020, la CNIL a également reçu 382 nouvelles plaintes relatives au déréférencement (- 9,5 %) et a obtenu la résolution des situations dans 93,2 % des cas transmis aux moteurs de recherche.

S'il est difficile de connaître précisément les raisons de cette baisse des plaintes en matière de déréférencement, il est probable que l'action de la CNIL sur ce sujet depuis des années et les arrêts rendus en 2019 par la Cour de justice de l'Union européenne et le Conseil d'État[31] ont conduit les sociétés exploitant des moteurs de recherche à faire droit plus fréquemment aux demandes des internautes.

Les systèmes utilisés en entreprise

La surveillance des employés sur leur lieu ou pendant leur temps de travail, par des outils tels que la vidéosurveillance, la géolocalisation, les écoutes téléphoniques, etc. génère toujours de nombreuses plaintes (10 % des plaintes reçues en 2020) qui visent des acteurs du secteur privé comme du secteur public.

La vidéosurveillance (750 nouvelles plaintes en 2020) concentre toujours le plus de plaintes dans le secteur Travail, 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.

Défendre son droit à la tranquillité et la prise en compte de ses droits

Le nombre de plaintes relatives à la réception de prospection est particulièrement important (11 % des plaintes). Qu'il s'agisse de prospection commerciale, associative, politique, reçue par voies postale, téléphonique ou électronique, les personnes qui saisissent la CNIL d'une plainte pour ces motifs sont nombreuses. Les publicités par courrier électronique et par SMS génèrent le plus de plaintes.

Histoires vécues...

Monsieur X. était filmé en permanence sur son poste de travail dans un PC Sécurité.

La CNIL est intervenue auprès de son employeur afin de lui rappeler que les caméras installées doivent être orientées sur les accès et les installations techniques sensibles mais ne doivent pas filmer les postes de travail des agents qui s'y trouvent.

Après intervention de la CNIL, l'entreprise a modifié l'orientation de la caméra en cause afin de ne plus visualiser en permanence le salarié sur son poste de travail.

Madame X. a candidaté à un poste dans une société. Lors du processus, réalisé en visioconférence, des photographies ont été prises à son insu et postées sur des réseaux sociaux, afin de promouvoir la société.

La CNIL est intervenue auprès de la société pour lui rappeler que la collecte et la publication sur internet de données personnelles sont soumises au respect du RGPD.

Après intervention de la CNIL, la société a procédé à l'effacement des photographies de Madame X., aussi bien sur les réseaux sociaux que dans ses fichiers internes. Elle s'est aussi engagée à modifier ses pratiques en termes de recrutement et à respecter le droit à la vie privée des candidats.

Madame G., magistrate, a fait l'objet d'un article de presse indiquant qu'elle aurait été écartée de la gestion d'un dossier médiatique du fait de ses origines, identiques à celles des victimes parties au procès. Cet article a été repris par de nombreux sites web. Madame G. a demandé le déréférencement de ces résultats au moteur de recherches, arguant que ces articles nuisent à son image professionnelle. L'exploitant du moteur de recherche a d'abord rejeté sa demande en considérant que compte tenu de son métier, l'information aurait toujours un intérêt particulier pour le public.

La CNIL est intervenue en mettant notamment en avant l'ancienneté de cette affaire désormais close, l'absence de rapport entre le fait d'avoir été écartée du dossier et les aptitudes professionnelles de Madame G. et le dommage professionnel qui résulte de ce référencement pour elle.

Après intervention de la CNIL, l'exploitant du moteur de recherche a déréférencé les résultats concernés.

Monsieur Z. a été cité dans un article de presse locale couvrant un sujet sur les activités proposées au sein de sa commune. Il s'est adressé au rédacteur en chef pour obtenir la suppression des données le concernant en prenant soin de justifier sa demande (il s'agissait d'activités strictement personnelles qui faisaient depuis l'objet de moqueries de la part de son entourage). Le journal local a refusé d'effacer ces données en invoquant « le droit à l'information ».

La CNIL est intervenue auprès du journal afin de lui rappeler qu'un tel refus ne peut se justifier par des considérations générales et qu'il devait démontrer, au cas par cas, les motifs qui justifieraient le maintien de la publication des nom et prénom de la personne concernée.

Après intervention de la CNIL, les nom et prénom de Monsieur. Z ont été effacés de l'article publié en ligne.

31 « Droit au déréférencement : le Conseil d'État tire les conséquences des arrêts de la Cour de justice de l'Union européenne », 27 mars 2020, cnil.fr

Histoires vécues...

Monsieur C. reçoit constamment de la publicité par courrier électronique de la part d'un même organisme. Lorsqu'il clique sur le lien de désabonnement présent en bas du message, il est orienté sur une page de création d'un compte client et ne parvient pas à se désabonner.

La CNIL est intervenue auprès de l'organisme pour résoudre le problème de Monsieur. C. et l'interroger sur les mesures prises pour veiller à ce que les personnes puissent facilement s'opposer à recevoir de la publicité de sa part.

Après cette intervention, Monsieur. C. a cessé de recevoir ces publicités et l'organisme a corrigé le lien de désabonnement afin de permettre de s'opposer simplement à la réception de courriel de prospection commerciale.

Monsieur X. a été inscrit par sa banque au fichier central des chèques et cartes bancaires (FCC – CB) après avoir effectué un retrait de carte bancaire sans provision. Il a constaté le maintien de son inscription malgré la régularisation de sa situation.

La CNIL est intervenue auprès de cette banque, qui a confirmé que le maintien de l'inscription était irrégulier : la banque n'avait pas affecté la demande de levée d'inscription au bon numéro de compte et la demande n'avait donc pas été traitée.

Après l'intervention de la CNIL, Monsieur. X. a immédiatement été déficher.

Monsieur X. a décidé de poursuivre son ancien employeur en vue de contester son licenciement. Dans ce contexte conflictuel, il demande accès à l'ensemble des données personnelles contenues dans son dossier professionnel. La société refuse, lui précisant que le contentieux les opposant l'empêche de transmettre ces éléments.

La CNIL est intervenue auprès de cette société pour lui rappeler que le droit d'accès peut s'exercer y compris lorsqu'une procédure contentieuse est en cours, et qu'elle est donc tenue d'examiner la demande reçue et d'y répondre dans les conditions prévues par le RGPD.

Les personnes déplorent que leur consentement n'ait pas été recueilli et/ou de ne pas parvenir à faire cesser la réception de ces publicités malgré leur opposition.

En 2020, la CNIL a poursuivi son partenariat avec Signal Spam pour identifier les expéditeurs de spam et agir auprès d'eux. Cela a notamment abouti à la sanction publique infligée à une société régulièrement en tête du classement des sociétés émettant le plus de messages signalés comme « spam » par les internautes sur le territoire français.

Dans tous les secteurs, le non-respect des droits des personnes est générateur d'un grand nombre de plaintes.

Comme les années précédentes, la CNIL a encore reçu beaucoup de plaintes (près de 400) 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), le fichier central des chèques (FCC).

La CNIL est également saisie par des personnes pour des difficultés d'accès à leur dossier personnel (dossier médical, dossier CAF, Pôle emploi, etc.).

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

Savoir ses données en sécurité

Les plaintes relatives à des défauts de sécurisation des données sont désormais régulières.

La CNIL constate ainsi que les erreurs de paramétrage entrainant une divulgation de données sur internet, le partage de données par courrier électronique ou encore la communication de mots de passe en clair sont nombreuses.

Qu'elles aient une origine accidentelle ou non, des violations de données sont régulièrement relayées par les plaignants, que ceux-ci soient simplement préoccupés des conséquences de ces incidents sur leurs propres données ou qu'ils s'en fassent le relais en tant qu'experts dans le domaine.

La CNIL est ainsi amenée à mener des vérifications et investigations pour vérifier les circonstances ayant conduit à ces défauts de sécurité des données, ainsi qu'à rappeler à leurs obligations de sécurité les organismes concernés.

C'est notamment dans le secteur médical que le nombre de plaintes a considérablement augmenté sur ces questions. Le souci de savoir qui, au sein d'un établissement de santé, peut accéder ou a eu accès à quels dossiers et quelles données, motive le plus souvent une telle démarche.

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

Une stabilité du nombre de demandes

En 2020, 3 996 demandes ont été valablement adressées à la CNIL afin qu'elle exerce les droits des usagers qui l'ont sollicité. Le nombre de ces demandes, dites « demandes d'accès indirect », est stable par rapport à 2019.

Ces saisines sont adressées par voie postale dans plus de 75 % des cas. L'année 2020 se distingue cependant par une forte croissance des demandes adressées par voie électronique (environ 530 demandes reçues par ce canal en 2019 contre environ 1050 en 2020, soit une augmentation de presque 100 %).

Afin d'instruire ces demandes, la CNIL a effectué environ 3 286 vérifications auprès des responsables de traitement, en diminution par rapport à 2019 (- 8 %). Cette baisse est notamment due à l'impossibilité d'effectuer des vérifications pendant la période de confinement.

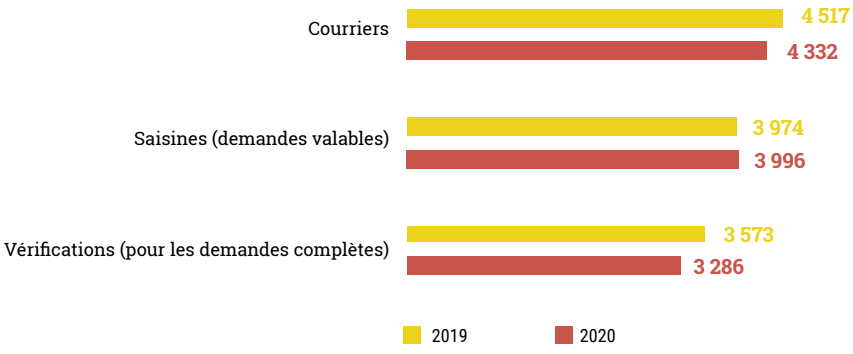
De nombreuses demandes incomplètes qui empêchent la CNIL d'agir

Afin de permettre à la CNIL d'instruire une demande, il est nécessaire de lui communiquer différents éléments qui font parfois défaut (voir encadré). Ainsi, la demande doit systématiquement mentionner le nom du fichier concerné, une copie de la pièce d'identité du demandeur ainsi que l'adresse postale du demandeur. D'autres éléments peuvent par ailleurs être requis dans certaines circonstances spécifiques.

De nombreuses demandes qui parviennent à la CNIL sont incomplètes (environ 15 %) retardant ainsi leur traitement. L'adresse postale, la copie d'un titre d'identité ou encore un mandat lorsque les démarches sont effectuées par un tiers figurent parmi les éléments les plus souvent manquants.

Dans ce cas, l'usager est informé de la nécessité d'adresser le document ou l'information manquante. Il dispose en principe d'un délai de deux mois pour compléter sa demande.

Demandes de droit d'accès indirect



FOCUS

Droit d'accès indirect : quels éléments adresser à la CNIL ?

Pour faire une demande de droit d'accès indirect, il est nécessaire de systématiquement indiquer :

- le nom du ou des fichiers concernés (afin de vous aider dans cet exercice, n'hésitez pas à vous rendre sur le site de la CNIL) ;
- la copie recto-verso d'un document d'identité avec mention des date et lieu de naissance ;
- une adresse postale afin que la CNIL vous adresse le résultat de ses vérifications par courrier.

Dans certaines circonstances, il peut être nécessaire de joindre d'autres éléments à votre demande :

- en cas d'intervention pour le compte d'une autre personne, tout élément justifiant votre qualité de représentant de la personne intéressée (copie du mandat, de la décision de placement sous tutelle ou curatelle, du livret de famille, etc.) ;
- tout élément justifiant l'envoi d'une demande préalable à cette autre administration (copie de la réponse du gestionnaire du fichier, du courrier envoyé ou de l'accusé réception de ce courrier), lorsque c'est nécessaire (ex. : TAJ).

FOCUS

Le FICOBA

Le FICOBA rassemble des informations relatives à tous les comptes bancaires ouverts en France. On peut ainsi y retrouver :

- les références de chaque compte, c'est-à-dire ses numéros (RIB, BIC ou IBAN) ou encore sa nature (compte courant, compte épargne logement, livret A, livret d'épargne populaire, etc.)
- le nom et l'adresse de la banque auprès de laquelle le compte a été ouvert ;
- les dates d'ouverture et de clôture de chaque compte.

Ce fichier ne contient en revanche aucune information concernant les opérations effectuées (retraits, paiements, virements, etc.) ou concernant les sommes disponibles sur les comptes. Pour accéder à ces informations, il est nécessaire de s'adresser à la banque auprès de laquelle le compte est ouvert.

Enfin, les informations relatives à un compte sont supprimées du FICOBA si le compte est fermé depuis plus de 10 ans.

Le FICOBA, un fichier toujours plus sollicité

En 2020, le nombre de demandes d'exercice des droits instruites par la CNIL concernant le FICOBA a progressé de 12 %, après une augmentation encore plus significative entre 2018 et 2019 (+ 40 %).

La CNIL a constaté une forte progression des demandes motivées par la crainte d'une usurpation d'identité. Ce motif apparaît dans plus de 35 % des demandes adressées à la CNIL en 2020 (contre 20 % en 2019). **Dans cette circonstance, les usagers sont également invités à s'adresser à la Banque de France** afin de vérifier s'ils sont enregistrés dans le fichier central des chèques (FCC) ou dans le fichier des incidents de remboursement des crédits aux particuliers (FICP).

Pour certains fichiers, l'usager doit préalablement saisir le gestionnaire (par exemple la direction générale de la Police nationale - DGPN) concerné par sa demande avant de faire une demande à la CNIL : c'est notamment le cas pour le traitement d'antécédents judiciaires (TAJ) ou encore pour le système d'information Schengen (SIS II).

La CNIL reçoit encore de nombreuses demandes formulées par des usagers qui n'ont pas préalablement saisi le gestionnaire. Dans ce cas, la CNIL adresse la demande au service compétent. Elle informe par ailleurs l'usager de ce transfert et de son droit de la saisir si le gestionnaire du fichier l'informe qu'il refuse de répondre à sa demande ou ne lui répond pas dans un délai de deux mois.

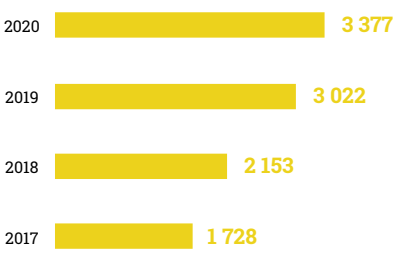
Histoire vécue...

Madame H. a mis en vente sa voiture sur un site de vente entre particuliers. Un potentiel acquéreur lui a alors demandé la communication de plusieurs documents afin, selon ses indications, de s'assurer que Madame H. était bel et bien la propriétaire du véhicule : photocopies d'une pièce d'identité, de la carte grise, d'un justificatif de domicile, etc.

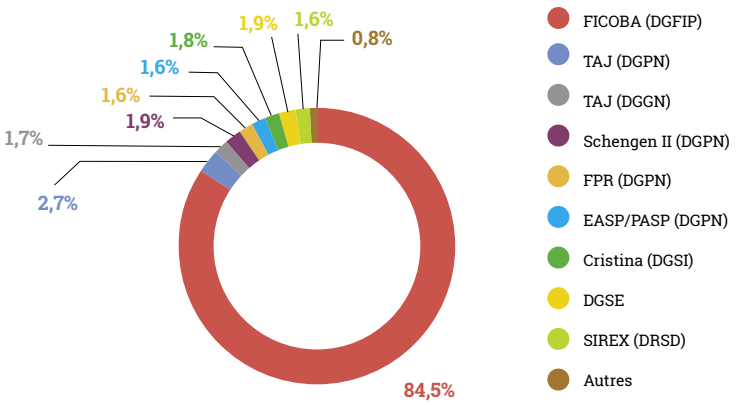
Quelques mois après avoir vendu sa voiture à un autre candidat, Madame H. a reçu plusieurs visites imprévues : des personnes se sont présentées chez elle en revendiquant la propriété du véhicule, pourtant déjà vendu. Ces acheteurs ont présenté des preuves de virements effectués sur un compte ouvert au nom de Madame H. mais inconnu de celle-ci.

Cette dernière s'adresse alors à la CNIL afin d'obtenir communication des comptes ouverts à son nom et, à la lecture de la liste de ces derniers, identifie des comptes ouverts à son insu. Sur la base de ces éléments, elle s'est rapprochée des services de police afin de compléter sa plainte et a engagé les démarches auprès des banques pour régulariser la situation.

Saisines sur le FICOBA



Les demandes par fichier



Histoire vécue...

Monsieur A. exerçait depuis plusieurs années une activité d'agent de sécurité. Sa carte professionnelle arrivant à expiration, son employeur a engagé les démarches nécessaires à son renouvellement.

Pour de telles activités, une enquête administrative est effectuée afin de vérifier que le comportement des candidats n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées. Dans le cadre de cette enquête, il est notamment recherché si le candidat figure ou non dans plusieurs fichiers, notamment dans le fichier des personnes recherchées (FPR). À l'issue de cette enquête, la carte professionnelle de Monsieur A. n'a pas été renouvelée.

N'ayant pas connaissance d'une inscription dans un quelconque fichier, Monsieur A. s'est adressé au gestionnaire du FPR pour savoir s'il figurait ou non dans ce fichier et obtenir, si besoin, l'effacement des données le concernant. Le gestionnaire du FPR ayant répondu défavorablement à sa demande, Monsieur A. s'est adressé à la CNIL pour exercer ses droits par son intermédiaire.

La CNIL a d'abord effectué une première vérification auprès du gestionnaire du FPR. Il est alors apparu que Monsieur A. figurait effectivement dans le FPR sur la base d'un signalement émis par un service de renseignement.

Afin de s'assurer du bien-fondé de cette inscription, la CNIL s'est ensuite rendue auprès de ce service de renseignement et a constaté que les éléments à l'origine du signalement dans le FPR étaient anciens et ne permettaient plus d'identifier un risque concernant Monsieur A.

Suivant l'avis de la CNIL, le service de renseignement a renoncé au signalement de Monsieur A. dans le FPR, ce dont la CNIL s'est assurée lors d'une dernière vérification auprès du gestionnaire de ce fichier.

Il n'a cependant pas été possible d'informer Monsieur A. du résultat de l'action de la CNIL : le gestionnaire du FPR s'est en effet opposé à la communication de ces éléments comme les textes le lui permettent.

La situation de Monsieur A. a cependant évolué de façon positive : il a pu à nouveau envisager l'obtention d'un agrément afin d'exercer son activité d'agent de sécurité.

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, plusieurs mesures répressives peuvent être prises, de la mise en demeure à la sanction pécuniaire pouvant atteindre 4 % du chiffre d'affaires mondial.

Hugo
Juriste au service des contrôles - affaires économiques

Belaïd
Auditeur des systèmes d'information au service des contrôles – RH, santé et affaires publiques.

Contrôler, c'est vérifier concrètement comment et pourquoi les données personnelles des utilisateurs sont traitées par les organismes. En pratique, nous interrogeons les responsables de traitement afin de comprendre les conditions opérationnelles de mise en œuvre des traitements. Nous vérifions notamment les mesures de sécurité mises en place afin de protéger les données.

Lors d'un contrôle sur place, nous prenons copie de l'ensemble des pièces jugées utiles à la procédure (contrats, extractions de base de données), et consignons dans un procès-verbal les constats effectués et les informations délivrées par les personnes interrogées.

Le plus souvent, nous menons nos enquêtes en binôme, constitué d'un juriste et d'un informaticien (auditeur des systèmes d'informations). Ces enquêtes peuvent être diligentées sur place, en ligne, sur pièces, ou encore sur audition. Si les contrôles sur place sont généralement privilégiés, la crise sanitaire et les confinements successifs ont imposé un recours plus important aux contrôles en ligne et sur pièces pour l'année 2020.

Nos contrôles sont variés, ils concernent tout type d'organisme (public, privé, associatif) sur l'ensemble du territoire français. Nous sommes ainsi amenés à contrôler aussi bien des applications mobiles développées par de jeunes start-ups que de grandes multinationales ou encore des fichiers mis en œuvre par des ministères régaliens.

Cette année, en plus des thématiques annuelles et des contrôles menés sur la base des plaintes reçues, nous avons également été fortement mobilisés par les contrôles des traitements mis en œuvre dans le cadre de la lutte contre la COVID-19. À ce titre, 25 contrôles ont été réalisés tout au long de l'année 2020.

LES CONTRÔLES DE LA CNIL

247

CONTRÔLES

DONT :

82

CONTRÔLES EN LIGNE

74

CONTRÔLES SUR PIÈCES

72

CONTRÔLES SUR PLACE

19

CONTRÔLES SUR AUDITION

La CNIL conduit chaque année un grand nombre d'investigations qui prennent des formes diverses (contrôles sur place ou en ligne, demande de communication de pièces ou encore auditions) et qui peuvent se cumuler : la CNIL peut, par exemple, contrôler un site web en ligne puis sur place.

Elle a ainsi conduit, de manière générale, **6 500 actes d'investigation en 2020**. Ces vérifications peuvent s'effectuer dans le cadre de procédures formelles de contrôle, notamment en réponse à des plaintes ou lors d'une procédure de sanction et comprennent également les demandes de droit d'accès indirect.

Parmi ces actes d'investigation, la CNIL a ouvert **247 procédures formelles de contrôle**, principalement en ligne, et a traité **56 signalements** de violations de données.

Cette année, la crise sanitaire a conduit la CNIL à adapter son activité de contrôle. Lors du premier confinement, une partie des missions d'investigation a, en effet, été suspendue et les délais accordés aux organismes pour répondre ont été rallongés.

Par la suite, les contrôles sur place, qui représentent habituellement la modalité principale de contrôle (56 % des contrôles en 2019 contre 29 % en 2020), ont le plus souvent été remplacés par les autres modes d'investigations : les contrôles en ligne (34 %), sur pièces (29 %) et sur audition (8 %).

La stratégie répressive centrée sur les préoccupations et difficultés rencontrées par les citoyens a été poursuivie : les plaintes sont donc toujours la principale source de contrôle (40 % des contrôles). Les contrôles effectués sur initiative (32 %) sont le plus souvent en lien avec l'actualité. De plus en plus souvent, la CNIL doit réaliser des missions en urgence pour mettre fin à une violation manifeste ou pour sauvegarder la preuve d'agissements contraires au RGPD (par exemple en 2020, l'utilisation de drones par les forces de l'ordre ou une atteinte à la sécurité des données dans un établissement de santé). La CNIL procède également à des contrôles auprès d'organismes ayant fait l'objet de mesures correctrices afin de s'assurer de la pérennité ou de l'effectivité des mesures mises en œuvre.

Une partie des missions menées en 2020 était directement liée à la crise sanitaire. En effet, dès le mois de juin, la CNIL a été fortement mobilisée par les contrôles des traitements mis en œuvre dans le cadre de la lutte contre la COVID-19 : l'application StopCovid (devenue TousAntiCovid) et les traitements SI-DEP et Contact Covid.

Par ailleurs, comme les années précédentes, **la CNIL est restée particulièrement vigilante sur le sujet de la sécurité des données personnelles**. Elle a ainsi mené 56 vérifications à la suite de signalements concernant des données accessibles sur internet sans mesure de protection. Ces vérifications lui ont permis de faire cesser les violations de données personnelles dans un délai très restreint.

Enfin, malgré le contexte sanitaire, le travail de coopération avec les autres autorités de protection de données s'est poursuivi en 2020. La CNIL a ainsi participé à une *task force* rassemblant plusieurs États membres de l'Union européenne qui ont lancé simultanément des investigations sur les traitements mis en œuvre dans le cadre de l'application TikTok. Elle a également échangé à de nombreuses reprises avec ses homologues dans le cadre de demandes d'assistance mutuelle.

INFOSPLUS

L'origine des procédures formelles de contrôle

40 %
s'inscrivent dans le cadre de l'instruction de plaintes ou de signalements.

32 %
sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;

15 %
résultent des thématiques prioritaires annuelles décidées par la CNIL ;

10 %
sont liés aux contrôles mis en œuvre dans le cadre de la lutte contre la COVID-19 ;

3 %
sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction.

Bilans des thématiques annuelles prioritaires pour 2020

En dehors des contrôles effectués sur le respect des règles concernant les cookies et autres traceurs (voir page 38), la CNIL a mené des investigations sur deux autres thématiques majeures, annoncées en mars 2020 : les données de santé et certains services faisant usage de données de géolocalisation.

LA SÉCURITÉ DES DONNÉES DE SANTÉ

La CNIL a souhaité, par cette thématique prioritaire, s'intéresser aux mesures de sécurité mises en œuvre par les structures de soins, par les professionnels de santé (ou pour leur compte) et par les sociétés prestataires de services du domaine de la santé.

Des contrôles ont été conduits auprès de sept organismes, établissements de santé et fournisseurs de services à destination des professionnels de santé et des patients, plus particulièrement sur la question de l'accès au dossier patient informatisé au sein de CHU (centres hospitaliers universitaires), sur les logiciels de prise de rendez-vous en ligne et sur les *data brokers* (courtiers en données) de santé. À ce stade, il apparaît que les données de santé des patients sont trop souvent accessibles à un grand nombre de personnes, avec un manque de vigilance de la part des responsables de traitement sur ces accès.

La crise sanitaire a également conduit à une réorientation des contrôles vers les traitements mis en œuvre en réponse à la pandémie, afin d'en vérifier la conformité (voir page 33).

MOBILITÉS ET SERVICES DE PROXIMITÉ, LES NOUVEAUX USAGES DES DONNÉES DE GÉOLOCALISATION

De nombreuses solutions se développent avec pour objectif affiché de faciliter la vie quotidienne : recommandation des modes de transport adaptés selon un trajet défini, optimisation des parcours de déplacement, etc. Ces solutions font le plus souvent appel à des données de géolocalisation, qui soulèvent potentiellement des risques d'atteinte à la vie privée.

En 2020, des contrôles ont été menés auprès de dix organismes proposant des services de proximité (services de conciergerie de proximité, mise en relation entre particuliers pour de l'aide à domicile et travaux, etc.) ainsi que des services innovants en matière de mobilité (services de location de véhicules partagés, de vélos en location longue durée, de trottinettes en libre-service, etc.). **Ces contrôles ont eu pour objectif de vérifier la pertinence des données collectées**, en particulier s'agissant des données de géolocalisation, de **l'information des personnes** ainsi que de la **sécurité des données traitées**.

DÉFINITION

Le principe de minimisation, issu du RGPD, prévoit que les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Il ressort des missions effectuées que les organismes ont pris conscience du cadre légal qui s'impose à eux en matière de protection des données de leurs utilisateurs et ont désigné, pour la majorité d'entre eux, un délégué à la protection des données.

Néanmoins, concernant les données de géolocalisation, il a été constaté que **certains organismes ne respectent pas le principe de minimisation des données** et géolocalisent les personnes pendant toute la durée d'utilisation du service sans que cela ne soit nécessaire au bon fonctionnement de celui-ci (en particulier, lors de la location d'un véhicule).

L'information fournie aux personnes n'est pas toujours satisfaisante. Elle est souvent incomplète (absence d'information concernant les bases légales et les durées de conservation) ou difficilement accessible et intelligible (en particulier, du fait du recours à un vocabulaire abstrait et ambigu).

Enfin, les vérifications ont également mis en lumière de mauvaises pratiques en termes de sécurité des données traitées, plus particulièrement s'agissant de la complexité des mots de passe.

FOCUS

La charte des contrôles

En raison des enjeux importants liés aux contrôles de la CNIL, il est essentiel que les organismes concernés comprennent le déroulement des investigations et sachent comment la CNIL peut intervenir.

Publiée en septembre 2020, **la charte des contrôles** présente en détail le processus d'un contrôle de la CNIL. Elle précise l'**objectif**, le **contexte procédural et législatif**, le **déroulement** et les **suites possibles** d'un contrôle. La charte rappelle également que les contrôles sont déclenchés sur décision de la présidente de la CNIL et sont réalisés par des agents habilités et soumis au secret professionnel.

De même que les organismes contrôlés ont des droits (d'information, de vérification des identités des agents de contrôle, d'être assistés d'un conseil), la charte rappelle leur devoir de coopérer avec la délégation en charge du contrôle.

La charte est un outil qui contribue au bon déroulement des contrôles, qui constituent une modalité d'action essentielle pour une protection effective des données personnelles.

Au regard de ces différents constats, plusieurs mesures correctrices (par exemple des mises en demeure) pourraient être adoptées dans les prochains mois.

LES SANCTIONS PRONONCÉES

Chiffres clés

15

DÉCISIONS ADOPTÉES PAR LA FORMATION RESTREINTE, DONT :

11
AMENDES POUR UN MONTANT TOTAL DE 138 489 300 EUROS (6 AMENDES SEULES ET 5 AMENDES ASSOCIÉES À DES INJONCTIONS SOUS ASTREINTE)

1
INJONCTION SOUS ASTREINTE (NON ASSOCIÉE À UNE AMENDE)

2
RAPPELS À L'ORDRE

1
NON-LIEU

14

PROJETS DE SANCTION EUROPÉENS EXAMINÉS PAR LA CNIL, DONT :

6
DÉCISIONS ADOPTÉES PAR LA FORMATION RESTREINTE OU SON PRÉSIDENT, CONTENANT DES OBJECTIONS PERTINENTES ET MOTIVÉES ET / OU DES COMMENTAIRES

49

MISES EN DEMEURE, DONT :

3
MISES EN DEMEURE PUBLIQUES

4
MISES EN DEMEURE ADOPTÉES EN COOPÉRATION AVEC LES CNIL EUROPÉENS

Un montant total record

En 2020, la formation restreinte (voir encadré) a prononcé **14 sanctions**, dont 11 publiques, ainsi qu'une décision aboutissant à un non-lieu. Ces sanctions comportent 11 amendes administratives, d'un montant total de **138 489 300 euros**, et 5 injonctions sous astreinte.

Cette année, les décisions de la formation restreinte ont concerné des secteurs d'activité et des acteurs très divers, ainsi que des manquements très variés (voir le tableau). Pour la première fois, la formation restreinte a adopté une sanction en coopération avec ses homologues européens, dans le cadre du mécanisme prévu par le RGPD, le « guichet unique ».

Dans le cadre de la coopération européenne, la formation restreinte et son président ont également examiné 14 projets de décision soumis par différentes autorités de protection des données de l'Union européenne. 6 décisions ont été prononcées, comportant principalement des objections pertinentes et motivées (c'est-à-dire des demandes formelles de modification du projet de décision soumis, par exemple afin que le montant d'une sanction soit revu pour être plus dissuasif).

INFOSPLUS

La formation restreinte de la CNIL

La formation restreinte de la CNIL, composée de 6 membres (dont un président distinct du président de la CNIL), est l'organe chargé de prononcer des sanctions. En 2020, le président de la formation restreinte est Alexandre Linden.

Les mises en demeure, qui représentent un type particulier de décision, ne sont pas prononcées par cette formation mais par la présidente de la CNIL.

Aperçu des décisions adoptées par la formation restreinte

Date de la délibération	Nom ou type d'organisme	Décision adoptée	Manquements principaux/Thème
28/07/2020	Spartoo	Sanction pécuniaire de 250 000 euros et injonction sous astreinte	Minimisation des données, durées de conservation, information des personnes, sécurité
03/09/2020	Association politique	Non-lieu	Défaut de coopération avec la CNIL
03/09/2020	Une députée	Rappel à l'ordre	Traitement illicite des données
03/09/2020	Rectorat de l'académie de Normandie	Rappel à l'ordre	Traitement illicite des données
18/11/2020	Carrefour France	Sanction pécuniaire de 2 250 000 euros	Durées de conservation, information des personnes, droits des personnes, sécurité, manquement relatif aux cookies
18/11/2020	Carrefour Banque	Sanction pécuniaire de 800 000 euros	Traitement déloyal des données, information des personnes, manquement relatif aux cookies
18/11/2020	Coopérative de commerçants détaillants	Sanction pécuniaire de 150 000 euros	Sécurité
03/12/2020	Société de transport de voyageurs par taxi	Sanction pécuniaire de 3 000 euros	Défaut de coopération avec la CNIL
07/12/2020	Google LLC et Google Ireland Limited	Sanctions pécuniaires de 60 et 40 millions d'euros et injonction sous astreinte	Manquement relatif aux cookies
07/12/2020	Amazon Europe Core	Sanction pécuniaire de 35 millions d'euros et injonction sous astreinte	Manquement relatif aux cookies
07/12/2020	DR X	Sanction pécuniaire de 3 000 euros	Sécurité, notification de violation de données
07/12/2020	DR Y	Sanction pécuniaire de 6 000 euros	Sécurité, notification de violation de données
07/12/2020	Performeclic	Sanction pécuniaire de 7 300 euros et injonction sous astreinte	Défaut de consentement (article L. 34-5 du CPCE), pertinence des données, durées de conservation, information des personnes, droits des personnes, défaut d'encadrement contractuel du sous-traitant
08/12/2020	Société de prestations de garde d'enfants à domicile	Injonction sous astreinte	Minimisation des données, durées de conservation, sécurité
08/12/2020	Nestor	Sanction pécuniaire de 20 000 euros et injonction sous astreinte	Défaut de consentement (article L. 34-5 du CPCE), information des personnes, droits des personnes, sécurité

Les mises en demeure

En 2020, la présidente de la CNIL a prononcé 49 mises en demeure, dont 3 ont été rendues publiques. Deux mises en demeure ont été adoptées en février 2020 à l'encontre d'EDF et d'ENGIE, notamment pour non-respect de certaines conditions de recueil du consentement concernant les données des compteurs communicants LINKY. La troisième mise en demeure rendue publique en juillet 2020 portait sur l'application « StopCovid » (voir page 25).

FOCUS

Deux amendes record adoptées par l'autorité britannique de protection des données en coopération avec la CNIL

L'ICO, autorité britannique de protection des données, a infligé deux amendes record en matière de sécurité au titre du RGPD. Ces amendes, de 20 millions de livres sterling (environ 22 millions d'euros) pour British Airways et de 18,4 millions de livres sterling (environ 20 millions d'euros) pour Marriott, ont été décidées en réponse à des violations de données ayant rendu accessibles à des tiers de très nombreuses données personnelles.

L'adoption de ces deux sanctions rappelle que la sécurité des données nécessite une vigilance permanente, tout particulièrement pour de tels opérateurs, avec de lourdes conséquences en cas d'infraction. Ces décisions illustrent par ailleurs une coopération fructueuse entre autorités de protection européennes, au service des citoyens.

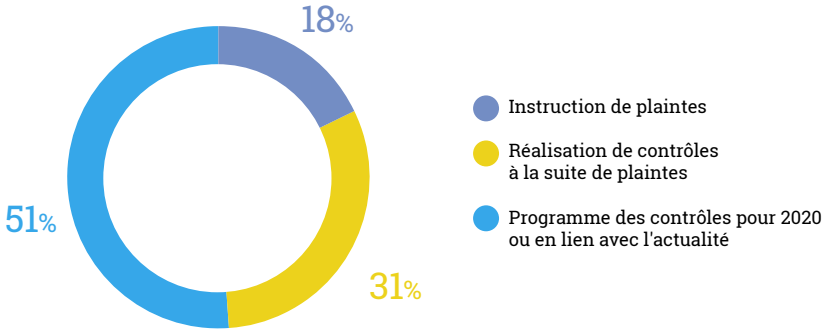
En effet, en application du mécanisme de coopération prévu par le RGPD, le « guichet unique », les projets de décisions ont été adressés aux autorités européennes de protection des données et ont été minutieusement examinés par la CNIL. La formation restreinte de la CNIL s'est ainsi prononcée sur les suites à donner. Après des échanges fructueux avec l'ICO, la CNIL a approuvé les projets tant s'agissant des manquements retenus que des montants des amendes proposées. Elle a notamment estimé que ces montants substantiels, et sans précédent en matière de sécurité, étaient proportionnés au regard de la gravité des manquements constatés.

À la suite de plaintes, la présidente de la CNIL a également mis en demeure plusieurs organismes utilisant des badgeuses photo de mettre leurs dispositifs de contrôle des horaires en conformité avec le RGPD. Des mises en demeure ont également été adoptées à l'encontre de communes ne respectant pas le cadre légal pour la verbalisation par lecture automatisée des plaques d'immatriculation (LAPI).

4 mises en demeure ont par ailleurs été adoptées en coopération avec des autorités de protection européennes, dans le cadre du mécanisme de guichet unique.

En outre, la présidente a également adressé 38 rappels à l'ordre et 2 avertissements à des organismes suite à des contrôles ou à des plaintes. Parmi eux, 7 font suite à des plaintes de résidents d'autres pays européens à l'encontre d'organismes français.

Origine des mises en demeure



L'année 2020 reflète ainsi une tendance équilibrée quant à l'origine des mises en demeure, qui résultent à parts égales de plaintes reçues par la CNIL et de contrôles réalisés à son initiative.

FOCUS

Décision Spartoo :

une première sanction adoptée après une procédure de coopération européenne

La société Spartoo est spécialisée dans le secteur de la vente en ligne de chaussures. Elle dispose d'un site web accessible dans treize pays de l'Union européenne. La CNIL a contrôlé la société, en mai 2018, et a constaté des manquements concernant les données personnelles des clients, des prospects et des salariés.

Une procédure de sanction à l'encontre de cette société a été engagée en 2019. Les clients et prospects de la société étant situés dans plusieurs pays européens, la CNIL a coopéré tout au long de la procédure avec ses homologues en vue de l'adoption de la décision de sanction.

Sur la base des investigations menées, la formation restreinte de la CNIL a considéré que la société avait manqué à plusieurs obligations prévues par le RGPD.

La société a d'abord manqué à son obligation de minimiser les données traitées. En l'espèce, Spartoo collectait des données non nécessaires aux finalités poursuivies et conservait également des données qu'elle n'utilisait plus par la suite. Par exemple, elle procédait à l'enregistrement intégral et permanent des appels téléphoniques reçus par les salariés du service client. Or, ces enregistrements étaient utilisés uniquement par la personne chargée de la formation des salariés, qui n'écoutait qu'un enregistrement par semaine et par salarié. Cet enregistrement intégral et permanent était donc excessif.

La société a ensuite manqué à son obligation de limiter la durée de conservation des données. Aucune durée de conservation des données des clients et des prospects n'était mise en place par la société au jour du contrôle réalisé, et la société a ainsi conservé pendant plusieurs années un nombre très important de données d'anciens clients (plus de 3 millions de clients ne s'étant pas connectés à leur compte depuis plus de 5 ans). La société conservait également les données de ses prospects alors qu'elle avait arrêté de leur adresser de la publicité depuis plusieurs années.

La société a aussi manqué à son obligation d'information des personnes, puisque l'information fournie dans sa politique de confidentialité comprenait des mentions erronées et les salariés n'étaient pas correctement informés de l'enregistrement des appels reçus.

Enfin, la société a également manqué à son obligation d'assurer la sécurité des données en exigeant des mots de passe d'accès aux comptes clients pas assez robustes et en conservant pendant six mois, et en clair, des scans de carte bancaire.

En conséquence, et après concertation avec l'ensemble des autorités de protection des données européennes concernées, la formation restreinte a prononcé en juillet 2020 une amende de 250 000 euros et a enjoint à la société de mettre ses traitements en conformité avec le RGPD et d'en justifier sous un délai de trois mois à compter de la notification de la délibération, sous astreinte de 250 euros par jour de retard.

FOCUS

Focus sur les sanctions Google et Amazon en matière de cookies

Par deux délibérations du 7 décembre 2020, la formation restreinte de la CNIL a prononcé des amendes record à l'encontre de Google et d'Amazon, respectivement à hauteur de 100 millions d'euros et de 35 millions d'euros, pour avoir enfreint la législation française sur les cookies.

Entre novembre 2019 et juillet 2020, la CNIL a procédé à des investigations relatives au dépôt de cookies sur les terminaux des internautes résidant en France lorsque ces derniers se rendent sur les sites web google.fr et amazon.fr.

Sur la base de ces investigations, la formation restreinte a relevé plusieurs violations à l'article 82 de la loi Informatique et Libertés.

LES MANQUEMENTS À LA LOI : ABSENCE DE CONSENTEMENT ET DÉFAUT D'INFORMATION

Tout d'abord, lorsqu'un internaute se rendait sur les sites web google.fr et amazon.fr, des cookies publicitaires étaient immédiatement déposés sur son terminal, sans aucune action de sa part. Or, ce type de cookies, non essentiels au service, ne peuvent être déposés sans que l'internaute ait préalablement donné son consentement.

La formation restreinte a ensuite considéré que l'information fournie lors de la consultation de ces sites n'était pas suffisamment claire sur les finalités poursuivies par les cookies, ni sur les moyens permettant de les refuser. Concernant Amazon, elle a également relevé que, lorsque les utilisateurs se rendaient sur le site amazon.fr après avoir cliqué sur une annonce affichée sur un autre site, aucune information ne leur était donnée.

Enfin, concernant Google, une défaillance partielle du mécanisme « d'opposition » a été relevée, un des cookies publicitaires restant stocké sur l'ordinateur après la désactivation, par l'internaute, de la personnalisation des annonces.

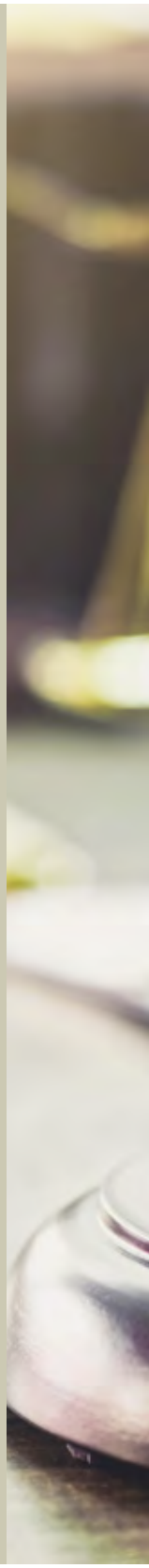
LES SANCTIONS PRONONCÉES PAR LA FORMATION RESTREINTE

La formation restreinte a prononcé des amendes publiques de 35 millions d'euros à l'encontre d'Amazon et de 100 millions d'euros à l'encontre de Google (60 millions d'euros à l'encontre de Google LLC et 40 millions à l'égard de Google Ireland Limited).

Pour déterminer ces montants, la formation restreinte a notamment tenu compte du nombre considérable de personnes concernées par les manquements, en rappelant le rôle prépondérant joué par le moteur de recherche Google Search et par la plateforme d'achat en ligne Amazon en France, et des bénéfices tirés par les sociétés sur le marché de la publicité en ligne ou sur la visibilité des produits sur le web.

En complément des amendes, la formation restreinte a également adopté des injonctions sous astreinte afin que les sociétés fournissent une information conforme à la loi Informatique et Libertés dans un délai de trois mois. À défaut, les sociétés s'exposent chacune au paiement d'une astreinte de 100 000 euros par jour de retard.

S'agissant enfin de la compétence, la formation restreinte a rappelé que la CNIL est compétente pour contrôler et sanctionner les cookies déposés par les sociétés sur les ordinateurs des utilisateurs résidant en France, ces opérations relevant de la directive ePrivacy, transposée à l'article 82 de la loi Informatique et Libertés, et étant réalisées dans le cadre des activités des établissements français de ces sociétés, conformément à l'article 3 de la loi.



CONTENTIEUX

Dans certains cas, il est possible de contester les décisions de la CNIL, par exemple des sanctions, devant le Conseil d'État, la plus haute juridiction administrative française. Dans d'autres cas, des recours peuvent être déposés devant des tribunaux administratifs. La CNIL revient sur trois grandes décisions qui ont marqué 2020.

Corentin
Juriste au service des sanctions et du contentieux

J'ai rejoint le service des sanctions et du contentieux il y a presque trois ans. Ce service est composé d'une cheffe de service et de son adjointe, de dix juristes et de deux assistantes. Ensemble, nous sommes chargés de mettre en œuvre la procédure répressive de l'institution. Nous avons aussi la charge de défendre, lorsqu'elles sont attaquées devant les juridictions administratives (et principalement devant le Conseil d'État), les décisions prises par la CNIL, et notamment les sanctions prononcées par la formation restreinte et les mises en demeure adoptées par la présidente.

J'interviens après les travaux et investigations réalisés par mes collègues des services des contrôles ou du service des plaintes. Le service des sanctions constitue en effet le dernier maillon de la chaine répressive. Saisi des dossiers orientés vers mon service, je prépare des projets de mises en demeure prononcées par la présidente et j'analyse les réponses que les responsables de traitement y apportent. Lorsque les sociétés visées ne se sont pas mises en conformité après une mise en demeure, ou lorsque les spécificités du dossier justifient que la présidente engage directement une procédure de sanction, j'assiste le rapporteur qu'elle aura désigné dans la rédaction de son rapport et dans les échanges qui interviendront avec le responsable de traitement concerné pendant toute la procédure de sanction menée devant la formation restreinte de la CNIL.

Je peux aussi répondre, lorsque nous en recevons, aux saisines et autres demandes d'avis émanant d'autorités judiciaires (juges d'instruction, procureurs de la République, services de police ou de gendarmerie).

Enfin, je participe à la coopération européenne, notamment lors de l'examen de projets de sanctions soumis par nos homologues dans le cadre de la procédure de coopération prévue par le RGPD, ou lors de travaux menés avec les autorités de protection des données au niveau du CEPD.

La CNIL est partie ou observateur dans de nombreux recours introduits devant le Conseil d'État et les tribunaux administratifs. Ces recours, qui présentent une grande variété, peuvent concerner :

- la contestation d'une sanction prononcée par la CNIL ;
- la contestation d'une recommandation adoptée en séance plénière ;
- une clôture de plainte prise par la présidente de la CNIL ;
- une demande indemnitaire en cas de faute de la CNIL dans l'exercice de son activité ;
- la contestation d'un décret autorisant la création d'un traitement automatisé de données personnelles.

En 2020, **18 nouveaux recours** ont été introduits devant le Conseil d'État et **15 mémoires ont été produits par la CNIL**.

Les recours contre les sanctions revêtent une importance particulière au regard de leurs enjeux, tant en matière de montant des sanctions en cause que des questions juridiques à trancher. **Ainsi, le Conseil d'État a rendu plusieurs décisions centrales pour la CNIL au cours de l'année**. Il a en effet confirmé la sanction de 50 millions d'euros prononcée à l'encontre de la société Google LLC en 2019, validant l'application des principes clés du règlement général sur la protection des données par la CNIL (voir focus sur la décision Google).

D'autres sanctions de la formation restreinte ont été confirmées par le Conseil d'État :

- la sanction de 400 000 euros prononcée par la formation restreinte à l'encontre d'une société spécialisée dans la promotion immobilière pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre des modalités de conservation des données inappropriées (décision du 4 novembre 2020) ;
- l'amende administrative de 30 000 euros prise à l'encontre d'un organisme de logements sociaux pour détournement de finalités du traitement des données personnelles des locataires des logements sociaux (décision du 5 octobre 2020).

Les délibérations adoptant les recommandations de la CNIL peuvent aussi faire l'objet d'un recours pour excès de pouvoir devant le Conseil d'État. Ce fût le cas avec la délibération du 6 septembre 2018 adoptant une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance, validée par le Conseil d'État le 10 décembre 2020 (voir encadré sur la décision CDISCOUNT).

Par ailleurs, **plusieurs mémoires en observations ont été produits par la CNIL** parmi lesquels notamment, deux mémoires à l'appui de requêtes en référé dans le cadre du traitement et de la centralisation des données de santé par la Plateforme des données de santé *(Health Data Hub)* et du recours dirigé contre l'usage de drones par le ministère de l'Intérieur. La CNIL a également présenté des observations dans le cadre du recours dirigé contre le décret autorisant la création d'une identité numérique avec reconnaissance faciale (ALICEM) pour l'accès à des services en ligne (voir encadré sur la décision ALICEM). Les mémoires en observations amènent ainsi la CNIL à rappeler ses positions sur des questions de société majeures.

FOCUS

Décision CDISCOUNT

Le Conseil d'État a confirmé, le 10 décembre 2020, la recommandation « Carte bancaire » de la CNIL.

Le contexte

Lorsqu'un responsable de traitement souhaite conserver les données bancaires de ses clients afin de faciliter leurs éventuels achats ultérieurs, la CNIL considère qu'il est nécessaire pour l'organisme de recueillir le consentement préalable des personnes. Or, la société CDISCOUNT souhaitait pouvoir enregistrer par défaut les numéros de carte bancaire de ses clients sans avoir à recueillir leur consentement préalable. La société demandait donc que la CNIL reconnaisse, à partir d'une certaine récurrence d'achat (mais sans pour autant que le client souscrive à un abonnement), que la société disposait d'un intérêt légitime à conserver ces données bancaires.

La décision du Conseil d'État

Le 10 décembre 2020, le Conseil d'État a rejeté le recours de la société CDISCOUNT contre la décision implicite de refus de la CNIL de modifier sa recommandation du 6 septembre 2018 sur le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance.

Le Conseil d'État a rejeté le recours de la société en **écartant les différentes bases légales autres que le consentement**. Il a notamment procédé, au titre de l'intérêt légitime, à une mise en balance des intérêts des sociétés et des personnes concernées.

Il a en effet considéré que l'intérêt des sociétés, qui consiste à faciliter des paiements ultérieurs en dispensant le client de saisir son numéro de carte bancaire à chacun de ses achats, ne saurait prévaloir sur l'intérêt des clients de protéger leurs données au regard de la sensibilité des informations bancaires et des préjudices susceptibles de résulter de la captation de ces données et d'une utilisation détournée. Ceci, d'autant que les personnes concernées ne peuvent raisonnablement s'attendre à ce que les entreprises conservent leurs données bancaires sans leur consentement lors d'achats ponctuels.

FOCUS

Décision ALICEM

Le Conseil d'État a confirmé, le 4 novembre 2020, la création d'une identité numérique avec reconnaissance faciale (ALICEM).

Le contexte

Le décret du 13 mai 2019, pris après un avis de la CNIL, a autorisé la mise en œuvre d'un traitement automatisé de données personnelles dénommé « authentification en ligne certifiée sur mobile » (ALICEM). Il prévoit, pour les titulaires d'un passeport ou d'une carte de séjour biométrique, la création d'une identité numérique avec reconnaissance faciale pour l'accès à des services en ligne.

L'association La Quadrature du Net a contesté ce décret, reprenant la réserve émise par la CNIL dans son avis du 18 octobre 2018. Elle a fait valoir que le consentement des utilisateurs de l'application ALICEM au traitement de données biométriques issues de la reconnaissance faciale n'était pas librement recueilli, contrairement aux exigences de l'article 9 du RGPD, faute de mettre en place un autre moyen d'identification que la reconnaissance faciale pour l'utilisation de l'application ALICEM. La CNIL a également déposé un mémoire en observation à l'appui du recours.

La décision du Conseil d'État

Dans sa décision du 4 novembre 2020, le Conseil d'État a rejeté la requête de la Quadrature du Net. Il considère que **le consentement au traitement de données biométriques est libre** dès lors que les téléservices accessibles via l'application Alicem l'étaient également à travers le dispositif FranceConnect, dont l'utilisation ne présuppose pas le consentement à un traitement de reconnaissance faciale.

Le Conseil d'État précise que **le refus du consentement de la personne à la reconnaissance faciale ne lui fait donc pas subir de préjudice** puisqu'elle peut accéder aux mêmes téléservices que ceux accessibles via l'application ALICEM, sans recours à la reconnaissance faciale.

Le Conseil d'État considère ainsi que l**a liberté du consentement s'apprécie dans le cas d'espèce** au regard des alternatives proposées dans FranceConnect et que **l'usage d'un téléservice n'est pas obligatoire**.

Ainsi, aujourd'hui, sans création d'une identité numérique de niveau élevé, de type ALICEM, un usager peut continuer à accéder aux mêmes services en ligne car les fournisseurs de services en ligne n'exigent pas une telle identification. En revanche, à l'avenir, le développement de certains services en ligne nécessitant une identification de niveau élevé (par exemple le vote électronique avec une identité numérique) privera l'usager d'y accéder dès lors qu'il ne disposera pas d'une telle identité.

FOCUS

Décision GOOGLE

Le Conseil d'État a confirmé, le 19 juin 2020, la sanction de 50 millions d'euros prononcée en 2019 par la CNIL.

Le contexte

Le 21 janvier 2019, la formation restreinte de la CNIL a prononcé à l'encontre de la société Google LLC une amende de 50 millions d'euros, sanctionnant des manquements relatifs à l'information et au consentement au traitement des données personnelles des utilisateurs du système d'exploitation Android.

La formation restreinte avait considéré que les informations communiquées aux utilisateurs créant un compte Google n'étaient pas toujours claires et facilement accessibles. Elles étaient en outre incomplètes. La formation restreinte reprochait également à la société Google LLC de ne pas recueillir un consentement valable des utilisateurs pour le traitement relatif à la personnalisation de la publicité. En effet, le recueil du consentement se faisait au moyen d'une case précochée par défaut.

La société Google LLC a contesté devant le Conseil d'État cette sanction.

La décision du Conseil d'État

sur la compétence de la CNIL

Tout d'abord, la société Google estimait que l'autorité de protection des données irlandaise était seule compétente pour contrôler ses activités dans l'Union européenne, en application du mécanisme du guichet unique. Ce mécanisme prévoit que, en cas de traitement transfrontalier, l'autorité de contrôle de l'État où est situé l'établissement principal de la société est considérée comme autorité chef de file.

Sur ce point, le Conseil d'État a considéré que le système du guichet unique n'était pas applicable. En effet, l'établissement principal du responsable de traitement correspond en principe au lieu de son administration centrale dans l'Union européenne (UE), c'est-à-dire le lieu de son siège réel.

Ce critère doit cependant être écarté lorsqu'un autre établissement de la société est compétent pour prendre les décisions relatives aux finalités et aux moyens du traitement et dispose du pouvoir de les faire appliquer à l'échelle de l'UE. Lorsqu'au sein de l'UE, le responsable de traitement ne dispose ni d'une administration centrale, ni d'un établissement disposant d'un pouvoir de décision sur le traitement, le Conseil d'État rappelle que le mécanisme du guichet unique ne peut pas s'appliquer. Considérant que rien n'indiquait que la société Google Ireland Limited exerçait, au jour de la décision, un pouvoir de direction et de contrôle réel sur les autres filiales européennes ni qu'elle était en mesure de prendre des décisions quant aux finalités et aux moyens du traitement en cause, **le Conseil d'État a confirmé que la CNIL était compétente pour prononcer la sanction contestée**.

Sur les manquements constatés

Ensuite, le Conseil d'État a confirmé l'appréciation faite par la CNIL sur les manquements constatés. Il a en effet considéré que l'information était éparpillée, ce qui nuisait à son accessibilité et à sa clarté alors que les traitements en cause sont particulièrement intrusifs par leur nombre et la nature des données collectées. En outre, l'information disponible était lacunaire.

De même, le Conseil d'État a considéré que, faute de disposer d'une information suffisante au moment où elles exprimaient leur choix, **les personnes concernées ne pouvaient donner un consentement libre et éclairé** au traitement de leurs données aux fins de personnalisation de la publicité.

Sur le montant de la sanction

Dans ces conditions, compte tenu de la gravité des manquements commis, de leur caractère continu et de leur durée, **le Conseil d'État a considéré que le montant de l'amende n'était pas disproportionné**.

ANTICIPER,
innover et développer la réflexion éthique

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 2020, la CNIL a mené plusieurs réflexions sur la portabilité, les assistants vocaux et les mutations dans le monde du travail, qui ont fait l'objet d'évènements en ligne.

Martin
Chargé d'études prospectives au pôle innovation, études et prospectives

Le laboratoire d'innovation numérique de la CNIL est composé de profils variés, dont les parcours vont de l'expertise technique à celle des sciences humaines et sociales, en passant par le design. Son rôle est d'appréhender les innovations dans le numérique, d'en mesurer les usages comme les impacts sur la vie privée des individus. Cela passe notamment par des expérimentations techniques (par exemple sur les assistants vocaux), des études exploratoires (sur le quotidien des personnes face au numérique), de la création d'outils (à destination des besoins internes, mais également pour les usagers de la CNIL, à l'instar de CookieViz), ou encore par la création de liens avec les différents acteurs du numérique, qu'ils s'agissent des milieux de la recherche, de la société civile, des entreprises et startups, etc.

L'ensemble de ces travaux est recensé sur le site linc.cnil.fr, sur lequel nous publions également des articles ou des interviews sur les sujets touchant au numérique et à la protection des données personnelles. Nous produisons également des études plus longues, sous la forme des Cahiers IP (Innovation et Prospective), qui nous permettent d'alimenter la réflexion sur des enjeux encore émergents. Ils ont également pour but de créer de la discussion : dans leurs dernières parties sont formulées des recommandations et des pistes, tant pour le régulateur que pour certains autres acteurs concernés par le sujet d'exploration. Le 8e cahier IP, publié au premier semestre 2021, concernera ainsi la protection des données au quotidien par les individus.

PORTABILITÉ : DÉVELOPPER LES DROITS ET LES USAGES

Un droit prévu par le RGPD, une stratégie européenne

Le droit à la portabilité, consacré par le règlement général sur la protection des données (RGPD) en 2018, marque une véritable innovation par le droit. Si tout citoyen européen doit pouvoir conserver la maîtrise de ses données, **l'article 20 du RGPD permet à chacun de pouvoir les réutiliser librement**, par exemple en les transmettant d'un service à un autre.

Le droit à la portabilité offre de nouvelles perspectives pour les utilisateurs, mais aussi pour tout un écosystème d'acteurs, privés et publics, souhaitant créer des services innovants.

La circulation des données est au cœur des enjeux de régulation croisés entre droits des individus, droit de la concurrence et protection des consommateurs. Dans un contexte où la Commission européenne, dans sa stratégie européenne pour les données, réaffirme que « la façon dont les données sont collectées et utilisées doit placer les intérêts de l'individu en première place », l'article 20 du RGPD a aussi pour ambition de « permettre de nouveaux flux de données et de favoriser la concurrence ».

Un sujet étudié par la CNIL depuis 2013

Très tôt, la CNIL s'est emparée du sujet pour définir ce nouveau droit à la portabilité. Dès 2013, son laboratoire d'innovation numérique (LINC) prenait part au projet de *Self Data* porté par la FING (Fondation internet nouvelle génération).

En 2017, elle a activement participé à la rédaction des lignes directrices du G29 (nom du groupe des CNIL européennes avant l'entrée en application du RGPD) sur ce droit, participait aux conférences *MyData*, dont l'objectif est de promouvoir de nouveaux modèles de gestion des données, sous le contrôle des utilisateurs, dès 2016. Dans cette continuité et deux ans après l'entrée en application du RGPD, la CNIL réaffirme son engagement pour le développement et l'application de ce droit consacré par l'article 20 de ce règlement.

Un évènement dédié au droit à la portabilité

La CNIL a organisé, le 23 novembre 2020, un événement en visioconférence dédié au droit à la portabilité. Près de 1 500 personnes se sont inscrites, avec des pics d'audience à près de 600 personnes connectées simultanément. Ces échanges ont permis de dresser un premier état des lieux de la portabilité, en France et dans le monde, de répondre à des questions pratiques et lever d'éventuels freins au développement de ce droit.

Cet après-midi d'échanges, à l'invitation de **Marie-Laure Denis**, présidente de la CNIL, réunissait notamment **Thierry Breton**, commissaire européen au Marché intérieur, **Isabelle de Silva**, présidente de l'Autorité de la concurrence, **Noah Phillips**, commissaire de la Federal Trade Commission (États-Unis), **Sir Tim Berners-Lee**, cofondateur d'Inrupt, ainsi que **des représentants des parties prenantes d'entreprises privées, associations, porteurs de solutions et promoteurs de la portabilité**.

FOCUS

Une recommandation à venir sur l'exercice des droits via un mandat

Toute personne peut mandater une société afin que celle-ci exerce ses droits à sa place. Afin de clarifier le cadre applicable, la CNIL a ouvert en novembre 2020 à la consultation publique son projet de recommandation sur l'exercice des droits via un mandat.

Les recommandations concernent notamment les questions de la sécurisation de la transmission des données par le mandataire à la personne concernée, ou à un autre responsable de traitement (dans le cadre d'une demande de portabilité) – notamment via des API –, le stockage des données, la réutilisation des données, etc. Des réponses qui permettront de clarifier le cadre pour les acteurs de la portabilité.

Le projet de recommandation devrait être adopté définitivement au premier semestre 2021.

Le droit à la portabilité offre de nouvelles perspectives pour les utilisateurs, mais aussi pour tout un écosystème d'acteurs, privés et publics, souhaitant créer des services innovants.

Les tables rondes proposées devaient permettre d'apporter des réponses à trois grandes questions :

- **Quels sont les enjeux en matière de régulations croisées ?**
- **Quels sont les leviers pour l'innovation et le développement ?**
- **Comment mettre en œuvre des solutions concrètes pour fluidifier la circulation des données entre services, dans le respect des droits des personnes ?**

Dans son introduction, Thierry Breton a réaffirmé le caractère « primordial de faire vraiment fonctionner la portabilité des données, pour les entreprises et pour les citoyens ». Il a évoqué le projet de *Data Governance Act* (DGA), publié en décembre 2020, qui a pour vocation à accompagner et renforcer ce droit, pour « permettre l'utilisation de données personnelles avec l'aide d'un intermédiaire de partage de données personnelles ».

Ces intermédiaires, que l'on nomme parfois les cloud personnels, ou les *PIMS* (*personal information management system*) seraient soumis, avec le DGA, à une procédure de notification, et à des règles à respecter, au-delà du RGPD.

Lors de son intervention, Isabelle De Silva a rappelé l'intérêt de la portabilité d'un point de vue concurrentiel, un droit qui « favorise la mobilité et empêche que quelqu'un se trouve enfermé dans un écosystème ». Un droit qu'il faut promouvoir pour Alain Bazot, président de l'UFC Que Choisir, car « la portabilité est un concept encore largement méconnu, l'Arlésienne du RGPD ». Marie-Laure Denis a confirmé que « ce droit est encore peu actionné par les individus, de même la CNIL reçoit peu de plaintes à ce sujet, une trentaine de plaintes en deux ans » et ajoute que « son développement passera par les usages, par la création de nouveaux services et par les solutions offertes aux individus ».

Ce droit, s'il est encore peu revendiqué par le grand public, est déjà porté par des startups, mais aussi des grands acteurs français, qui y ont vu très tôt un levier d'innovation partagée avec leurs clients et se sont déjà lancées dans des démarches proactives et innovantes. Enedis, représentée par Lydia Sartout, (directrice pôle projets et solutions), a lancé une plateforme dédiée à la portabilité[32], afin de permettre des nouveaux services basés sur les données de Linky. Romain Liberge, *chief digital officer* de la MAIF, a expliqué comment la mutuelle a expérimenté avec ses sociétaires la mise à disposition d'espace personnels de données, « pour accompagner un mouvement de réappropriation de leurs données par les utilisateurs, pour rééquilibrer la relation et maintenir la confiance », avec un enjeu, « trouver des cas d'usages pour rendre ce sujet simple d'accès ».

Ces expériences démontrent l'importance, pour le développement des usages, de la mise en place de solutions interopérables pour la mise en œuvre concrète de la circulation des données. Alors que le *Data Transfer Project* réunit des plateformes internationales dans un projet de connecteur de données *open source*, Tarik Krim (Polite.one) a estimé que « l'interopérabilité est l'outil de l'Internet ouvert, la portabilité est l'outil [contre] l'internet boîte noire ».

L'association NewGovernance, portée par Mathias de Bièvre, va plus loin et milite pour le développement de nouveaux standards européens, non plus seulement techniques, mais de gouvernance des données. Chacun se retrouve dans la nécessité de passer par les solutions technologiques pour rendre lisibles les droits et les services associés à la circulation des données sous le contrôle des utilisateurs.

En conclusion, Marie-Laure Denis a réaffirmé la contribution de la CNIL, « dans son rôle de régulateur, la CNIL entend continuer à contribuer au développement des outils qui permettront l'interopérabilité » et l'effectivité du droit à la portabilité, notamment par la publication d'une recommandation sur l'exercice des droits via un mandat (voir encadré), qui permettra de répondre aux questions, tant des responsables de traitement tenus de mettre en œuvre la portabilité des données, que des nouveaux acteurs qui se positionnent sur ce marché. Enfin, elle a rappelé « comme elle le fait pour l'ensemble des droits des personnes qui sont au cœur de ses missions, la CNIL continuera de veiller à garantir l'exercice légitime de ce droit, chaque fois qu'il est requis ».

INFOSPLUS

La rediffusion de l'évènement sur la portabilité est disponible sur le site web de la CNIL :

cnil.fr/evenement-portabilite-2020

32 https://datahub-enedis.fr

AIR : UN NOUVEAU FORMAT POUR LA MISSION ÉTHIQUE DE LA CNIL

La loi pour une République numérique du 7 octobre 2016 a confié à la CNIL la mission de conduire une réflexion sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques. De par son rôle en matière de protection des données et sa position au carrefour entre régulation et anticipation prospective, la CNIL pose un regard différent sur ces questions reliant éthique, libertés, données et usages du numérique.

Après avoir organisé une série d'événements sur le thème de l'intelligence artificielle et des algorithmes en 2017, puis un colloque au Conseil économique, social et environnemental sur le thème des *civic tech* en 2019, la CNIL a décidé d'ancrer sa mission éthique dans le paysage événementiel de l'innovation en la dotant d'un nom identifiable : **« Avenirs, Innovations, Révolutions », trois mots-clés formant l'acronyme « air ».**

Avec cette marque, la CNIL souhaite créer un rendez-vous annuel, pour prendre de la hauteur et poser des clés de compréhension du monde numérique actuel, afin de se projeter vers des futurs éthiquement souhaitables. Cette refonte s'accompagne également d'une nouvelle identité graphique, d'une page dédiée sur le site de la CNIL (**cnil.fr/air**) et de **cahiers**, qui permettent de cristalliser les débats, synthétiser les moments saillants du colloque et acter certaines recommandations éthiques émises en vue de jouer un rôle auprès des décideurs.

air2020 : Droit(s) et libertés numériques au travail

air2020, organisé le 9 novembre 2020, a ainsi inauguré le parcours de réflexion que la CNIL souhaite construire. Cet évènement, qui a permis de convier de nombreux interlocuteurs à se joindre aux débats (entreprises et organisations, institutions, experts, grand public), a proposé une approche **pluridisciplinaire**, en alternant sujets d'actualité, expériences terrain, regards scientifiques et scénarios spéculatifs de « design fiction », dans la continuité des cahiers Innovation et Prospective.

En 2020, le thème retenu était celui des **ressources humaines**, secteur vivant une réelle révolution numérique de par la modernisation très rapide de ses activités, qu'il s'agisse de la digitalisation de la fonction RH, de la réorganisation des entreprises, des nouveaux outils de recrutement et de management automatisé en temps réel. Les DRH doivent ainsi maîtriser l'analyse de données avec les considérations éthiques indispensables que celle-ci implique.

Après une introduction de la présidente de la CNIL, **Marie-Laure Denis**, et une présentation de **Paul Duan**, président et cofondateur de l'ONG Bayes Impact, plusieurs tables-rondes ont ainsi été organisées lors de cet évènement :

- **« Quelle place pour l'IA sur le marché de l'emploi ? »**, animée par **Sarah Akel**, directrice de l'innovation RH chez Change The Work et avec **Stéphanie Lecerf**, directrice de l'éthique et des affaires juridiques du cabinet Michael Page International France et vice-présidente d'A compétence égale ; **Laurence Devillers**, professeur en Intelligence Artificielle au LIMSI-CNRS-CERNA-DATAIA ; **Henri Isaac**, président de renaissance Numérique et maître de conférences à l'université PSL Paris-Dauphine et **Michel Cottura**, adjoint au DGA offre de service en charge du Pilotage des programmes et de la MOA chez Pôle emploi et directeur du programme intelligence emploi.

- **« Télétravail, retour d'expérience »**, avec les témoignages de **Amandine Brugière**, responsable du département Etudes Capitalisation Prospective chez Anact ; **Bruno Mettling**, président-fondateur de topics (conseil en stratégie de transformation), ancien DRH d'Orange Groupe et auteur du rapport ministériel Transformation numérique et vie au travail de 2015 ; **Danièle Linhart**, sociologue du travail, directrice de recherches émérite au CNRS, membre du laboratoire GTM-CRESPPA et **Éric Delisle**, chef du service des questions sociales, RH et sports à la CNIL.

- **« *People analytics* : surveillance ou bienveillance ? »**, avec deux témoignages d'**Olivier Tesquet**, journaliste spécialisé dans les questions numériques à Télérama et auteur de l'enquête d'investigation, *À la trace* sur la surveillance numérique, en particulier dans la sphère du travail et de **Bastien Kerspern**, co-fondateur et designer chez Design friction.

La CNIL a ainsi souhaité mobiliser tous les savoirs disponibles et confronter les points de vue pour concevoir une régulation adaptée et permettre un meilleur respect de nos droits et libertés.

En outre, la crise sanitaire, en accroissant significativement le recours au télétravail, a ouvert des débats en termes de protection de la vie privée, de surveillance au travail et de dialogue social. La CNIL aborde ces questions régulièrement : environ 20 % des plaintes qui lui sont adressées sont liées à la surveillance, tant dans des structures publiques que privées (+ 15 % par rapport à 2019). Ce bouleversement organisationnel collectif pourrait avoir des conséquences sur le long terme sur l'encadrement et la surveillance des employés, sur la sécurité des outils collaboratifs et de visioconférence, ainsi que sur l'équilibre entre la vie professionnelle et la vie personnelle, appelant une vigilance particulière quant à la protection de la vie privée.


CNIL.
air 2020
DROIT(S)
ET LIBERTÉS
NUMÉRIQUES
AU TRAVAIL :
RÉALITÉS
ET HORIZONS
9 novembre
à partir de 14h
Infos et inscription : cnil.fr/fr/evenement-air-2020

Les cahiers air : un nouveau format éditorial pour la CNIL

Le cœur des débats a été rassemblé dans un nouveau format éditorial : les cahiers air. Sa première édition, le cahier air2020, servira de base de réflexion pour les futures publications, guides, référentiels, lignes directrices et recommandations actuellement en cours ; une mise à jour de la recommandation du 21 mars 2002 relative au recrutement sera prochainement réalisée et publiée. Ce cahier permettra également à la CNIL d'accomplir pleinement son travail d'analyse et d'anticipation au service des citoyens, en partageant à large échelle ces travaux avec les décideurs publics et privés, afin de les aider à identifier des problèmes émergents, à nourrir leur veille et à les inciter à faire dialoguer, à leur tour, leurs parties prenantes. La CNIL travaille actuellement à l'élaboration du programme air2021 qui sera annoncé à la fin de l'été 2021.

INFOSPLUS

La rediffusion de l'évènement air2020 est disponible sur le site web de la CNIL :

cnil.fr/air2020

ASSISTANTS VOCAUX : LE PREMIER LIVRE BLANC DE LA CNIL

Le 7 septembre 2020, **la CNIL a publié son premier livre blanc**, intitulé *À votre écoute : exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*. Ce livre blanc, disponible sur le site web de la CNIL, est libre d'accès et gratuit.

Pour accompagner sa publication, une conférence en ligne a été organisée en partenariat avec le Voice Lab et a réuni plusieurs spécialistes du sujet pour évoquer le développement de ces « nouveaux majordomes » et des enjeux qui leur sont liés.

Une anthologie des travaux de la CNIL depuis 2016

La CNIL, par l'intermédiaire de son laboratoire d'innovation numérique (le LINC), suit depuis plusieurs années la question des assistants vocaux. En effet, dès 2016, des premières explorations étaient entreprises, permettant notamment d'alimenter des recommandations d'usages publiées dès l'arrivée de ces assistants vocaux sur le marché français l'année suivante. Depuis, des travaux d'analyse technique, des échanges avec des concepteurs, mais également des entretiens avec des spécialistes du sujet de la voix[33] ont permis de prolonger les réflexions et l'accompagnement des acteurs et du grand public.

Que ce soit dans nos foyers via les enceintes connectées ou dans d'autres objets connectés, comme au sein d'une voiture ou d'appareils ménagers, le déploiement de ces assistants est de plus en plus important. La CNIL entend appréhender dans sa globalité le sujet et ses enjeux du point de vue de la protection des données personnelles, afin de donner des clés aux différents acteurs.

À travers quatre chapitres, la publication présente ainsi :

- le **développement des assistants vocaux**, leur diffusion, les acteurs de l'écosystème et les usages que les individus en font ;
- les **questions éthiques** et en particulier celles relatives aux données personnelles et aux libertés ;
- des **cas d'application du RGPD** selon les usages et les acteurs en présence ;
- et enfin, **des conseils à destination des différents types d'acteurs**, du concepteur de l'assistant vocal à l'individu qui l'utilise, en passant par les développeurs d'application, les intégrateurs ou encore ceux qui déploient ces solutions.

La CNIL propose également, depuis la parution de ce livre blanc, un dossier thématique complet sur son site web, qui comprend des fiches pratiques, des ressources issues du livre blanc pour les professionnels et les particuliers, ainsi que plusieurs vidéos pédagogiques[34].

Un événement en ligne pour échanger sur ces enjeux

L'événement du 7 septembre 2020, diffusé librement en ligne, a rassemblé plus de 300 personnes. Ces dernières avaient la possibilité de poser des questions via un formulaire en ligne, et les personnalités présentes ont pu répondre aux interrogations des spectateurs.

INFOSPLUS

Les vidéos des interventions ont été mises en ligne à la suite de l'évènement et sont disponibles sur le site de la CNIL :

cnil.fr/assistants-vocaux-evenement-2020

33 Dossier « Assistants vocaux », 25 juin 2018, linc.cnil.fr

34 « Assistants vocaux : les conseils pour les utilisateurs et les professionnels », cnil.fr

En s'associant au Voice Lab, association française regroupant une communauté d'acteurs (institutionnels, de la recherche, de l'industrie, etc.) des technologies de la voix, la CNIL a pu porter un évènement commun qui a rassemblé spécialistes de la voix comme de la protection des données, professionnels comme grand public.

Après une **présentation du contenu du livre blanc**, neuf intervenants ont pris la parole :

- **Laurence Devillers**, professeure IA et éthique à la Sorbonne et CNRS Limsi et **Alexei Grinbaum** physicien et philosophe, chercheur au laboratoire LARSIM du CEA-Saclay, tous deux membres du Comité national pilote d'éthique du numérique (CNPEN), ont présenté leurs travaux et réflexions sur la question du déploiement de ces assistants vocaux et des enjeux éthiques qui leur étaient associés.

- **Emmanuel Vincent**, chercheur Inria et directeur de recherche au sein de l'équipe Multispeech a ensuite présenté l'état de la recherche scientifique croisant traitement de la parole et respect de la vie privée.

- **Christophe Cousin**, directeur des études, des affaires économiques et de la prospective au CSA et **Raphaël Berger**, directeur des études et de l'offre légale à la Hadopi ont présenté les résultats de leurs travaux issus du rapport conjoint entre les deux administrations, publié en 2019 : *Assistants vocaux et enceintes connectées - L'impact de la voix sur l'offre et les usages culturels et médias.*

- **Katya Lainé**, co-présidente du comité AI, Innovation & Technology du Syntec Numérique et CEO de Kwalys, éditeur français de plateforme d'IA conversationnelle, a, quant à elle, développé sa vision sur les enjeux économiques des assistants vocaux pour les entreprises, et les opportunités de la création de ce nouveau canal d'échanges entre entreprises ou institutions et les individus.

- **Zoé Aegerter,** designer consultante et **Sabrina Delale**, *design voice strategist*, toutes deux membres du Voice Lab et co-organistratrices de l'évènement, sont revenues sur les enjeux du *privacy by design*, mais aussi du design de la *privacy*.

- **Karel Bourgois**, président du Voice Lab, fondateur de Voxist et président de Slatchapp, a enfin conclu l'événement, rappelant les grands défis des assistants vocaux et des agents conversationnels de manière générale, mais également la nécessité des échanges entre les différentes parties prenantes afin de faire émerger des solutions vertueuses.

FOCUS

Les principes cardinaux pour la mise en place d'assistants vocaux

La CNIL met en avant quatre principes cardinaux, socle nécessaire pour susciter la confiance et l'adhésion des utilisateurs vis-à-vis de ces nouveaux équipements :

1. **Entretenir les frictions désirables :** plutôt que de se concentrer sur la mise en œuvre d'une expérience utilisateur absolument sans couture, profiter des moments de frictions (c'est-à-dire des moments de choix, de paramétrages nécessitant l'attention de l'utilisateur) pour présenter la réalité des traitements de données aux utilisateurs de manière adaptée.
2. **Privilégier le local au distant :** autant que faire se peut, mettre en œuvre des modalités et capacités de traitement des données directement dans les dispositifs, ce qui confère à l'utilisateur une bonne maîtrise de celles-ci et constitue un facteur de confiance et d'acceptabilité.
3. **Assurer les moyens de contrôle** : permettre à l'utilisateur de comprendre et maîtriser les usages qui sont faits de leurs données et de paramétrer le fonctionnement du dispositif selon ses choix.
4. **S'adapter au média vocal :** se reposer sur des interfaces exclusivement audio soulève d'importants défis en matière de présentation de l'information à l'utilisateur, de recueil de son consentement ou de mise en œuvre de moyens de contrôle. Il est donc nécessaire de mener une réflexion sur les moyens à déployer.

Les sujets de réflexion en 2021

Une nouvelle stratégie d'accompagnement

L'accompagnement des organismes publics et privés dans leur mise en conformité est une des missions essentielles de la CNIL. Dans un contexte où le RGPD pose un principe de responsabilisation des professionnels quant à leur conformité de leurs traitements de données, la CNIL apporte sécurité juridique et prévisibilité de la régulation.

La charte d'accompagnement des professionnels, une initiative inédite

La politique d'accompagnement de la CNIL a franchi, début 2021, une nouvelle étape dans le sens de la transparence avec la publication de la première charte d'accompagnement des professionnels[35]. Celle-ci donne aux responsables de traitement, sous-traitants ou fournisseurs de solutions techniques, les meilleures précisions qu'ils peuvent attendre de l'accompagnement apporté par la CNIL dans la limite de ses ressources.

La CNIL s'inscrit pleinement dans le mouvement d'une régulation ouverte sur les problématiques innovantes : consultations publiques en amont de la prise de décision, « bac à sable » RGPD, accueil d'expérimentations, etc. Elle déploie depuis 2017 une stratégie en direction des startups et témoigne, plus généralement, une grande attention aux modèles d'affaires innovants et aux technologies émergentes.

La CNIL promeut également l'inter-régulation dans le cadre de dialogues réguliers avec les autres régulateurs, superviseurs sectoriels ou autres autorités publiques, avec pour objectif une régulation cohérente dans ses différentes dimensions.

« La CNIL a mis en place une étanchéité entre services d'accompagnement et services répressifs, qui prévaut dans le cadre de la question posée aux services d'accompagnement et pour une activité à venir. »

35 « La CNIL publie sa charte d'accompagnement des professionnels », 12 février 2021, cnil.fr

INFOSPLUS

L'accompagnement apporté par la CNIL se déploie à trois niveaux :

GÉNÉRAL

La CNIL structure et publie sur son site web du « droit souple » qui comprend des référentiels, lignes directrices, recommandations, guides de bonnes pratiques, etc. à destination de l'ensemble des responsables de traitement. Il complète le « droit dur », obligatoire, composé notamment du RGPD et de la loi. La CNIL publie régulièrement son programme de travail et reste à l'écoute des besoins du terrain en la matière.

SECTORIEL

Outre les outils d'accompagnement sectoriel comme les codes de conduite ou les mécanismes de certification (voir page 64), la CNIL s'appuie prioritairement sur les fédérations professionnelles ou les groupes d'intérêt et partenaires privilégiés « têtes de réseau » avec qui elle entretient des relations régulières.

INDIVIDUEL

La CNIL est accessible aux professionnels via ses différentes permanences téléphoniques mais aussi dans le cadre d'une demande de conseil. La CNIL, compte tenu de ses ressources, priorise ce dernier point.

Le bac à sable RGPD

Comme évoqué dans son rapport annuel publié en 2019[36], la CNIL a pris le parti de compléter ses instruments traditionnels d'appui à l'innovation par la mise en place d'un « bac à sable » RGPD qui fournit un accompagnement renforcé, pendant une durée déterminée, à des projets emblématiques d'utilité publique. L'objectif est de proposer aux organismes d'aller plus loin que la simple conformité et de promouvoir des modèles d'affaires vertueux pour la vie privée et la protection des données. En effet, la protection des données est un facteur de confiance du public mais aussi, en elle-même, un vecteur d'innovation.

Publié en février 2021, le premier appel à projets « bac à sable » propose un accompagnement renforcé de 3 projets innovants dans le domaine de la santé numérique. Ce sujet, prioritaire pour les pouvoirs publics et la société, comporte des enjeux importants pour les libertés individuelles du fait du traitement de données de santé (qui sont des données sensibles).

Le bac à sable de la CNIL aura une vocation expérimentale pour lever une difficulté ou une incertitude, identifiée de manière partenariale avec le porteur de projet. Cette démarche vise à mettre en œuvre le respect de la vie privée dès la conception *(privacy by design)* d'un projet. Il ne vise pas des produits ou services déjà opérationnels.

Le bac à sable est ouvert à tous les produits ou services innovants, quel que soit le statut (public ou privé), la taille ou l'âge (*startup* ou acteur déjà existant), le secteur (industrie, services) et le caractère numérique ou non de l'activité concernée (neutralité technologique). Les critères portent sur le fond du projet : bénéfice pour le public, intérêt pour la protection des données, lien avec les priorités de la CNIL, engagement fort du porteur de projet.

Des contacts étroits et répétés avec les équipes juridiques et techniques de la CNIL apporteront dès ce printemps de la clarté sur la règle des solutions développées par le porteur de projet, en contrepartie des engagements pris par ce dernier.

Contrairement à d'autres « bac à sable » réglementaires, celui proposé par la CNIL ne permettra pas de s'affranchir des règles applicables, le RGPD ne prévoyant pas de dérogation pour ce motif. Le porteur de projet sera donc, quand le projet sera rendu opérationnel, pleinement responsable au titre du principe de responsabilité du RGPD. De plus, la CNIL a mis en place une étanchéité entre services d'accompagnement et services répressifs, qui prévaut dans le cadre de la question posée aux services d'accompagnement et pour une activité à venir : en d'autres termes, l'accompagnement de la CNIL n'empêchera pas des mesures répressives, par exemple une procédure de mise en demeure ou une sanction, si des manquements sont constatés.

Sur la base de cette première étape, l'année 2022 permettra, selon les premiers résultats et les ressources qui lui seront attribuées, d'amplifier ce dispositif.

> « La protection des données est un facteur de confiance du public mais aussi, en elle-même, un vecteur d'innovation. »

36 « Un bac à sable règlementaire en matière de données personnelles », Rapport annuel 2019 de la CNIL, p. 108, cnil.fr

Crise sanitaire : et après ?

La crise sanitaire a révélé plusieurs enjeux de réflexion prospective concernant la place des technologies numériques et des données personnelles dans notre société. Le solutionnisme technologique, la souveraineté et l'environnement sont notamment des enjeux sociaux de plus en plus liés à la protection des données personnelles et des libertés fondamentales.

Le confinement, un révélateur des inégalités sociales dans le numérique

L'épidémie de COVID-19, les mesures de confinement et de distanciation sociale imposées à la population, ont fait évoluer massivement les pratiques numériques (voir page 23).

S'il est encore tôt pour déterminer si cette intensification de ces usages mènera à un changement d'habitude durable, celle-ci révèle toutefois de profondes inégalités sociales quant à l'accès au numérique. Pour les 12 % de Français ne disposant pas d'une connexion de qualité minimale à internet, les mesures de confinement ont accentué l'exclusion sociale. De plus, nombre de foyers ne disposent pas du matériel ou d'un débit de connexion adéquat.

Des familles ont par exemple été contraintes de se partager un unique smartphone pour assurer toutes leurs pratiques numériques, du suivi des cours à distance donnés par les professeurs au maintien d'un lien social via les réseaux sociaux. Outre les difficultés pratiques et le retard scolaire que cela implique, ce partage familial d'un même dispositif pose question en termes de confidentialité des informations de chacun des utilisateurs. Par ailleurs, pour les 13 millions de Français en difficulté avec les outils numériques, la numérisation de nombreux services (de l'obtention d'une attestation de déplacement à la réalisation de démarches administratives) a accru les inégalités d'usage entre les individus. Confrontés à des adoptions à marche forcée de nouveaux usages, il convient de veiller à ce que la protection des données personnelles soit le parent pauvre de ces apprentissages.

La banalisation des dispositifs de surveillance

La crise sanitaire s'est caractérisée par une myriade d'initiatives portées tant par des autorités publiques que par des acteurs privés. Loin d'être orchestrés par un pouvoir central dans une politique globale et cohérente, les dispositifs de surveillance sont pluriels et s'entremêlent, de manière concurrentielle ou complémentaire, portés par des acteurs aux intérêts multiples, à l'échelle locale, nationale, européenne voire internationale. Ces dispositifs de surveillance utilisés pendant l'épidémie reposent sur des technologies et des infrastructures informationnelles largement préexistantes à la crise sanitaire. Toutefois, leur usage s'est banalisé dans des secteurs d'activité multiple, de la sécurité dans l'espace public au contrôle de l'activité des salariés ou des examens des étudiants, fragilisant l'équilibre précaire entre liberté et sécurité.

« Pour les 12 % de Français ne disposant pas d'une connexion de qualité minimale à internet, les mesures de confinement ont accentué l'exclusion sociale. »

FOCUS

La CNIL a publié, début 2021, un point d'étape sur ses activités dans le contexte de la COVID-19. Ce rapport, disponible dans le dossier thématique « COVID-19 », revient notamment sur les enjeux posés par l'utilisation des données personnelles et les pratiques numériques des Français.

Les données personnelles, un enjeu majeur de gestion de la crise

La nécessité des infrastructures publiques

Les données constituent un savoir important pour appréhender et gérer l'épidémie de COVID-19.

De la donnée de santé du dépistage d'un individu aux nombres agrégés de cas présentés chaque jour par la Direction générale de la santé, jusqu'aux instruments de traçage des populations porteuses du virus et à risque : toutes ces données, personnelles ou anonymisées, ont été utilisées dans le cadre de la mise en œuvre des soins et des politiques adaptées. Les écueils initiaux dans la remontée du nombre de cas au début de la crise sanitaire ont montré le caractère crucial des outils de surveillance sanitaire pour rendre visible le virus et sa propagation.

La CNIL restera vigilante quant au déploiement de ces solutions et de celles à venir, qui devront toujours être temporaires, proportionnées et respecter les impératifs de sécurité. Elle sera également sensible au respect des droits des personnes et à la destruction des données dès que l'objectif visé sera atteint et se réservera le droit de contrôler les systèmes concernés.

Données de paiement : de nouvelles réalités

Les données de paiement, leur circulation et leur protection font partie intégrante des enjeux de société. En 2020, la pandémie a remis cette question sur le devant de la scène, en accélérant certaines transformations à l'œuvre dans le domaine des paiements (recours accru au paiement sans contact, recul de l'usage des espèces, progrès des achats en ligne, etc.).

La tendance du recours aux espèces est au déclin, l'usage des nouveaux moyens de paiement numériques tel que le paiement mobile s'intensifie, les transferts de pair à pair augmentent, le recours aux portefeuilles électroniques s'accentue et le fintechs (technologies financières) se développent avec la mise en œuvre, notamment, de la deuxième directive sur les services de paiement (dite « DSP 2 »).

Le domaine des paiements connaîtra, à terme, des transformations encore plus profondes avec de nouvelles évolutions techniques comme les **projets de cryptomonnaies en cours** et ceux des **monnaies numériques de banque centrale** mais aussi le projet de réseau paneuropéen de carte bancaire EPI *(European Payments Initiative)*.

Dans ce contexte où les données de paiement sortent des parcours monétiques sécurisés traditionnels et circulent de manière croissante en ligne pour de nombreux usages numériques (parfois encore méconnus), la CNIL a estimé indispensable de développer sa compréhension dans ce domaine, afin d'affiner sa doctrine en matière de données de paiement et voir comment accompagner les évolutions en cours et futures.

Les données de paiement concentrent en effet des enjeux importants en termes de protection des données personnelles. Elles sont nombreuses (données d'achat, financières, contextuelles) et concernent quasiment tous les aspects de l'existence des personnes. Elles sont largement historicisées, peuvent être utilisées pour commettre des fraudes et également, dans certains cas, contenir des informations sensibles au sens du RGPD (par exemple dans le cas d'un don fait à une association politique ou religieuse).

En outre, le choix du moyen de paiement, et en particulier les possibilités de recourir aux espèces, comporte également des enjeux importants d'anonymat et de protection de la vie privée.

Un futur livre blanc sur les données de paiement

La CNIL entend aborder ce sujet de manière graduelle. L'objectif ultime est de parvenir à une entière conformité des différents acteurs concernés aux principes portés par le RGPD (banques et leurs prestataires commerçants, e-commerçants, prestataires de service de paiement) et à une bonne connaissance par les clients des risques et des enjeux du sujet. Cet objectif appelle dans un premier temps à des travaux de doctrine et d'accompagnement, sur le plan national ou européen.

La CNIL publiera en 2021 un **livre blanc sur les données de paiement**. Celui-ci posera des premiers jalons d'analyse économique et juridique, permettra une consultation publique sur des questions de conformité plus précises et définira, une feuille de route d'accompagnement des différents acteurs pour les années à venir.

« Les mesures de confinement et de distanciation sociale imposées à la population, ont fait évoluer les pratiques numériques. »

« Le choix du moyen de paiement [...] comporte également des enjeux importants d'anonymat et de protection de la vie privée. »

Apporter une protection des données au quotidien

Au printemps 2021, la CNIL a publié son 8e cahier Innovation et Prospective consacré à la protection des données des individus au quotidien. Cette publication explore la construction historique du droit autour de la protection des données personnelles, la diversité des pratiques individuelles en la matière, les situations sociales qui déterminent le recours à la CNIL et les étapes préalables à celui-ci.
Enfin, des recommandations sont esquissées afin de développer les leviers collectifs de protection des données personnelles.

> « La protection des données gagne ainsi à être considérée du point de vue de ses publics et doit être interrogée du point de vue plus transversal des inégalités et des hiérarchies sociales. »

Le droit actuel de la protection de la vie privée et des données personnelles est le résultat d'une construction sociohistorique ayant émergé dans le monde occidental, en Europe et aux États-Unis, à partir du XIXe siècle, puis renforcé à partir des années 1960. Élaborés dans des contextes nationaux et des traditions juridiques différentes, ces droits ont pour point commun la place centrale attribuée aux droits de l'individu et au principe d'autodétermination informationnelle. En d'autres termes, l'individu doit être en mesure de contrôler les informations le concernant, de consentir ou de s'opposer à l'usage par autrui de ses informations personnelles.

Cependant, les pratiques numériques sont profondément sociales. Elles sont inscrites dans des rapports de dominations et insérées dans des structures socioéconomiques, qui entravent les capacités effectives des individus à maîtriser pleinement les flux des informations les concernant. La protection des données gagne ainsi à être considérée du point de vue de ses publics et doit être interrogée du point de vue plus transversal des inégalités et des hiérarchies sociales. Tout le monde n'est pas affecté de la même manière, n'a pas accès aux mêmes informations, n'a pas les mêmes ressources ou capacité à gérer ses conséquences. Dans cette perspective, il est souhaitable de porter une attention et un message différent à certaines personnes, certains groupes sociaux, selon leurs vulnérabilités particulières.

Les principales situations problématiques

La CNIL a réalisé une analyse exploratoire des courriers et des plaintes reçus. Cette étude vise à comprendre **ce qui détermine le recours aux droits** et offre un regard sur ce que les individus considèrent comme des atteintes à « l'intégrité contextuelle », c'est-à-dire leur perception des technologies et des pratiques de collecte et de diffusion des informations comme une menace pour leur vie privée. Si les raisons d'agir sont multiples, quatre situations conduisent les individus à se mobiliser fréquemment pour leurs droits auprès de la CNIL :

- quand leur **réputation** est menacée par des informations disponibles en ligne ;
- lorsqu'ils sont victimes **d'intrusion** dans leur sphère privée par de la prospection commerciale ;
- en cas de **surveillance** sur leur lieu de travail ;
- l'inscription dans des **fichiers nationaux** (accidents bancaires, antécédents judiciaires, etc.).

Des recommandations pour les acteurs du numérique

Au-delà de la diversité de ces situations, ces plaintes permettent de voir les chemins du droit empruntés par les individus, un parcours aux multiples obstacles qu'ils doivent surmonter avant de faire valoir leurs droits auprès de la CNIL. Le recours aux droits est le fruit d'un processus incertain, au cours duquel **l'infrastructure de données** doit être rendue visible, l'individu doit se considérer comme une victime du traitement de données ; et doit être dans une situation sociale asymétrique qui l'empêche de résoudre le problème par lui-même.

Ces conditions nécessaires induisent, des inégalités dans le recours aux droits entre les individus.

Tous n'ont, en effet, pas le temps, les connaissances ou les moyens financiers suffisant à consacrer à la protection de leurs données personnelles. Selon les dispositifs matériels d'accès aux droits mis en œuvre par les organismes et les compétences dont sont dotées les individus, les chemins du droit peuvent être longs et complexes.

Au-delà des droits individuels, des leviers collectifs doivent être développés pour protéger la vie privée des individus.

Pour cela, la CNIL entend poursuivre les travaux engagés en interne et avec les milieux de la recherche visant à mieux appréhender les usages numériques quotidiens.

Elle recommande également de :

- rendre visibles les infrastructures de données, c'est-à-dire de rendre davantage transparents le dispositif de collecte de données et les organisations qui y sont attachées ;
- d'encourager le développement et la création de nouveaux corps intermédiaires de la donnée, comme des associations de consommateurs ou des syndicats qui peuvent agréger et représenter les intérêts des personnes en matière de protection des données ;

et

- de produire de la prévention positive des usages numériques, visant à mieux prendre en considération les usages et leurs contextes pour adapter les discours sur les enjeux de la protection des données, au travers notamment d'une meilleure compréhension des imaginaires collectifs et individuels.

Les données, un enjeu environnemental

Dès aujourd'hui et dans les années à venir, le réchauffement climatique et la transition environnementale sont au cœur des défis à relever pour l'humanité.

Dès 2021, le lien entre protection des données et celle de l'environnement fera l'objet de travaux prospectifs du laboratoire d'innovation numérique de la CNIL (LINC).

Les données au centre de toutes les préoccupations

Les données peuvent être considérées comme un « carburant » de l'économie, ce qui nécessite certaines régulations : par le RGPD pour les données personnelles, et par une série de textes en cours de négociation au sein de l'Union européenne sur des thèmes connexes *(Digital Services Act, Digital Markets Act, Digital Governance Act)*. Les données, leur maîtrise et leur circulation sont ainsi au cœur de toutes les préoccupations et génèrent, à plus d'un titre, de l'énergie.

Pourtant, les données n'ont que leur usage de carburant en commun avec le pétrole : elles ne sont donc pas « le pétrole du XIe siècle ». Le pétrole est une énergie fossile dont les ressources sont finies tandis que les données sont des biens duplicables à l'infini : Ce sont leur principale caractéristique. Toutefois, alors que les données sont généralement considérées comme des biens immat riels, et non tangibles, elles n'existent pas sans se reposer sur des infrastructures, des systèmes et des dispositifs qui sont, quant à eux, bien matériels.

Cette considération des données a longtemps eu pour résultat une vision biaisée de leur lien à l'environnement. **Le numérique a d'abord été perçu comme une réponse à la transition énergétique**, notamment dans sa capacité à rendre plus efficient les systèmes productifs, à optimiser l'usage de ressources rares, à éviter les déplacements des personnes ou encore à mesurer et réduire les consommations énergétiques. **Il est aujourd'hui critiqué par certains pour l'ampleur de son empreinte carbone**. Ce secteur industriel s'appuie sur des ressources naturelles, est très consommateur en énergie, produit de la chaleur et des déchets. Son impact sur le climat, de plus en plus questionné, tend à être davantage documenté.

Dès 2006, l'essayiste américain Nicholas Carr estimait que maintenir en vie pendant un an un avatar dans le jeu de

« 53 % des consommations énergétiques du numérique seraient le fait du stockage des données. »

> « Certains principes fondamentaux, tels que la minimisation de la collecte des données et la limitation de la durée de conservation, s'ils n'ont pas cet objectif à l'origine, peuvent contribuer aux objectifs de modération énergétique. »

réalité virtuelle Second Life consommait autant d'énergie qu'un Brésilien moyen sur la même période, soit 1 752 kilowatts. heure[37]. Depuis, de nombreux travaux ont été menés pour réduire la consommation énergétique des *data centers*, voire utiliser l'énergie qu'ils produisent pour chauffer des bâtiments, comme OVH à Lille, ou dans le quartier de la Butte aux Cailles à Paris. L'ADEME (Agence de l'environnement et de la maîtrise de l'énergie) estime cependant que le secteur du numérique est « responsable aujourd'hui de 4 % des émissions mondiales de gaz à effet de serre et la forte augmentation des usages laisse présager un doublement de cette empreinte carbone d'ici 2025 »[38]. Les données ne sont pas stockées dans les nuages, mais sur des serveurs physiques qui doivent être construits et alimentés en énergie. Ils sont parfois très éloignés géographiquement des utilisateurs : une donnée (téléchargement, vidéo, email, requête de recherche…) parcourrait en moyenne 15 000 kilomètres. Ainsi, 53 % des consommations énergétiques du numérique proviennent du stockage des données et des infrastructures leur permettant de circuler (contre 47 % pour les équipements des consommateurs).

Un engagement de la CNIL et des travaux à venir

Fin 2019, la CNIL s'était engagée dans un manifeste commun avec sept autorités administratives indépendantes, à « accompagner l'évolution des acteurs […], éclairer la société qui les interpelle également sur ces enjeux »[39], pour le respect des accords de Paris. Le LINC a choisi en 2021 d'explorer les liens entre la protection des données et l'environnement.

Une lecture du RGPD sous l'angle de la **sobriété numérique** pourrait permettre de proposer des bonnes pratiques. Certains principes fondamentaux, tels que la minimisation de la collecte des données et la limitation de la durée de conservation, s'ils n'ont pas cet objectif à l'origine, peuvent contribuer aux objectifs de modération énergétique. Les paradoxes posés par le développement des blockchains, le mythe du *big data* et ses conséquences sur l'écologie des données, portent en eux des risques comparables aux « marées noires » pétrolières.

En effet, la CNIL constate de plus en plus de fuites de données, permises par la vulnérabilité des systèmes et les possibles conséquences en cas d'erreurs, de défaillances ou encore d'attaques.

La publicité en ligne, par exemple, concentre à elle seule un certain nombre d'enjeux communs avec la protection de l'environnement. La CNIL a publié en 2020 ses recommandations relatives aux cookies, qui concerne un secteur autant consommateur de données que producteur de CO2 : une étude de 2016, publiée dans la revue *Environmental Impact Assessment*[40], estimait que la consommation mondiale de la publicité numérique s'élevait à 106 térawattheures (TWh), 1,5 fois la consommation annuelle d'électricité de la Région Île-de-France pour la même année. La même étude estimait à 60 mégatonnes de CO2 les émissions de la publicité sur Internet. Dans la continuité de cette étude, il serait également utile d'estimer la consommation des usages de l'IA, de la reconnaissance faciale ou des assistants vocaux, par exemple.

Si les études existantes admettent la difficulté à évaluer précisément l'impact environnemental de chaque pratique, il est certain que le développement de dispositifs basés sur la collecte, le traitement et le stockage de données à grande échelle **contribue aux émissions de gaz à effets de serre** en même temps qu'ils ont un impact sur la protection des données et des libertés. Si l'application du RGPD, en limitant la consommation massive de données, a des conséquences positives pour l'environnement, il est également possible de dire que certaines solutions, comme le recours au chiffrement (par ailleurs légitimement encouragé par la CNIL), entraîne un surcoût énergétique. Ces questions et ces liens feront l'objet de travaux prospectifs, de publications et d'expérimentations par le laboratoire d'innovation numérique de la CNIL au cours de l'année 2021.

37 « Avatars consume as much electricity as Brazilians », 5 décembre 2006, roughtype.com
38 « La face cachée du numérique », janvier 2021, ademe.fr
39 « Les autorités publiques et administratives indépendantes développent leur collaboration vis-à-vis des défis posés par le réchauffement climatique », 20 décembre 2019, cnil.fr
40 « Environmental impact assessment of online advertising », novembre 2018, sciencedirect.com

FOCUS

air2021

L'ouverture des données publiques et la question de l'interrégulation

Le cadre juridique de l'*open data* et son articulation avec la réglementation relative à la protection des données personnelles a suscité ces dernières années de nombreuses réflexions de la part des différents acteurs concernés.

À l'échelle de la France, **le rapport de la mission Bothorel sur la politique publique de la donnée, des algorithmes et des codes sources**[41], remis en décembre 2020 au Gouvernement, éclaire la mise en œuvre du principe d'ouverture par défaut et de gratuité des données publiques, en dehors des exceptions prévues par les textes, notamment en matière de protection de la vie privée. Il a rappelé que lorsque celles-ci ne pouvaient pas être ouvertes, les données pouvaient être mises à la disposition de tiers agréés ou partagées entre administrations, à des fins de simplification de la vie quotidienne numérique des citoyens. L'État pourrait, de même, se doter d'un cadre juridique et technique de confiance pour favoriser et accélérer l'accès sécurisé des chercheurs, des innovateurs et des entrepreneurs aux données dont ils ont légitimement besoin dans leurs activités.

À l'échelle de l'Europe, la Commission européenne a dévoilé en novembre dernier sa proposition de **règlement sur la gouvernance européenne des données *(Data Governance Act)***, après avoir procédé à une consultation publique. Ce texte doit non seulement garantir la confiance en fournissant un cadre juridique européen de partage des données mais aussi proposer une base technique, le tout dans l'objectif d'encourager la circulation des données entre entreprises ainsi qu'entre entreprises et administrations publiques. L'articulation de ces propositions de ce règlement avec les dispositions du RGPD et la question de la localisation des données, à la suite de l'invalidation *Privacy Shield* par l'arrêt Schrems II, devraient donner lieu à d'intenses discussions.

La CNIL approfondira ces questions sous leur prisme éthique, du point de vue de l'intérêt général et de la protection des libertés fondamentales des personnes. L'événement aura lieu en fin d'année 2021.

41 Rapport pour une politique publique de la donnée, 23 décembre 2020, gouvernement.fr

Les Ressources

LES RESSOURCES HUMAINES

Dans la continuité des années précédentes, la CNIL a bénéficié de 10 créations de postes en 2020, portant son plafond d'emploi de 215 à 225 afin de faire face à toutes ses missions et aux sollicitations gouvernementales toujours plus nombreuses.

Deux nouvelles fonctions d'expertise ont été créées (juriste référent au service des affaires économiques et ingénieur référent santé au service de l'expertise technologique) ainsi que la nouvelle fonction d'assistant chargé de la coopération européenne au service des plaintes afin d'optimiser l'efficience du traitement des plaintes transfrontalières avec les homologues européens de la CNIL.

Pour renforcer l'appui aux équipes au regard du RGPD, la CNIL a continué à renforcer les métiers traditionnels, notamment ceux issus de la chaîne répressive (auditeur des systèmes d'information, juristes, chargé du développement des outils).

Pour mieux accompagner la croissance de l'équipe et faire face à une activité à fort enjeu, elle a choisi d'étoffer l'encadrement du service des sanctions et du contentieux (adjoint au chef du service). Enfin, au regard du développement de la CNIL, un poste d'ingénieur systèmes, réseaux et sécurité des SI est venu renforcer le service de l'informatique interne.

L'entrée en vigueur du nouveau règlement de gestion, le 1er janvier 2020, permet de rationaliser la gestion des ressources humaines à la CNIL, mais aussi d'augmenter son attractivité, notamment sur des fonctions tournées vers les nouvelles technologies, en offrant des rémunérations et des perspectives de carrière plus intéressantes.

La gestion fine du plafond d'emplois a permis, en utilisant au mieux les marges dégagées par les vacances de postes (dues aux délais de recrutements dans le cadre de créations ou du renouvellement du personnel), d'apporter le maximum de soutien aux directions métiers en leur attribuant des contrats non permanents et en utilisant au mieux les ressources. **Ainsi, le plafond d'emploi a été consommé à hauteur de 99 %.**

Toutefois, la quasi-totalité des missions soit en grande partie réalisable à distance, ainsi que les investissements informatiques récents, ont permis aux agents de poursuivre leur travail sans avoir à recourir aux autorisations spéciales d'absence prévues dans la fonction publique dans ce contexte particulier. De même, les recrutements de nouveaux collaborateurs et leur accueil ont été assurés pendant cette période, ainsi que toutes les opérations relatives à la carrière et la rémunération.

Il est à noter que 29 agents de différentes directions, particulièrement mobilisés en raison de la situation exceptionnelle, ont bénéficié de la « prime COVID », prévue par le décret du 14 mai 2020.

DONNÉES SOCIALES

225 postes fin 2020

59% des agents travaillant à la CNIL sont arrivés entre 2015 et 2020

39 ans Âge moyen

8 ans Ancienneté moyenne

34% des postes occupés par des juristes,

13% par des assistants,

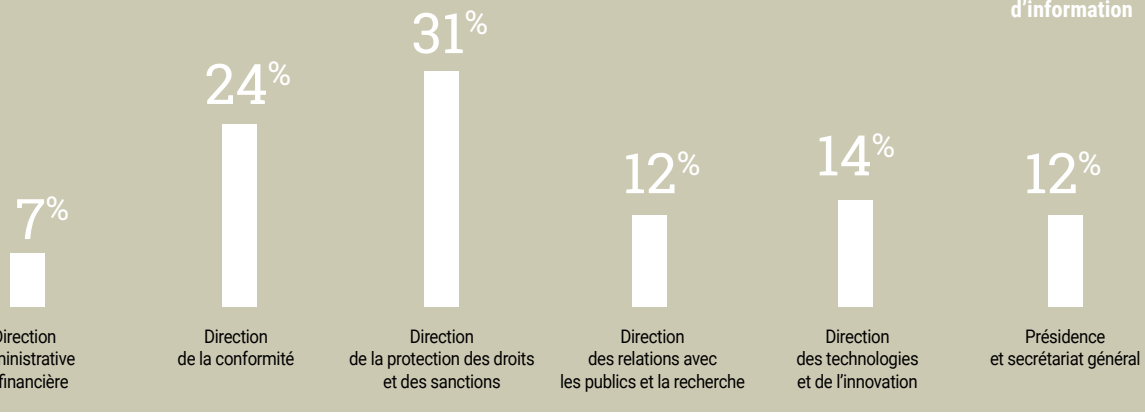
11% par des ingénieurs ou auditeurs des systèmes d'information

238 agents présents au 31/12, y compris non permanents

80% des agents occupent un poste de catégorie A

63% de femmes

37% d'hommes



LES RESSOURCES FINANCIÈRES

En 2020, le budget alloué à la CNIL s'est élevé à 20 143 890 € en autorisations d'engagement (AE) et en crédits de paiement (CP) répartis comme suit :

• **16 710 552 €** pour la masse salariale (titre 2) ;
• **3 433 338 €** pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6).

À l'instar des exercices précédents, la CNIL a poursuivi et accentué ses efforts de maîtrise budgétaire, qui se traduisent par une consommation des dépenses de personnel de 97,4 % et du plafond d'emploi de 99,3 %.

Par ailleurs, une annulation de crédits de titre II est intervenue en fin de gestion sur le programme 308 (protection des droits et des libertés) et a eu des conséquences sur les crédits de la CNIL à hauteur 300 000 €.

Concernant les dépenses de fonctionnement, l'exécution est conforme aux prévisions annoncées, quasiment de 100 %, ce qui confirme une gestion rigoureuse et au plus près des crédits accordés en loi de finance. Il est à préciser que la CNIL a procédé en fin de gestion et sur la demande du responsable du programme 308, à une remontée de crédits de paiement de 100 000 €.

L'exécution au 31 décembre 2020 s'élève ainsi à 3 433 281 € en AE et 3 286 755 € en CP soit une consommation des ressources allouées de 99,99 % en AE et de 98,60 % en CP.

Les réalisations marquantes de 2020 portent sur l'adoption, en raison de la crise sanitaire, d'une nouvelle organisation à distance. Des dépenses supplémentaires, directement et indirectement liées à la crise, sont venues impacter le budget de fonctionnement à hauteur de 100 000 euros.

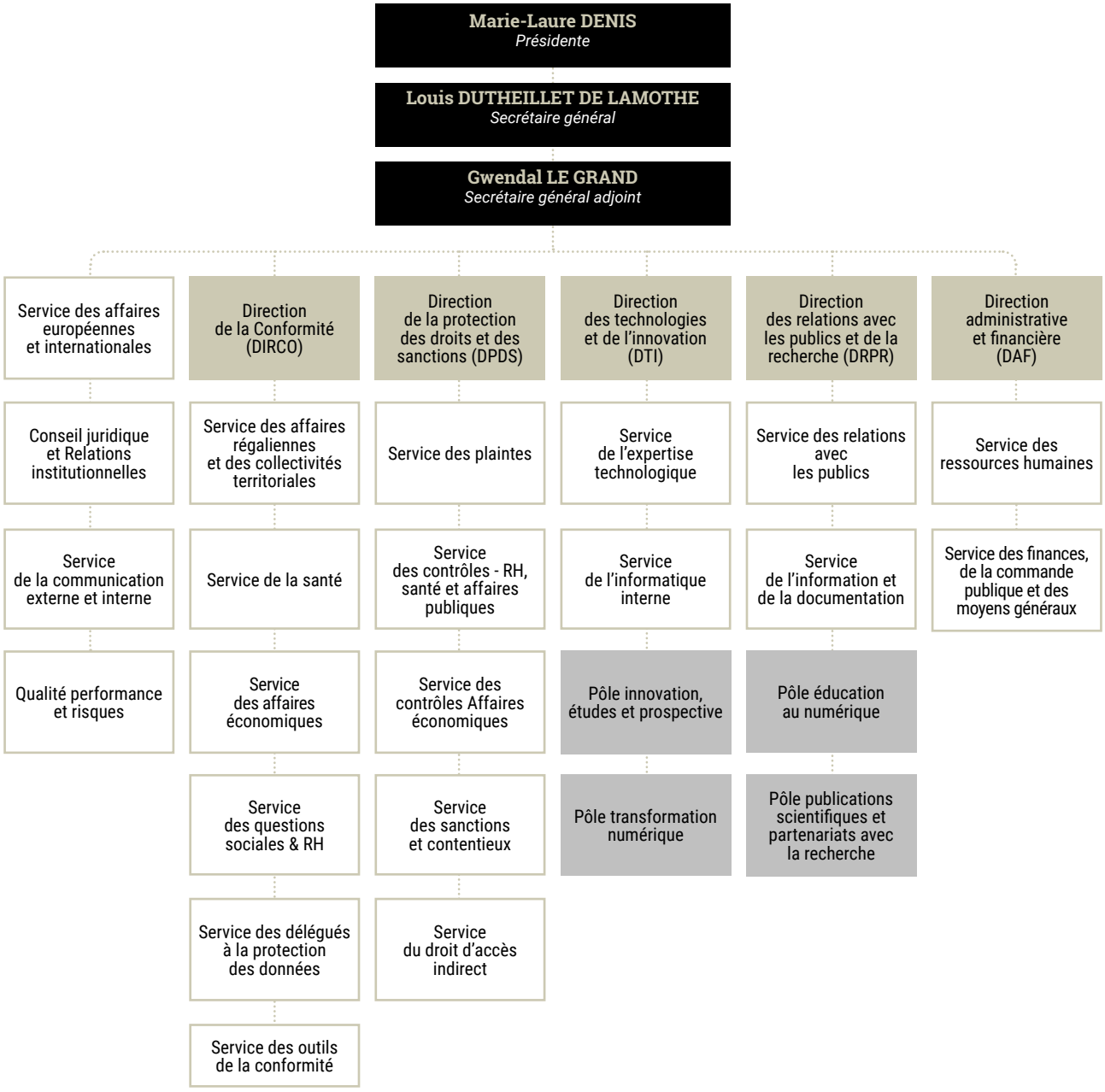
Outre l'achat de produits d'hygiène, permettant aux agents de se protéger du virus, l'organisation du travail en distanciel a accru considérablement le besoin en matériels informatiques et en outils de communication performants et efficaces pour garantir un niveau de productivité optimum. Cela a permis, notamment, de tenir **plus de 20 000 réunions en visioconférence internes**, et de répondre à 24 000 appels téléphoniques et à près de 20 000 requêtes écrites de la part du public en 2020. Certaines dépenses de formation et de missions et déplacements, qui n'ont pas pu être réalisées du fait du contexte sanitaire, compensent cependant les dépenses supplémentaires.

Par ailleurs, la CNIL poursuit ses efforts de réduction des coûts en adhérant, chaque fois que les sujets s'y prêtent, aux prestations mutualisées offertes par la Direction des services administratifs et financiers des services du Premier ministre.

Enfin, la CNIL a accéléré son adhésion aux marchés portés par le Bureau des achats ministériels, ainsi qu'à ceux portés par la Direction des achats de l'État.

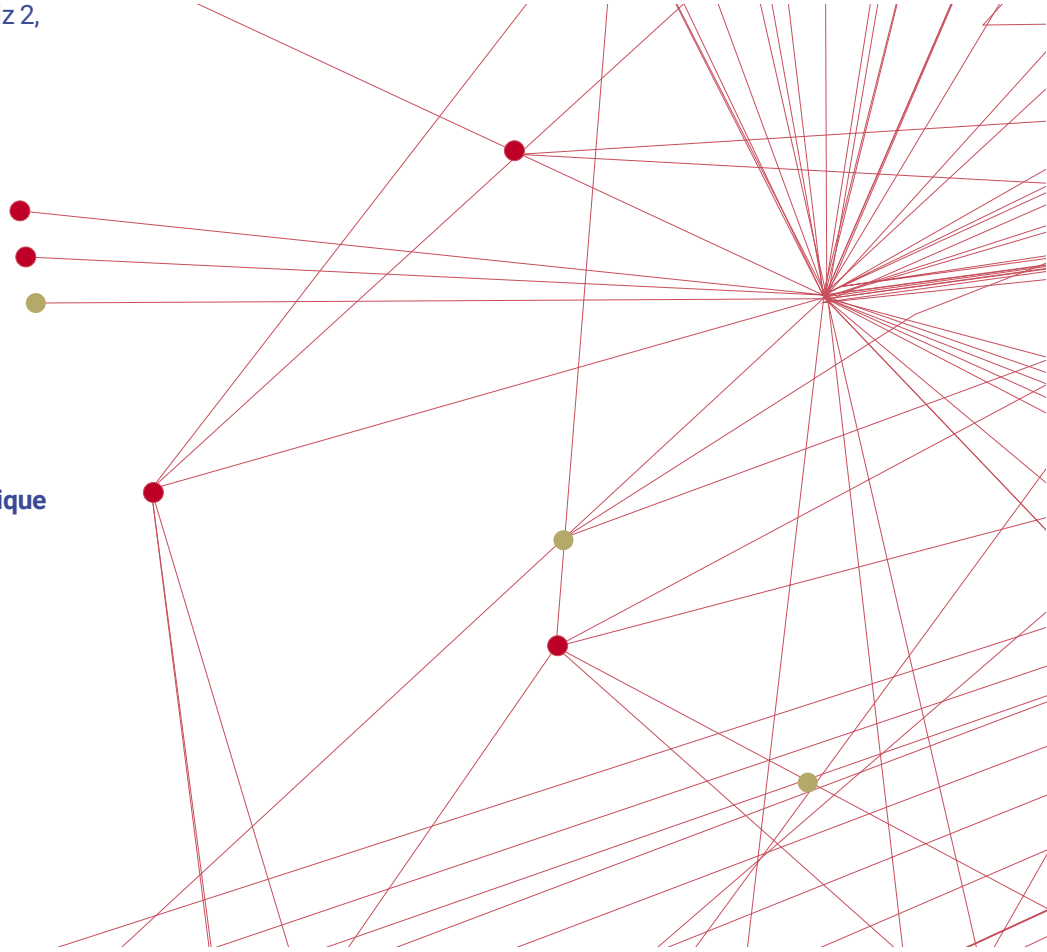
CRÉDITS 2020	Autorisations d'engagement	Crédits de paiement
Budget LFI	**20 423 725**	**20 423 725**
Titre 2	**16 792 515**	**16 792 515**
Hors Titre 2	**3 631 210**	**3 631 210**
Budget disponible	**20 143 890**	**20 143 890**
Titre 2	**16 710 552**	**16 710 552**
Hors Titre 2	**3 433 338**	**3 433 338**
Remontée de Crédits au programme		**-100 000**
Budget consommé	**19 181 771**	**19 035 245**
Titre 2	**15 748 490**	**15 748 490**
Hors Titre 2	**3 433 281**	**3 286 755**

Organigramme des directions et services



Ce visuel est issu du logiciel Cookieviz 2, développé par la CNIL.
Il permet de visualiser et ainsi de mesurer l'impact des cookies lors de sa navigation.

> linc.cnil.fr



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

cnil.fr
educnum.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles