2021

Rapport annuel

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

2021

Rapport annuel

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 - 75334 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

Crédit photos : CNIL, Adobe stock, Juliette Leclercq, Patrick Gaillardin / hanslucas.

Date de publication : Mai 2022

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, le rôle de la Commission nationale de l'informatique et des libertés est de préserver les libertés des citoyens à l'ère du tout-numérique en accompagnant et en contrôlant l'usage des données personnelles contenues dans les fichiers et traitements informatiques ou papier, aussi bien publics que privés.

Le numérique doit être au service des citoyens. Son développement doit garantir l'identité humaine, les droits de l'homme, la vie privée, et les 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.).

SOMMAIRE

Introduction

1 La CNIL en bref

2 Bilan d'activité

3 Perspectives

LES VALEURS DE LA CNIL

INDÉPENDANCE

Autonomie décisionnelle et pouvoir d'agir

Autorité administrative indépendante, la CNIL est composée d'un Collège pluridisciplinaire de 18 membres.

-

La CNIL ne reçoit d'instruction d'aucune autorité.
Les ministères, autorités publiques, dirigeants d'entreprises, publiques ou privées, ne peuvent s'opposer à son action.

-

Elle a le pouvoir d'agir :
le gouvernement doit la consulter avant de mettre en œuvre des fichiers, elle est consultée par les parlementaires, elle traite les plaintes qu'elle reçoit, et a un pouvoir de contrôle et de sanction.

CONVICTION

Engagement, dialogue, sens de l'intérêt général

La CNIL est une institution au service des citoyens.
Elle est à l'écoute des particuliers et des associations de protection de la vie privée, elle assure une veille et est en mesure de s'autosaisir sur des thèmes identifiés comme prioritaires.

-

C'est également un acteur moteur de la souveraineté numérique européenne par une coopération étroite avec ses homologues européens.

-

La CNIL nourrit le débat sur les usages numériques insuffisamment encadrés à ce jour.

EXPERTISE

Compétence, qualité, exigence

La CNIL est l'autorité indépendante référente de la protection des données personnelles des Français depuis plus de 40 ans.

-

Elle est experte des questions juridiques (RGPD, loi Informatique et Libertés) et numériques (sécurité, anticipation, usages, technologies, exploitation et commerce des données) liées à l'usage des données personnelles.

COLLÉGIALITÉ

Collectif, compromis, pluridisciplinarité

L'organisation de la CNIL lui permet d'être réactive et créative

-

Forte de ses partenariats et du réseau des DPO dont elle assure l'animation, **la CNIL est en prise directe avec le terrain** et développe une approche ouverte et pragmatique.

-

La CNIL est une organisation à taille humaine,
conviviale, marquée par une cohésion des équipes très forte.

AVANT-PROPOS DE LA PRÉSIDENTE

Marie-Laure DENIS
Présidente de la CNIL

LE BILAN 2021 DE LA CNIL TÉMOIGNE D'UNE ACTIVITÉ PARTICULIÈREMENT INTENSE, MARQUÉE PAR UNE POLITIQUE D'ACCOMPAGNEMENT RENOUVELÉE, L'ACCROISSEMENT DES MESURES RÉPRESSIVES ET UN RENFORCEMENT DES ACTIONS POUR LA CYBERSÉCURITÉ.

La sollicitation croissante de la CNIL par tous les acteurs de la société, qu'il s'agisse des particuliers, des entreprises, des pouvoirs publics, des associations ou des médias, n'est pas conjoncturelle. La crise sanitaire, qui a continué à mobiliser le Collège et les équipes de la CNIL, a accéléré cette tendance, tout comme l'arrivée à maturité de certaines technologies, reposant notamment sur l'intelligence artificielle. Plus que jamais, **c'est le respect d'un équilibre entre accompagnement de la transformation numérique et protection des droits des personnes qui permettra de relever les défis soulevés par la numérisation de notre environnement quotidien**.

« En 2021, les pratiques non conformes ont été sanctionnées »

En 2021, les efforts de l'institution ont été résolument tournés vers l'accompagnement de l'ensemble des acteurs

La CNIL a adapté ses offres aux enjeux et aux besoins des organismes. Le succès rencontré par notre **premier « bac à sable » consacré aux données de santé**, qui a reçu plus d'une soixantaine de candidatures, est un exemple de cette évolution. Ce dispositif est pérennisé ; **la thématique pour 2022 est celle des outils numériques dans le domaine de l'éducation.**

L'accompagnement des pouvoirs publics a, lui aussi, été intense puisque la CNIL a répondu à **22 auditions parlementaires et rendu 121 avis sur des projets de lois et de décrets**. Elle a par ailleurs traité 576 dossiers d'autorisation en santé au cours de l'année 2021.

En parallèle, la CNIL a mis en œuvre une réponse répressive proportionnée et dissuasive, mobilisée avec discernement envers des acteurs de toutes tailles et tous secteurs confondus.

Notre action relative aux **cookies** en est une illustration. En 2020, nous avions posé un cadre clair, accompagné, et donné du temps à la mise en conformité. En 2021, les pratiques non conformes ont été sanctionnées, afin de garantir que chaque utilisateur de site web soit en mesure d'effectuer un choix réel et éclairé quant à la collecte de ses données en ligne.

Le Conseil d'État a d'ailleurs validé nos importantes amendes en la matière : c'est une étape majeure qui confirme notre compétence à prendre des sanctions sur les cookies en dehors du guichet unique européen.

De manière plus générale, la CNIL a procédé en 2021 à **384 contrôles**. Elle a reçu plus de **14 143 plaintes** et en a **clôturées 12 522**. Elle a par ailleurs reçu plus de **5 000 notifications** de violations de données. Les manquements constatés à l'occasion de certaines des instructions menées ont conduit la CNIL à prononcer **135 mises en demeure et 18 sanctions**, pour un montant cumulé d'amendes historique qui dépasse les **214 millions d'euros**.

Sur le plan européen, la CNIL a également été particulièrement active au sein du Comité européen de la protection des données (CEPD)[1]

Elle a ainsi participé à la rédaction et à l'adoption de toutes les lignes directrices destinées à guider les organismes dans la mise en œuvre du RGPD. À cela s'ajoute une participation active aux différentes décisions prises par nos homologues, notamment **la sanction luxembourgeoise contre Amazon de 746 millions d'euros** à laquelle la CNIL a considérablement contribué en intervenant dans les procédures de contrôle.

La CNIL a également été fortement impliquée dans la nécessaire **construction de la souveraineté numérique européenne au travers de la régulation des flux de données hors de l'Union européenne**. Avec ses homologues, elle s'est attachée à tirer les conséquences de l'arrêt « Schrems II » rendu par la Cour de justice de l'Union européenne en juillet 2020 invalidant le *Privacy Shield*, accord entre l'Union européenne et les États-Unis encadrant auparavant les transferts de données à caractère personnel. Dans le même temps, la CNIL s'est mobilisée aux côtés de l'ANSSI pour le **développement d'offres de services cloud protectrices de nos droits**.

La CNIL n'est donc pas seulement une voix utile au débat public et susceptible d'orienter des évolutions réglementaires ou législatives. Son action est concrète et tangible, en réponse aux défis qui nous attendent. Mais si nous voulons contribuer à renforcer la confiance dans une société et une économie où la donnée joue un rôle de plus en plus central, nous devons, encore et toujours, continuer à nous renouveler.

En 2022, notre action et nos priorités

1 Le CEPD (ou EDPB, de l'anglais *European Data Protection Board*) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données et encourage la coopération entre les autorités de protection des données de l'Union européenne.

En 2022, notre action et nos priorités s'articuleront autour de trois piliers

La CNIL renforcera tout d'abord sa démarche d'ouverture pour gagner en efficience.

Nous devons améliorer l'efficacité de notre **coopération avec nos homologues européens** pour aboutir à des décisions collectives d'envergure concernant les grands acteurs du numérique. La CNIL s'y investit quotidiennement et continuera de le faire avec conviction et détermination pour affirmer davantage la pleine capacité du RGPD à réguler l'écosystème numérique européen et mondial.

Nous renforcerons également nos liens avec les autres AAI, en particulier avec l'Autorité de la concurrence et l'ARCOM (Autorité de Régulation de la Communication Audiovisuelle et Numérique). Il s'agit de multiplier les effets de levier et de **garantir que les individus aient une compréhension claire** de la façon dont leurs données seront utilisées.

Il nous faudra, par ailleurs, continuer à échanger avec les **acteurs de la société civile**, confronter nos analyses à leurs attentes. Ce dialogue permettra de nourrir nos travaux sur l'évolution de nos services en ligne et l'offre de contenus, pour les rendre encore plus adaptés et accessibles à tous.

La CNIL maintiendra son ambition en matière de respect des droits des personnes, qui est aussi une exigence collective.

Nous aurons pour objectif de **rendre encore plus facile l'exercice des droits** pour les personnes et de contraindre plus rapidement les organismes qui manqueraient à leurs obligations. En contrepartie, nous devrons être en mesure d'**apporter des réponses plus adaptées et dans des délais plus courts aux besoins des entreprises, des administrations et des associations**.

Pour ce faire, nous poursuivrons **trois chantiers** engagés l'année dernière. Nous renforcerons la **logique de responsabilisation** et le respect des droits des personnes en réduisant notamment les délais d'instruction des plaintes. Nous améliorerons l'**accompagnement des professionnels**, avec l'évolution de notre service des délégués à la protection des données, qui assurera désormais le déploiement des dispositifs d'accompagnement innovant, dont le « bac à sable » 2022. Enfin, **nous consoliderons notre doctrine et développerons de nouveaux outils**.

Nous continuerons à solliciter tous les leviers d'une **régulation globale** (clarification du cadre juridique, accompagnement, contrôles) à l'instar de celle mise en œuvre lors du plan d'action sur les cookies. Nous l'appliquerons à trois technologies impliquant une utilisation massive de données : **les caméras augmentées, les transferts dans le cloud et les applications des smartphones**. La CNIL s'attachera tout particulièrement au respect des droits des personnes qui constitue pour les responsables de traitement, un enjeu de responsabilité et d'image.

Dans la même logique, en tant qu'acteur majeur de la **cybersécurité**, la CNIL continuera de se mobiliser pour que les entreprises et les administrations aient pleinement conscience que ce sujet est devenu un impératif stratégique. Nous poursuivrons et amplifierons notre coopération avec les autres régulateurs et les parties prenantes concernés pour assurer la cohérence de notre action, comme en témoigne notre récente adhésion au dispositif Cybermalveillance.gouv.fr.

Nous préparerons la transformation de notre institution, à l'aune d'une nouvelle étape de la régulation du numérique.

La CNIL comptera **270 agents à la fin de l'année 2022**. Il nous faudra réfléchir à l'évolution du fonctionnement et des pratiques d'une institution en croissance. Au-delà, **le contexte européen de la régulation du numérique est en plein bouleversement**. La perspective de l'adoption de nouveaux textes (*Data Governance Act*, *Data Act*, *Digital Markets Act*, *Digital Services Act*, règlement IA, règlement *ePrivacy*) pourrait éventuellement aboutir à confier à la CNIL de nouvelles missions pour le contrôle des mesures mises en œuvre. En tout état de cause, il conviendra de veiller à ce que ces textes soient cohérents avec le cadre juridique de la protection des données.

L'émergence permanente de nouvelles technologies et l'omniprésence des traitements de données à caractère personnel dans tous les champs de la vie sont les défis auxquels la CNIL sera encore confrontée en 2022. Le maintien d'un juste équilibre entre accompagnement et contrôle permettra à la CNIL d'y répondre et de favoriser une innovation respectueuse de nos valeurs communes. **Construire une société numérique de confiance aux côtés des citoyens, des entreprises et des administrations, telle est notre ambition.**

LES TEMPS FORTS 2021

Janvier

25/01 > Collectivités territoriales : la CNIL et l'association Déclic signent une convention de partenariat

Février

03/02 > La CNIL rend son avis sur la proposition de loi « sécurité globale »

15/02 > Lancement du premier « bac à sable » RGPD dans le domaine de la santé

18/02 > Reconnaissance faciale et interdiction commerciale de stade : la CNIL adresse un avertissement à un club sportif

Mars

04/03 > Fuite de données de santé : pour la première fois, le tribunal judiciaire de Paris demande le blocage d'un site web

Mai

12/05 > Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement : la CNIL publie ses avis

Juin

03/06 > Premier code de conduite européen pour les services de cloud

07/06 > La CNIL rend son avis sur la mise en œuvre du passe sanitaire

18/06 > Règlementation de l'IA : l'avis de la CNIL et de ses homologues

Juillet

16/07 > L'homologue luxembourgeois de la CNIL prononce une amende de 746 millions d'euros à l'encontre d'Amazon

20/07 > Sanction de 1,75 million d'euros à l'encontre d'AG2R LA MONDIALE

21/07 > La CNIL publie sa position sur l'extension du recours obligatoire au passe sanitaire

26/07 > Lobbying : sanction de 400 000 euros contre Monsanto

27/07 > Cookies : sanction de 50 000 euros à l'encontre de la Société du Figaro

Septembre

07 et 08/09 > Premier G7 des autorités de protection des données

24/09 > Fichier automatisé des empreintes digitales : la CNIL rappelle à l'ordre le ministère de l'Intérieur

Octobre

04/10 > La CNIL met en demeure Francetest pour sécurisation insuffisante des données de santé

06/10 > La CNIL publie un nouveau Livre blanc sur les données et moyens de paiement

18/10 > *Global Privacy and Data Protection Awards 2021 :* la CNIL récompensée pour son logiciel et les analyses de CookieViz 2.0

29/10 > Fichiers d'évaluation des agents : la CNIL prononce une sanction de 400 000 euros à l'encontre de la RATP

Novembre

08/11 > Évènement air2021 : entre partage et protection, quelle éthique pour l'ouverture des données ?

18/11 > Les pratiques de la plateforme Vinted contrôlées par des autorités de protection des données européennes

26/11 > La CNIL et le ministère de l'Éducation nationale, de la Jeunesse et des Sports renouvellent leur partenariat

26/11 > Reconnaissance faciale : la CNIL met en demeure CLEARVIEW AI de cesser la réutilisation de photographies accessibles sur internet

Décembre

14/12 > Refuser les cookies doit être aussi simple qu'accepter : la CNIL poursuit son action et adresse de nouvelles mises en demeure

23/12 > Caméra-piéton et vidéoprotection : la présidente de la CNIL met en demeure une commune

31/12 > Cookies : la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à hauteur de 60 millions d'euros pour non-respect de la loi

La CNIL en bref

LES CHIFFRES CLÉS 2021

CONSEILLER & RÉGLEMENTER

22 AUDITIONS PARLEMENTAIRES

13 QUESTIONNAIRES ADRESSÉS AU PARLEMENT OU À UN PARLEMENTAIRE EN MISSION

154 DÉLIBÉRATIONS DONT **121** AVIS SUR DES PROJETS DE TEXTE

576 DOSSIERS D'AUTORISATION EN SANTÉ TRAITÉS DONT **54** AUTORISATIONS DE RECHERCHE SUR LA COVID-19

ACCOMPAGNER LA CONFORMITÉ

81 393 ORGANISMES ONT DÉSIGNÉ UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

28 810 DPO DÉSIGNÉS

+13% PAR RAPPORT À 2020

123 882 COMPTES CRÉÉS SUR LE MOOC[1] ATELIER RGPD[2]

5 037 NOTIFICATIONS DE VIOLATIONS DE DONNÉES **+79%**

PROTÉGER

14 143 PLAINTES QUI ONT CONDUIT À

5 848 RÉPONSES RAPIDES

8 295 ÉTUDES PLUS APPROFONDIES

12 522 PLAINTES CLÔTURÉES

5 329 DEMANDES VALABLES DE DROIT D'ACCÈS INDIRECT (DAI)

3 960 VÉRIFICATIONS EFFECTUÉES

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

INFORMER

161 475 APPELS REÇUS **+33%**

16 898 REQUÊTES REÇUES PAR VOIE ÉLECTRONIQUE

10 809 884 VISITES SUR LES SITES WEB DE LA CNIL **+12%**

130 800 *FOLLOWERS* SUR TWITTER **+5%**

43 724 FANS SUR FACEBOOK **+17%**

153 732 ABONNÉS SUR LINKEDIN **+16%**

CONTRÔLER & SANCTIONNER

384 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT

118 CONTRÔLES SUR PLACE

65 CONTRÔLES SUR PIÈCE

173 CONTRÔLES EN LIGNE

28 CONTRÔLES SUR AUDITION

135 MISES EN DEMEURE DONT 2 PUBLIQUES

45 RAPPELS À L'ORDRE DE LA PRÉSIDENTE

18 SANCTIONS DONT

15 AMENDES

POUR UN MONTANT CUMULÉ DE

214 106 000 EUROS

DONT 5 ASSOCIÉES À DES INJONCTIONS SOUS ASTREINTE

2 RAPPELS À L'ORDRE DE LA FORMATION RESTREINTE AVEC INJONCTIONS

1 LIQUIDATION D'ASTREINTE

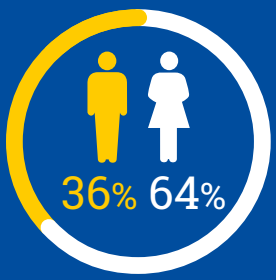
+17 projets de sanctions européens examinés par la CNIL

RESSOURCES HUMAINES

BUDGET

21,8

MILLIONS D'EUROS



245 emplois

39 ans

Âge moyen

81% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A

59% D'AGENTS ARRIVÉS ENTRE 2016 ET 2021

8 ANS

ANCIENNETÉ MOYENNE DES AGENTS DE LA CNIL

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

5 PERSONNALITÉS QUALIFIÉES

4 PARLEMENTAIRES

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

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

La CNIL peut être saisie par différents acteurs publics sur des projets de textes tels que des décrets ou des lois avant leur adoption
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. Elle conseille tout particulièrement le gouvernement, qui doit obligatoirement demander son avis pour certains projets.

EN 2021, LA CNIL A RENDU 121 AVIS SUR DES PROJETS DE TEXTE.

L'objectif de l'avis

L'avis rendu par la CNIL :

- a pour objectif **d'éclairer le gouvernement ou le Parlement** ;
- **peut entraîner des modifications**, que ce soit pour tenir compte des observations formulées par la CNIL, ou de l'examen ultérieur du texte par exemple par le Conseil d'État ou le Conseil constitutionnel.

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

Les textes concernés

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

Concrètement, il peut s'agir :
- de propositions de loi (à l'initiative du Parlement) ;
- de projets de loi ou d'ordonnance (à l'initiative du gouvernement) ;
- de projets de décret ou d'arrêté (gouvernement).

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.

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

Secteur : Intérieur

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)

Philippe-Pierre CABOURDIN

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

Secteurs : Banque - Assurance - Fiscalité

LES MEMBRES ÉLUS DE LA FORMATION RESTREINTE

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

Claude CASTELLUCCIA

Directeur de recherche à l'Inria Grenoble

Secteurs : Administration numérique - Communications électroniques et technologies innovantes – Recherche - Statistiques

Anne DEBET

Professeur des universités

Secteurs : Données publiques - Partage de données - Nouveaux outils de conformité

Alain DRU

Membre du Conseil économique, social et environnemental

Secteurs : Environnement - Énergie - Transport

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 - Immobilier

Loïc HERVÉ
Sénateur de la Haute-Savoie

Secteurs : Travail et ressources humaines

Isabelle LATOURNARIE-WILLEMS
Conseillère maître à la Cour des comptes

Secteur : Défense

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

Secteurs : Travail et ressources humaines

Bertrand DU MARAIS
Conseiller d'État

Secteurs : Plateformes en ligne (réseaux sociaux) et moteurs de recherche – Questions interrégulation, 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)

Aminata NIAKATÉ
Avocate, membre du Conseil économique, social et environnemental

Secteur : Vie politique et citoyenne – Sport – Médias - Culture

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

Secteurs : Santé - Assurance maladie – Recherche médicale

Sylvie ROBERT
Sénatrice d'Ille-et-Vilaine

Secteurs : Éducation et enseignement supérieur (hors sujets recherche)

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

L'ORGANISATION DE LA CNIL

Organigramme des directions et services

LES DIRECTIONS DE LA CNIL

Louis DUTHEILLET DE LAMOTHE
Secrétaire général

LE SECRÉTARIAT GÉNÉRAL

« Le secrétariat général **coordonne et encadre les activités des cinq directions de la CNIL.** Il organise également **le fonctionnement du Collège et de la formation restreinte.** Plusieurs équipes lui sont directement rattachées : le service des affaires européennes et internationales, le service de la communication externe et interne, la mission « Qualité, performance, risques » et le pôle Conseil juridique et relations institutionnelles. »

Thomas DAUTIEU
Directeur de la conformité

LA DIRECTION DE LA CONFORMITÉ

« La direction de la conformité a pour mission **d'accompagner les acteurs publics et privés dans leur démarche de mise en conformité** au regard du RGPD et de la loi Informatique et Libertés. Cet accompagnement peut être individuel, ou général et sectoriel. Il se fait grâce à la production de « droit souple » (référentiels, lignes directrices, recommandations, etc.), parfois en coopération avec nos homologues européens. Il repose aussi sur des outils innovants comme le MOOC RGPD, le **« bac à sable »** et des fiches pratiques disponibles sur le site web de la CNIL. La direction instruit également l'ensemble des **demandes d'avis** adressés par le gouvernement, et a en charge la gestion des séances plénières du Collège. Pour mener ces activités, elle est composée de quatre services sectoriels, de deux services dédiés aux acteurs et outils de la conformité et d'un pôle d'assistantes chargées d'assurer la préparation et le suivi des décisions adoptées en séance plénière. »

Karin KIEFER
Directrice de la protection des droits et des sanctions

LA DIRECTION DE LA PROTECTION DES DROITS ET DES SANCTIONS

« La direction de la protection des droits et des sanctions est chargée du **contrôle de la conformité des traitements de données personnelles.** Elle a pour mission d'instruire les **plaintes de personnes souhaitant exercer leurs droits** ou dénonçant une pratique non conforme. Elle procède également aux contrôles des traitements de données personnelles mis en œuvre par des organismes publics et privés et est en charge des **mesures correctrices prises par la CNIL** (amendes, mises en demeure…). Enfin, la direction traite le contentieux de la CNIL et répond aux demandes d'avis des autorités judiciaires. Sur le plan européen, les équipes **coopèrent avec nos homologues dans le cadre du guichet unique,** par exemple sur des projets de sanction concernant des fichiers transfrontaliers. Pour réaliser ces missions, elle s'appuie sur deux services en charge de l'exercice des droits et des plaintes, deux services des contrôles et un service des sanctions et du contentieux. »

LES DIRECTIONS DE LA CNIL

Bertrand PAILHÈS
Directeur des technologies
et de l'innovation

LA DIRECTION DES TECHNOLOGIES ET DE L'INNOVATION

« La direction des technologies et de l'innovation a pour principale mission de mettre **l'expertise technologique et informatique** de la CNIL à la disposition de l'ensemble des services et de **partager les enjeux d'innovation et de prospective en interne comme en externe.** Elle se compose du service de l'expertise technologique, du service de l'informatique interne, du laboratoire d'innovation numérique de la CNIL (LINC) et du pôle transformation numérique. Ses travaux doivent permettre **d'appréhender les nouvelles technologies**, leurs **enjeux en matière de protection de la vie privée** et les **bonnes pratiques à appliquer**. Pour ce faire, les équipes de la direction créent des outils à destination des entreprises et des usagers, en collaboration avec les autres services de la CNIL. Nous menons aussi des expérimentations et publions des articles et des études. La direction est également chargée de la gestion des notifications de violations de données personnelles adressées à la CNIL. »

Sophie VULLIET-TAVERNIER
Directrice des relations
avec les publics et la recherche

LA DIRECTION DES RELATIONS AVEC LES PUBLICS ET LA RECHERCHE

« **La direction renseigne et conseille les différents publics** qui sollicitent la CNIL au quotidien (particuliers, entreprises, collectivités locales, associations…). Elle comprend notamment le service des relations avec les publics qui est le point d'entrée des **nombreux appels, courriels et courriers qui nous sont adressés chaque jour.** Elle assure également la **gestion et la valorisation de la doctrine et des publications de la CNIL,** tant au niveau interne qu'au niveau externe. Par ailleurs, elle promeut, via la mise en place d'actions et de ressources pédagogiques, **une éducation citoyenne du numérique**. Enfin, elle suit **les partenariats de la CNIL** avec les acteurs concernés, notamment avec le monde de la recherche. »

Jean-MARC SALMON
Directeur administratif et financier

LA DIRECTION ADMINISTRATIVE ET FINANCIÈRE

« La direction administrative et financière de la CNIL comporte deux services : le service des ressources humaines et le service des finances, de la commande publique et des moyens généraux. Le premier assure les recrutements en lien avec les directions, la gestion des emplois, des carrières et de la formation. Il garantit également le **bon fonctionnement des instances de concertation et des relations sociales au sein de l'institution.** Le second élabore et met en œuvre le budget de la CNIL en assurant le suivi de son exécution. Il veille au **respect des règles de la commande publique pour l'ensemble des achats de la CNIL** et gère l'ensemble des activités visant au bon fonctionnement des services : courrier, reprographie, gestion des fournitures et du mobilier, relations avec l'exploitant du bâtiment Ségur-Fontenoy. »

LES RESSOURCES HUMAINES

En 2021, la CNIL a bénéficié de 20 créations de postes, portant son plafond d'emplois de 225 à 245 ETP, afin de faire face à toutes ses nouvelles missions et aux sollicitations gouvernementales toujours plus nombreuses.

L'accent a surtout été porté sur la chaine répressive (9 créations à la Direction de la protection des droits et des sanctions) ainsi que sur les postes d'encadrement de proximité en raison de l'étoffement des services (création de 6 postes d'adjoint au chef de service).

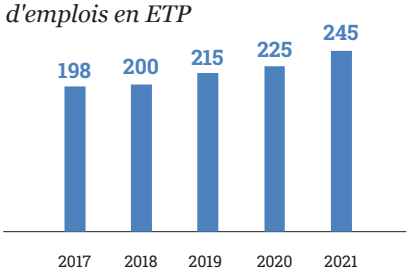
En utilisant au mieux les marges dégagées par les vacances de poste dues aux délais de recrutements pour les créations ou au renouvellement naturel du personnel, le plafond d'emplois a été consommé à plus de 99 %. Cette gestion fine des ressources a permis d'apporter le maximum de soutien aux directions métiers en leur attribuant des contrats non permanents.

Après l'entrée en vigueur du nouveau règlement de gestion, au 1er janvier 2020, qui ouvrait des rémunérations et des perspectives de carrière plus intéressantes, un effort a été fait en 2021 sur la partie indemnitaire, avec une revalorisation sensible des primes de performance.

Si la crise sanitaire a continué à produire ses effets sur l'organisation du travail, la CNIL a néanmoins pu poursuivre l'accomplissement de ses missions de manière quasi-normale grâce à l'investissement de l'ensemble des agents et aux outils mis à disposition.

En outre, grâce à l'expérience du télétravail classique acquise depuis 2017, renforcée par le télétravail généralisé dû à la pandémie, la CNIL peut désormais attribuer jusqu'à 2 jours en moyenne de télétravail par semaine aux agents, contre 1 jour dans l'ancien dispositif.

Évolution du plafond d'emplois en ETP



DONNÉES SOCIALES

245
postes fin 2021

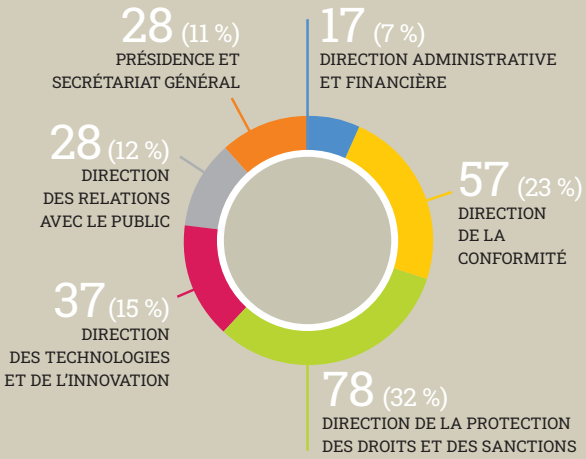
59%
des agents travaillant à la CNIL sont arrivés entre 2016 et 2021

81%
des agents occupent un poste de catégorie A

39 ans
Âge moyen

7 ans et 8 mois
Ancienneté moyenne

Répartition des postes par direction



Les métiers de la CNIL

33%
des postes sont occupés par des juristes

12%
par des assistants

11%
par des ingénieurs ou auditeurs des systèmes d'information

LES RESSOURCES FINANCIÈRES

LE BUDGET DE LA CNIL

En 2021, le budget alloué à la CNIL s'est élevé à **21 780 782 €** en autorisations d'engagement (AE) et **21 510 782 €** en crédits de paiement (CP) répartis comme suit :

- **18 017 267 €** pour la masse salariale (titre 2)
- **3 763 515 €** en AE et **3 493 515 €** en CP 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 personnels de 96 % et du plafond d'emplois de 99 %. 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 150 000 €.

Concernant les dépenses de fonctionnement, l'exécution est conforme aux prévisions annoncées, ce qui confirme une gestion rigoureuse et au plus près des crédits accordés en loi de finance.

L'exécution au 31 décembre 2021 s'élève ainsi à 3 763 479 € en AE et 3 468 080 € en CP, soit une consommation des ressources allouées de 100 % en AE et de 99,3 % en CP.

LES RÉALISATIONS MARQUANTES DE L'ANNÉE

L'adaptation au nouveau cadre normatif issu du RGPD et de la directive police justice a nécessité que la CNIL renforce les actions de formation à destination de ses agents et modernise son SI.

L'amélioration du schéma directeur des systèmes d'information : celle-ci s'est notamment traduite par la mise en œuvre des interopérabilités avec le système d'information commun des autorités de protection des données et le développement de l'infrastructure serveurs, afin de prendre en compte les augmentations de flux générés par le RGPD. La CNIL a également développé de nouveaux téléservices (désignation de l'autorité « chef de file », outil de notification de failles de sécurité, réalisation d'études d'impacts – PIA etc.), pour répondre aux exigences du règlement européen.

Le développement de ses actions de conseil et d'expertise de haut niveau sur les matières technologiques et juridiques : ce point constitue un enjeu primordial pour l'autorité, ses avis sur des projets de texte pouvant avoir un impact important tant au niveau sociétal que médiatique.

La création de nouveaux outils ou nouveaux contenus : pour répondre aux sollicitations du grand public, des professionnels, dont les délégués à la protection des données. Ainsi, face à son succès, le MOOC de la CNIL mis en ligne en janvier 2019 a dû faire l'objet d'une actualisation technique et graphique de grande ampleur en 2021.

La modernisation des outils de son infrastructure informatique : la CNIL s'est dotée de nouveaux serveurs et de licences informatiques innovantes et performantes. L'émergence de nouveaux téléservices, une politique de certification ambitieuse et l'interopérabilité essentielle du SI de la CNIL avec le système d'information des autorités européennes de protection ont eu pour conséquence l'augmentation des budgets informatiques. Par ailleurs, la CNIL a continué le développement de ses systèmes pour améliorer la relation avec l'usager et rendre ses outils encore plus efficaces, pour répondre au mieux à l'augmentation considérable des sollicitations.

La CNIL a également poursuivi ses efforts permanents de réduction et d'optimisation des coûts de fonctionnement en adhérant à l'ensemble des prestations mutualisées offertes par la Direction des Services Administratifs et Financiers des services du Premier ministre (marchés de soutien, gestion des déplacements et missions professionnelles, maintenance des véhicules, action sociale, arbre de Noël…).

Enfin, la mise en place de nouvelles procédures logistiques a permis aux agents des moyens généraux d'optimiser leurs missions et de réaliser plus de 900 interventions (hors présidence et reprographie) pour soutenir et moderniser l'activité de la CNIL, et cela en assurant une permanence quotidienne malgré la crise sanitaire.

18 017 267 €
pour la masse salariale

3 763 515 €
en autorisations d'engagement (AE)

3 493 515 €
pour les dépenses de fonctionnement, d'investissement et d'intervention

Budget opérationnel de programme 2021	Autorisations d'engagement	Crédits de paiement
Total budget PLF - crédits demandés	**21 839 016**	**21 839 016**
PLF Titre 2	18 107 806	18 107 806
PLF Hors Titre 2	3 731 210	3 731 210
Amendement	**- 18 694**	**- 18 694**
Total budget LFI - crédits votés	**21 820 322**	**21 820 322**
LFI Titre 2	18 107 806	18 107 806
LFI Hors Titre 2	3 712 516	3 712 516
Réserve précaution T2	- 90 539	- 90 539
Réserve précaution HT2	- 148 501	- 148 501
Gel et Sur-Gel de crédits HT2	- 74 250	- 74 250
Crédits complémentaires	273 750	3 750
Total budget ouvert	**21 780 782**	**21 510 782**
Budget T2	18 017 267	18 017 267
Budget Hors Titre 2	3 763 515	3 493 515
Total remontées de crédits au SPM	**150 000**	**150 000**
Budget T2	150 000	150 000
Budget Hors Titre 2	-	-
Total budget ouvert après remontées de crédit	**21 630 782**	**21 360 782**
Budget T2	17 867 267	17 867 267
Budget Hors Titre 2	3 763 515	3 493 515
Total budget consommé	**21 097 711**	**20 802 312**
Budget T2	17 334 232	17 334 232
Budget Hors Titre 2	3 763 479	3 468 080
Solde	**533 071**	**558 470**
Budget T2	533 035	533 035
Budget Hors Titre 2	36	25 435
% de consommation / budget ouvert global	97 %	97 %
% de consommation / budget ouvert T2	96 %	96 %
% de consommation / budget ouvert HT2	100 %	99 %
Postes	**245**	**-**
Plafond d'emplois en ETPT	235	-
Création de postes	20	-

L'environnement de la CNIL

Le Parlement européen et le Conseil de l'UE votent les lois de l'Union européenne. Le premier regroupe les députés européens, tandis que le second rassemble les ministres des États membres.

La Commission européenne propose des lois au Parlement et au Conseil de l'Union européenne. Elle veille également à leur application sur tout le territoire.

Règlement général sur la protection des données (2016)

Directive Police-Justice (2016)

Directive *ePrivacy* (2002 - modifiée en 2009)

Autres textes

Rend des avis

edpb

European Data Protection Board

Coopèrent

Les autorités de protection des données de l'Union européenne sont réunies au sein du Comité européen de la protection des données (EDPB en anglais). Celui-ci veille notamment à la cohérence des pratiques et des sanctions des autorités.

Adapté dans le droit national

Loi Informatique et Libertés (modifiée)

CNIL.

Contrôle les décisions

Prononce des avis

Participe à des auditions

Décrets, arrêtés, projets de lois, etc.

Propositions de lois

CONSEIL D'ÉTAT

Le Conseil d'État est la plus haute juridiction administrative française. Il peut juger la légalité de projets de décrets du gouvernement et peut confirmer ou invalider une délibération de la CNIL.

GOUVERNEMENT
Liberté
Égalité
Fraternité

ASSEMBLÉE NATIONALE

SÉNAT

La protection des données dans les grandes lignes

La CNIL entretient des liens étroits avec un grand nombre d'entités publiques françaises et européennes, dont certaines sont représentées ici.

Toutes ces relations, qu'il s'agisse d'échanges ou d'avis prévus par des lois, 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.

À cette carte peuvent 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 ».

La Cour de justice de l'Union européenne veille à l'uniformité de l'interprétation du droit européen sur tout le territoire. Ses jugements peuvent s'appliquer à tous les États membres.

Peut contrôler les décisions

CVRIA

Union européenne

France

Participe ou contribue

Accompagne et conseille

Contrôle et sanctionne

Anticipe et innove

Informe et protège

- **Organismes** (entreprises, associations, établissements publics, etc.)
- **État et collectivités territoriales**
- **Recherche publique**
- **Société civile et citoyens**

Monde

Autorités de protection

Autres instances

ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES

OECD

GPA
Global Privacy Assembly

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Bilan d'activité

LE MOT DU SECRÉTAIRE GÉNÉRAL ET DU SECRÉTAIRE GÉNÉRAL ADJOINT

Cette année encore, la crise sanitaire a pesé sur l'activité de la CNIL mais d'une moindre manière : l'expérience acquise l'année précédente, la mise en place d'outils et de procédures de travail à distance, ainsi que l'implication constante de son Collège et de ses agents ont permis à la CNIL de continuer à offrir un service public de qualité. Le retour à un mode de fonctionnement « presque » normal a permis de mener des travaux visant à rendre notre institution encore plus efficace, accessible et attractive.

Ainsi, l'année 2021 a été marquée par la conduite de plusieurs chantiers internes mais dont les effets doivent être ressentis à l'extérieur, tant par les particuliers que les gestionnaires de fichiers. Les actions entreprises ont essentiellement conduit à repenser notre organisation et nos outils, ainsi qu'à travailler à rendre le RGPD plus compréhensible et plus prévisible.
Ces mesures s'inscrivent dans une démarche d'amélioration continue de nos pratiques et se poursuivront en 2022.

Repenser notre organisation pour mieux répondre aux attentes du public

Une partie des adaptations menées par la CNIL en 2021 visent à mieux servir trois types de publics : les plaignants, les DPO et les organismes qu'ils représentent ainsi que les communautés scientifique et d'innovation.

Tout d'abord, c'est l'organisation des services dédiés à la gestion des plaintes qui a été modifiée avec un double objectif : **raccourcir les délais d'instruction et mieux suivre les procédures impliquant des investigations ou une coopération avec nos homologues européens.** En effet, avec un délai moyen de traitement des plaintes de cinq mois (recouvrant des situations très variées), le maintien d'un flux important de saisines (plus de 14 000) et une grande variété de manquements invoqués (illicéité du traitement, non-respect des droits, manquement à la sécurité), la nécessité de repenser nos schémas s'est imposée. En pratique, deux principales mesures ont été prises. La première a consisté à créer deux services distincts en charge de l'instruction des saisines : un service dédié aux réclamations et demandes de droit d'accès indirect pouvant faire l'objet d'une gestion rapide, dans des délais allant de quelques jours à deux mois ; un autre focalisé sur les dossiers nécessitant plusieurs échanges avec les parties (organisme mis en cause et plaignant). La seconde mesure a été de décider d'expérimenter le recours à un prestataire externe pour les plaintes les plus répétitives et simples. Nous ferons le bilan de ces changements début 2023.

Ensuite, la CNIL a prolongé la rénovation de sa stratégie d'accompagnement. Le lancement en 2021 d'un « bac à sable » offrant un accompagnement renforcé à des organismes du secteur de la santé après un processus d'appel à candidatures en est une manifestation. Une autre en est la création d'un nouveau « service de l'accompagnement et des délégués à la protection des données ». Concrètement, nous avons décidé de transformer le service des délégués à la protection des données existant en lui allouant quatre postes supplémentaires et en enrichissant la palette de ses moyens d'action. Ce nouveau service gardera son ADN. Il continuera à répondre aux questions des DPO,

à animer cette communauté et à diffuser des outils généraux d'aide à la conformité (MOOC, guide sur le DPO, etc.). Par ailleurs, il organisera désormais des déplacements en régions pour promouvoir le RGPD et il prendra en charge le dispositif de « bac à sable » annuel tout en gérant une nouvelle offre de service. Sur ce point, il s'agira d'accompagner pendant 18 à 24 mois des responsables de traitements sélectionnés car présentant un fort potentiel numérique et économique.

Nous avons également décidé de restructurer l'activité du Laboratoire d'innovation numérique de la CNIL, le LINC, pour en faire un service à part entière. Créé au début des années 2010, le LINC était un projet porté par un pôle de trois agents chargés de mettre en avant les activités d'innovation de la CNIL. En 2021, deux nouveaux postes ont été alloués à cette activité. **Désormais, en plus de mener et partager des réflexions sur les tendances émergentes d'usage du numérique et de conduire de projets d'expérimentation autour des données, le LINC développe des outils innovants pour les autres services de la CNIL (volet accompagnement et volet répressif) et renforce sa production de travaux et publications scientifiques.** L'action du laboratoire s'inscrira donc dans la continuité des travaux déjà menés mais doit aussi permettre d'outiller le régulateur et d'assurer une veille proactive sur tous les sujets d'innovations numériques.

Enfin, toujours dans cette recherche des moyens d'améliorer le service à l'usager, **l'année 2021 a également été celle du constat que notre réussite repose, pour partie, sur l'amélioration de nos outils :** ceux proposés aux professionnels et particuliers, mais aussi ceux utilisés par les agents de la CNIL dans l'accomplissement de leurs missions. Pour ne citer que quelques-unes des nombreuses réalisations de l'année, un nouvel outil de gestion de la relation usager (Publik) a été testé avec succès et va permettre de revoir nos téléservices, notamment en matière de plaintes et de droit d'accès indirect ; l'intranet de la CNIL a été entièrement rénové, au terme d'un travail considérable de plusieurs services de la CNIL ; notre outil de statistiques a été rénové pour piloter plus finement nos flux de saisines. Pour finir, l'adoption d'un nouveau schéma directeur des systèmes d'information permet de capitaliser sur ces progrès et de continuer à améliorer sensiblement nos outils de traitements de dossiers durant les trois années à venir.

Modifier et clarifier la norme pour gagner en efficacité

Parallèlement à ces mesures d'ordre organisationnel, l'année 2021 a aussi été consacrée au **maintien d'un juste équilibre entre accompagnement et mise en œuvre d'une politique répressive dissuasive.**

Nous nous sommes ainsi impliqués dans la réforme de la procédure de sanction prévue par la loi Informatique et Libertés pour en fluidifier et simplifier le déroulé. En effet, après trois ans de pratique du RGPD, la procédure s'est avérée partiellement inadaptée. Elle ne permettait d'adopter qu'un nombre limité de mesures, alors que nous recevons de plus en plus de plaintes, de signalements de violation ou d'alertes sur des mauvaises pratiques. **La nouvelle procédure répond à ce besoin car elle permet de distinguer les dossiers selon leur complexité et leur gravité.** Dorénavant, les dossiers à plus faibles enjeux ou plus simples, mais justifiant une saisine de la formation restreinte, pourront être traités selon une procédure simplifiée. En pratique, ce type de dossier pourra faire l'objet d'une décision par le seul président de la formation restreinte de la CNIL. Ce dernier pourra alors prononcer dans des délais plus resserrés des amendes d'un montant maximal de 20 000 euros et des astreintes de 100 euros par jour maximum. **Il s'agit d'un changement profond, dont la pleine appropriation nécessitera probablement plusieurs années**.

Si l'amélioration du processus répressif est essentielle pour assurer la crédibilité de l'action de la CNIL, elle doit s'accompagner d'une plus grande prévisibilité et accessibilité de la norme, notamment de la doctrine de la CNIL. Pour répondre à ce besoin nous avons mobilisé trois leviers.

La CNIL s'est tout d'abord dotée à la fin de l'année 2021, de « Tables informatique et libertés ». Elles ont vocation à compiler dans un seul document, ordonné par un plan de classement retraçant l'ensemble de la matière, un ensemble de cours résumés doctrinaux des prises de position des juridictions ou de la CNIL sur des points de principe. Cet outil de travail, inspiré des tables de jurisprudence utilisées par la plupart des grandes juridictions, doit permettre d'assurer une transmission de la connaissance et une cohérence dans l'application de la norme. Ces tables doctrinales seront complétées en 2022 et auront vocation à être anonymisées pour être mises à disposition du public.

Nous avons par ailleurs lancé un chantier de **simplification de la rédaction des avis de la CNIL** (près d'une centaine par an). Malgré la complexité des sujets, il s'agit de veiller encore davantage à ce que le texte des avis soit compréhensible par le plus grand nombre (ministère nous ayant saisis, Parlement, journalistes, citoyens intéressés, etc.), tout en conservant les qualités juridiques et techniques ainsi que les messages éthiques.

Enfin, nous nous sommes attachés à **enrichir nos contenus sur nos sites internet** (cnil.fr, linc.cnil.fr, design.cnil.fr), y compris en anglais. En 2021 ce sont plus de 130 actualités et communiqués qui ont été publiés venant ainsi enrichir les 10 000 pages déjà en ligne. Nous avons aussi fait attention à la variété de ces contenus afin de nous adresser à tous nos publics. Ont notamment été mis à disposition des guides pratiques (guide pour accompagner les associations), des recommandations (recommandation mots de passe), des conseils à destination du grand public (5 conseils pour protéger ma vie privée sur les réseaux sociaux). Nous avons également ouvert plusieurs consultations publiques pour impliquer les professionnels et la société civile dans la production de notre doctrine (guide recrutement). **Toutes ces actions ont mené à des seuils inédits de fréquentation de notre outil « Besoin d'aide » et de nos sites (10,8 millions de visiteurs).** Plus que jamais, rendre le RGPD prévisible et accessible à tous, du grand public éloigné de la technicité de la loi informatique et libertés à un public de juristes et d'ingénieurs spécialisés, qui tous viennent chercher après de nous des réponses à leurs légitimes interrogations, reste un défi.

En regardant dans le rétroviseur les accomplissements de la CNIL en 2021, nous constatons que notre institution a franchi un nouveau cap. Elle a su surmonter la surcharge provoquée par la crise sanitaire mais surtout adapter son fonctionnement et ses stratégies aux enjeux du RGPD. Les trois années à venir seront maintenant celles où ces réformes devront progressivement déployer leurs effets.

SENSIBILISER
et 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 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.

Flora,
Cheffe du service de la communication externe et interne, Secrétariat général

Le service de la communication externe et interne se compose d'un chef de service et de six agents aux profils et compétences complémentaires, chargés des relations médias, de l'édition, du webmastering, du community management, de la veille, de la réalisation de contenus multimédias, de l'évènementiel et de la communication interne. Notre rôle est de mettre en œuvre la politique et les projets de communication dans le cadre de la stratégie globale de la CNIL. L'équipe, qui doit être créative, réactive et pédagogue, travaille en étroite collaboration avec les cinq directions de l'institution.

Plus concrètement, nos missions peuvent se résumer ainsi : informer et sensibiliser, apporter des conseils pratiques, promouvoir et accompagner. À ce titre, nous concevons et réalisons tous les outils de communication numériques et papier en nous assurant de la qualité et de la cohérence des formes et contenus. Nous avons d'ailleurs produit, en 2021, deux documents de référence pour renforcer notre identité et gagner en lisibilité : une plateforme de marque et une nouvelle charte éditoriale.

Les enjeux liés à la protection des libertés et de la vie privée étant au cœur des débats à l'ère du tout-numérique, la CNIL est naturellement de plus en plus exposée et les attentes de nos publics de plus en plus fortes. En témoignent les centaines de demandes presse qui nous sont adressées chaque année ainsi que la croissance constante de nos nombres d'abonnés sur les réseaux sociaux et la fréquentation de notre site web.

LE SITE DE LA CNIL ET LES RÉSEAUX SOCIAUX

10,8 millions
de visites en 2021 sur les sites de la CNIL (cnil.fr, linc.cnil.fr, educnum.fr)

+ 12 % par rapport à 2020

129
actualités et communiqués publiés

480
contributions aux 8 consultations publiques

Près de 4 500
retombées presse

Plus de 600
demandes presse

Des visites record en 2021 sur les sites web

Avec près de 11 millions de visites en 2021, les sites web de la CNIL (cnil.fr, linc.cnil.fr et educnum.fr) constituent à ce jour les supports de communication les plus efficaces pour s'adresser à un large public. Le site cnil.fr permet, en particulier, d'accompagner les professionnels au travers de guides et de nombreuses ressources pratiques, de rappeler au grand public ses droits, ou des conseils pour répondre à des irritants du quotidien (appels non sollicités, vidéosurveillance au travail…) ainsi que d'informer sur les actions répressives de la CNIL.

En 2021, la CNIL a ainsi publié plus de 220 nouveaux contenus. Une attention particulière a été portée à la traduction et à la mise à disposition de contenus sur la version anglaise du site web, notamment concernant l'action répressive. Ce travail se poursuivra en 2022 avec la traduction de documents d'accompagnement pour les professionnels comme le guide pratique à destination des DPO.

Une offre particulièrement riche pour les professionnels

En 2020, les contenus les plus plébiscités concernaient majoritairement la crise sanitaire[4]. En 2021, les internautes privilégient de nouveau des contenus relatifs soit, pour les professionnels, à leurs obligations (cookies et autres traceurs, guide pour les TPE/PME, etc.), soit, pour les particuliers, à des outils pratiques du quotidien ou à leurs droits (générer un mot de passe solide, faire le ménage dans son historique de navigation). Pour autant, **le communiqué de presse le plus consulté en 2021 reste lié à la COVID-19**[5] avec plus de 40 000 vues.

FOCUS

Une communication plus accessible sur la protection des données

La CNIL propose une offre riche et variée pour s'adresser tant aux débutants qu'aux professionnels les plus expérimentés.

Afin d'assurer la qualité et la lisibilité de l'ensemble de ses contenus, la CNIL a décidé de créer un glossaire des termes complexes ou à éviter, appliqué à ses publications à destination du grand public dès la fin de l'année 2021 et mis à disposition du public début 2022.

Elle encourage les professionnels du droit et du numérique à privilégier eux-mêmes des termes simplifiés, dès que possible, pour communiquer de façon plus claire et permettre à tous de comprendre les concepts juridiques et techniques autour de la protection des données.

Extrait du glossaire

Termes juridiques	Termes simplifiés à utiliser
Décret n° 2019-536 du 29 mai 2019 [...]	Décret d'application de la loi Informatique et Libertés
Dispositions	Règles, principes
Dispose (loi)	Prévoit, indique, interdit, autorise, etc.
Le cas échéant	Si c'est le cas, dans ce cas, etc.

4 « Coronavirus (COVID-19) » sur cnil.fr
5 « La CNIL rappelle les principes à respecter pour diffuser aux médecins la liste de leurs patients non vaccinés » sur cnil.fr

Top 3 des fiches pour les particuliers les plus lues	
Cookies : les outils pour les maîtriser	392 559
Générer un mot de passe solide	294 867
Faites régulièrement le ménage dans l'historique de navigation	247 965

Top 3 des fiches pour les professionnels les plus lues	
Cookies et traceurs : que dit la loi ?	409 025
RGPD : de quoi parle-t-on ?	218 021
RGPD : par où commencer ?	165 897

Top 3 des communiqués les plus lus	
La CNIL rappelle les principes à respecter pour diffuser aux médecins la liste de leurs patients non vaccinés	43 902
Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir	37 393
La CNIL rend son avis sur le projet de passe sanitaire pour l'accès aux grands rassemblements de personnes	30 228

À eux seuls, les contenus sur les cookies et autres traceurs totalisent près de 1,4 million de vues uniques, en particulier pour les fiches pratiques (« Que dit la loi ? », « Comment mettre mon site web en conformité ? »). Les mises en demeure et les sanctions de la CNIL sur le sujet ont également été très suivies, reprises et commentées sur les réseaux sociaux et dans la presse.

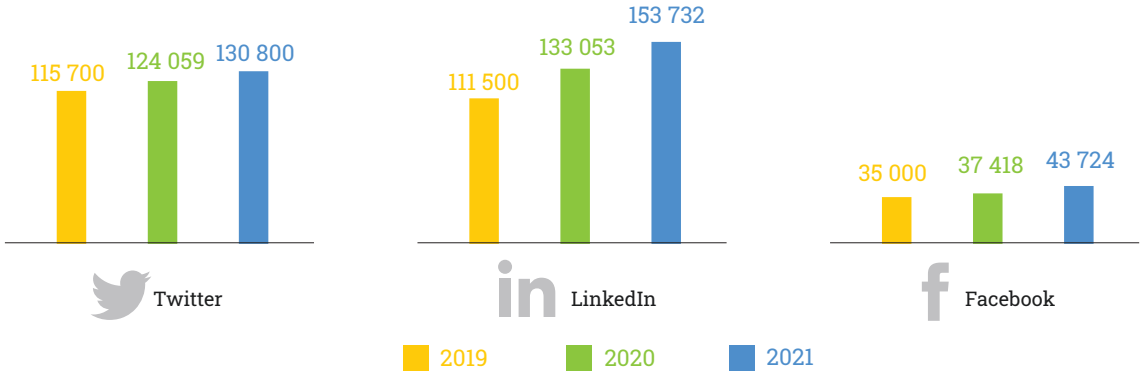
Compte tenu de la grande variété des sujets abordés et afin d'améliorer l'accessibilité de ses contenus, la CNIL proposera en 2022 une refonte de l'arborescence de l'espace professionnel de son site web. Elle offrira notamment une entrée en matière plus claire pour comprendre le RGPD et accéder aux outils.

Des conseils pratiques pour accompagner le grand public dans son quotidien numérique

L'information et la sensibilisation du grand public sont au cœur des préoccupations de la CNIL. Cela se traduit notamment par la mise à disposition 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. En 2021, la CNIL a également créé une rubrique dédiée aux outils numériques et aux conseils pour naviguer sur le web[6].

La CNIL sur les réseaux sociaux

En cohérence avec l'attractivité du site cnil.fr, le nombre d'abonnés de la CNIL sur les réseaux sociaux est en augmentation constante au fil des années.
En 2021, la CNIL compte + 5.4 % d'abonnés sur Twitter, + 15.5 % sur LinkedIn et près de 17 % d'abonnés supplémentaires pour Facebook, ce qui démontre un intérêt croissant des particuliers pour la protection de leurs données.



6 « Configurer ses outils » sur cnil.fr

FOCUS

De nouveaux formats pour informer et sensibiliser

En 2021, de nouvelles vidéos pédagogiques ont été produites par la CNIL afin d'accompagner ses publications sur cnil.fr et les réseaux sociaux. Courtes, dynamiques, elles visent le grand public et apportent des conseils pratiques pour protéger ses données personnelles et sa vie privée.

La CNIL, c'est quoi ?

Qu'est-ce qu'une donnée personnelle ?

LinkedIn s'inscrit comme le réseau privilégié des délégués à la protection des données, en témoigne le succès de la publication du guide pratique RGPD du DPO[7] qui a enregistré un record d'interactions.

Comme en 2020, les sujets qui ont suscité le plus d'engagement en 2021 sont les sujets liés à la COVID-19, (passe sanitaire, vaccination). Les sujets du quotidien numérique, comme les cookies, la cybersécurité et les bons conseils ont également généré des interactions auprès des particuliers.

Les alertes sur les différentes violations de données ou les arnaques au RGPD sont également massivement relayées. En outre, les sanctions et mises en demeure publiques prononcées par la CNIL, par exemple celles concernant Monsanto ou encore Clearview en fin d'année, suscitent toujours autant l'intérêt des internautes et génèrent beaucoup de conversations, tous réseaux confondus. Pour communiquer sur son action répressive, la CNIL a davantage développé la création d'infographies en 2021. Elles permettent de résumer, en quelques points, l'essentiel des délibérations de la CNIL, et sont très appréciées des abonnés.

La campagne des « Histoires vécues » qui a vu le jour en 2021 et qui relate des situations réelles de plaignants concernant la protection des données est un format prisé des internautes qui s'identifient facilement et n'hésitent pas à partager leurs propres expériences.

LES RÉPONSES AU PUBLIC

Des informations et conseils pour les particuliers et professionnels

La CNIL répond à des questions de plus en plus nombreuses, et de tout ordre, par téléphone, courrier électronique ou par voie postale.

Quatre jours par semaine, la CNIL **informe** et **conseille les particuliers** ainsi que les **professionnels** sur leurs droits et obligations, lors de permanences téléphoniques dédiées.

Le public peut aussi, à tout moment, poser des questions sur les services en ligne du site de la CNIL (Besoin d'aide) ou par courrier postal.

En 2021, la CNIL a ainsi reçu **161 475 appels, soit 33 % de plus** que l'année précédente, malgré la crise sanitaire et la fermeture partielle des permanences téléphoniques durant les confinements. **33 329 appels** ont été traités par les différentes permanences juridiques (+ 39 %).

Avec **16 898** demandes d'information et de conseil reçues, l'année 2021 marque en revanche une baisse **de 17 %** du nombre de ces demandes par rapport à l'année 2020, caractérisée par un record de demandes écrites. Ces demandes sont principalement adressées par les canaux électroniques (85 % par le formulaire « Nous contacter » via « Besoin d'aide ») et en majorité par les particuliers (74 %).

7 Pour en savoir plus sur ce guide, voir « Le premier guide pour les questions sur le DPO » page 82

> BESOIN D'AIDE

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

- les cookies et autres traceurs, les démarches à accomplir pour demander un déréférencement des moteurs de recherche, pour exercer ses droits auprès des sites web ;
- l'utilisation des données des salariés par les employeurs (en particulier la vidéosurveillance et la géolocalisation au travail) ;
- les données traitées par le secteur bancaire, en particulier les collectes relatives à la lutte contre le blanchiment et le financement du terrorisme, les démarches à accomplir pour accéder à FICOBA et les questions relatives au fichage bancaire ;
- les recueils de données effectués dans le cadre de la lutte contre la COVID et les garanties prises pour assurer leur confidentialité.

Un public de plus en plus conscient de ses droits

Les personnes ont de plus en plus conscience de leurs droits : cette tendance, déjà relevée en 2019 et en 2020, se caractérise également par une plus grande volonté de les exercer (49 % des demandes sont liées à l'exercice d'un droit).

161 475

appels reçus au standard téléphonique 01 53 73 22 22

1 555 264

consultations de la rubrique Besoin d'aide

33 329

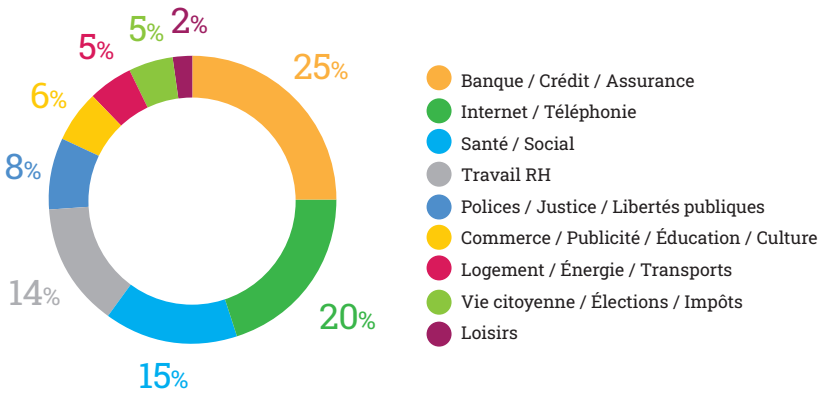
appels répondus par les permanences juridiques de la CNIL

16 898

demandes d'information et de conseil reçues

Elles manifestent également le besoin d'être accompagnées dans leurs démarches, par exemple pour obtenir l'effacement de données ou la suppression de leur compte auprès des réseaux sociaux.

Les requêtes traitées par la CNIL (par thème)



L'ÉDUCATION AU NUMÉRIQUE

Les outils numériques sont une source constante d'opportunités pour les jeunes internautes. Ils contribuent à leur éducation, à leur accès à l'information et aux loisirs, et leur permettent d'entretenir et de développer leurs relations. Mais les mineurs peuvent aussi s'y trouver exposés au cyberharcèlement, à des contenus choquants ou inappropriés, ainsi qu'à une collecte massive d'informations (identité, habitudes de vie, préférences…) en vue de les partager et les réutiliser. Or, si les mineurs sont sensibles à la protection de leur vie privée et de leur image en ligne, ils restent peu conscients des risques liés à la « marchandisation » de leurs données et aux procédés de captation de leur attention.

Afin de protéger et accompagner les plus jeunes dans leur vie numérique, la CNIL a poursuivi en 2021 ses travaux sur les droits numériques des mineurs, en concertation avec l'ensemble des parties prenantes. Elle a ainsi publié huit recommandations pour renforcer la protection des enfants en ligne (page 38).

Droits numériques des enfants : les recommandations de la CNIL

Les 8 recommandations à destination des mineurs pour protéger leurs données et leur vie privée sont le fruit de travaux menés sur le terrain : réalisation d'un sondage auprès de jeunes et de parents, organisation d'une série d'ateliers pour recueillir leur perception de la vie privée et de la protection des données, et lancement d'une consultation publique qui a rencontré un grand succès (plus de 700 contributions).

Les recommandations de la CNIL[8] ont pour objet :

- de clarifier le cadre juridique de l'exercice des droits numériques ;
- d'apporter des conseils pratiques et accompagner les différents acteurs (les mineurs, leurs parents, les acteurs du numérique, les pouvoirs publics).

8 « La CNIL publie huit recommandations pour renforcer la protection des mineurs en ligne », 9 juin 2021, cnil.fr

Elles visent à mettre en place un environnement numérique qui réponde tant au désir d'autonomie qu'au besoin de protection des mineurs.

Ces recommandations constituent un point d'étape dans les travaux de la CNIL. En effet, certaines d'entre elles doivent faire l'objet d'une concertation avec les acteurs concernés, **afin de les rendre techniquement opérationnelles et de proposer des conseils pratiques et des ressources pédagogiques adaptées**.

INFOSPLUS

La difficulté à exercer ses droits en chiffres

75 %
des 11-18 ans affirment trouver « difficile » d'obtenir la suppression d'un contenu les concernant qui a été publié par une autre personne.

35 %
ont cherché à supprimer leur compte sur un réseau social.

58 %
d'entre eux n'ont pas réussi à le faire.

Source : Enquête Génération numérique « les pratiques numériques des jeunes de 11 à 18 ans », mars 2021.

La CNIL attentive à la parole des enfants

À la veille de la Journée internationale des droits de l'enfant, qui s'est tenue le 20 novembre 2021, la présidente et les équipes de la CNIL se sont rendues dans une classe de CM2 à l'école primaire Jean-Louis Barrault de Bois-d'Arcy (78). Les élèves ont répondu à des questions sur le numérique et la protection des données personnelles dans un format ludique, avec l'aide de leur enseignante, puis ont pu découvrir plusieurs ressources pédagogiques produites par la CNIL.

Cette année, la CNIL a également multiplié les formations de formateurs pour toucher les publics jeunes, en s'appuyant notamment sur les Jeunes Ambassadeurs des droits de l'enfant, les animateurs de Génération Numérique et des clubs de football dans le cadre de l'opération Open football club.

Les actions partenariales, un levier pour toucher les plus jeunes

À l'occasion du salon Educatec-Educatice, le ministère de l'Éducation nationale, de la Jeunesse et des Sports et la CNIL ont renouvelé leur convention de partenariat afin de poursuivre leurs actions de sensibilisation à la protection des données personnelles dans les usages numériques de l'éducation. Les actions communes seront poursuivies et renforcées afin de sensibiliser les élèves, les familles et les enseignants, à une utilisation responsable du numérique.

Lors de cet évènement, une table-ronde réunissant la CNIL, le CSA, le Défenseur des droits et la Hadopi a également permis de valoriser le « kit du citoyen numérique »[9] réalisé par les quatre institutions et de présenter leurs principales actions de sensibilisation et d'éducation au numérique.

FOCUS

Repenser l'information pour les jeunes utilisateurs

En 2021, La CNIL a animé, avec l'appui d'une agence de *legal design*, une série d'ateliers impliquant des jeunes de différentes tranches d'âge, afin de repenser les interfaces sous l'angle de leurs droits.[10]

Ces travaux ont permis **d'élaborer des exemples de prototype d'interfaces**, allant du parcours d'inscription sur une plateforme au paramétrage de la géolocalisation, en passant par la gestion des données.

Les études de cas co-produites avec les participants de ces ateliers permettent **de montrer des façons de mettre en œuvre les concepts clés du RGPD** en fonction de divers cas d'usage.

9 « La CNIL, le CSA, le Défenseur des droits et l'Hadopi créent le kit pédagogique du citoyen numérique », 18 janvier 2021
10 « Les études de cas », design.cnil.fr

Les 8 recommandations de la CNIL pour renforcer la protection des mineurs en ligne

1 Encadrer la capacité d'agir des mineurs en ligne

Le RGPD permet aux mineurs, à partir d'un certain âge, de donner en toute autonomie leur accord à certaines utilisations de leurs données dans le cadre de services en ligne. La loi française a retenu l'âge de 15 ans.
Cela suppose que ces services :
- informent sur les utilisations envisagées des données et sur les droits des mineurs, de façon adaptée à leur âge ;
- facilitent l'exercice de leurs droits par les enfants et leurs parents.

2 Encourager les mineurs à exercer leurs droits

Face aux problèmes de cyberviolence, de cyberharcèlement ou d'exploitation de leur image en ligne, il est essentiel que les mineurs puissent exercer facilement leurs droits sur leurs données sur les réseaux sociaux et les plateformes de jeux ou de partage d'images et/ou de vidéos. Cette capacité d'agir de manière autonome n'exclut pas la possibilité pour les parents d'exercer les droits au nom de leur enfant ou de les accompagner dans cette démarche.

3 Accompagner les parents dans l'éducation au numérique

Constatant la fréquente méconnaissance des parents des règles de protection des droits des mineurs en ligne, la CNIL souhaite les accompagner dans l'éducation au numérique de leurs enfants, en collaboration avec ses partenaires, notamment institutionnels et associatifs, réunis au sein du collectif Educnum.

4 Rechercher le consentement d'un parent pour les mineurs de moins de 15 ans

L'utilisation de services en ligne nécessite l'accord conjoint d'au moins un titulaire de l'autorité parentale et de l'enfant concerné lorsque ce dernier a moins de 15 ans (l'accord de l'autre parent étant présumé). Cela peut concerner des fonctionnalités comme la géolocalisation ou le profilage. L'accord de l'enfant est à prendre en compte en fonction de son niveau de maturité.

15 ans

C'est l'âge à partir duquel les mineurs peuvent consentir seuls à certaines utilisations de leurs données en France. Exemple : s'inscrire à un réseau social ou à un site de jeux en ligne.

Retrouvez toutes les recommandations sur cnil.fr[11]

5 Promouvoir des outils de contrôle parental respectueux de la vie privée et de l'intérêt de l'enfant

Les outils de contrôle parental doivent être conformes aux règles de la protection des données. Ceci implique qu'ils tiennent compte de l'intérêt de l'enfant, en évitant tout système excessivement intrusif (par exemple une géolocalisation permanente), en informant clairement le mineur sur les modalités du contrôle parental et en empêchant d'autres personnes ou organismes d'avoir accès aux données des mineurs. Ces outils devraient être évalués en concertation avec les acteurs publics concernés et leur évaluation devrait être mise à la disposition des parents.

6 Renforcer l'information et les droits des mineurs par le design

L'information fournie par les services en ligne doit être claire. Elle devrait s'effectuer au moyen d'une présentation de leur politique de confidentialité, de conditions générales d'utilisation des services (CGU) et d'interfaces claires, simples, attractives et adaptées à l'âge de leurs utilisateurs mineurs.

Cet objectif devrait conduire à exclure le recours à des techniques de manipulation et de design trompeurs (*dark patterns*). De plus, des outils simples de paramétrage des mesures de confidentialité et la désactivation par défaut des options les plus intrusives devraient être prévues.

7 Vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée

Les systèmes de vérification de l'âge et de l'accord parental devraient être réservés aux seuls applications et sites qui le justifient. Cette mise en place devrait se faire en fonction des objectifs des sites, des données collectées et des risques. Il est également nécessaire de tenir compte des technologies disponibles sur le marché, de leur robustesse et de leur simplicité d'usage et d'éviter le recours à un système de reconnaissance faciale, qui serait disproportionné.
La CNIL encourage la mise en place de systèmes fondés sur l'intervention d'un tiers de confiance assurant un contrôle préalable de l'identité et de la qualité des personnes concernées (l'attribution de l'autorité parentale).

8 Prévoir des garanties spécifiques pour protéger l'intérêt de l'enfant

Enfin, la CNIL recommande aux plateformes et services en ligne utilisés par des mineurs de mettre en place à leur intention des mesures de protection spécifiques telles que :
- un paramétrage de confidentialité renforcée par défaut ;
- la désactivation par défaut des systèmes de création de profils, qui risqueraient d'influencer leurs choix et leurs intérêts ;
- la non-réutilisation et la non-transmission à des tiers de leurs données personnelles à des fins commerciales ou publicitaires, à moins d'être en mesure de démontrer leur intérêt au regard de l'intérêt supérieur de l'enfant.

11 « Les droits numériques des mineurs », cnil.fr

La parole à Céline MICHEL,

Enseignante à l'école primaire
Jean-Louis Barrault de Bois-d'Arcy

Aviez-vous déjà abordé le sujet de la protection des données personnelles avec vos élèves ?

C'est un sujet que j'aborde chaque année, notamment dans le cadre de la convention internationale des droits de l'enfant mais aussi en lien avec le programme de géographie « communiquer avec internet ». Chaque enfant passe d'ailleurs le « permis internet ».
À l'ère numérique, l'éducation à un usage citoyen, responsable et éthique des nouvelles technologies constitue une priorité d'action, tout particulièrement dans notre école où les élèves reçoivent une tablette individuelle en début d'année. Ils n'ont pas toujours conscience qu'ils ne peuvent pas utiliser l'application photo ou enregistrer sans l'autorisation préalable de la personne, même si c'est un camarade. Cela nécessite un véritable accompagnement.

Comment, selon vous, mieux les sensibiliser ?

En CM2, ils ne sont qu'au début de leur parcours qui donnera lieu à l'obtention d'une certification, à la fin du cycle 4 (5e, 4e, 3e) et au cycle terminal du lycée.
Mais ces premières années sont essentielles et cette sensibilisation a lieu principalement en classe. La majorité utilise déjà internet, les applications de réseaux sociaux.
Il faut donc partir de leur quotidien, avec souvent déjà de mauvaises pratiques ou représentations, et utiliser les nombreuses ressources existantes et de qualité.
Les affiches de la CNIL[12], les activités ludiques comme les Incowebs ou la BD « les As du web[13] » sont autant de supports à disposition. Les enseignants de cycle 3 (CM1, CM2) ont donc un rôle primordial. Il faut aussi qu'ils soient davantage eux-mêmes accompagnés dans l'usage du numérique.

Citation d'un élève de la classe
« On pensait que si on supprimait ça ne laissait pas de trace, mais en fait si ! »

Quel bilan faites-vous de la visite de la CNIL dans votre classe ?

Votre visite est un évènement dont les élèves de ma classe sont très fiers. Très vite, ils ont souhaité partager cette expérience et ce qu'ils avaient appris. Ils ont donc proposé de transmettre à leur tour le message auprès des autres classes. Ils ont pris conscience de l'existence certes d'un organisme qui était là pour protéger leurs droits dans notre quotidien, mais qu'ils étaient surtout les premiers acteurs de cette protection. En tant qu'enseignante, j'ai constaté que cette visite a généré un intérêt plus fort que les années précédentes.
La rencontre avec un intervenant extérieur est toujours plus marquante pour les élèves.
C'est une expérience à renouveler, de nombreux élèves ont déjà de bonnes bases pour naviguer dans ce monde numérique.

12 « 10 conseils de la CNIL pour rester net sur le web » (PDF, 531 ko), 7 mars 2016, cnil.fr
13 « Les As du web (PDF, 4,1 Mo), » securitytuesday.com

PROTÉGER
les citoyens

Lorsqu'elle reçoit une plainte, la CNIL échange généralement avec le responsable du fichier concerné sur les faits soulevés par le plaignant. En cas de manquement, elle lui demande de se mettre en conformité et de respecter les droits des personnes.

Viktorija,
Juriste, service de l'exercice des droits et des plaintes, Direction de la protection des droits et des sanctions

Depuis l'entrée en application du RGPD, nous ressentons, dans les plaintes que nous recevons, une implication grandissante de nos concitoyens pour le respect de leurs droits.

Cette prise de conscience globale des enjeux liés à la protection des données se manifeste par des plaintes qui vont soit concerner des difficultés dans l'exercice individuel des droits, soit alerter sur un comportement non conforme et un traitement de données illicite.

Plus concrètement, étant en charge des secteurs Banque/Régalien/Libertés Publiques, mon intervention peut par exemple permettre à un plaignant d'obtenir l'accès à ses données auprès d'un organisme bancaire et ainsi s'assurer que seules les données nécessaires sont traitées, d'obtenir l'effacement de ses données personnelles d'un article de presse publié en ligne ou encore lui permettre de ne plus être contacté par un candidat ou parti politique dans le cadre d'une campagne de communication.

Pour les dossiers concernant plusieurs plaignants ou pouvant avoir un impact sur un nombre important de personnes, je travaille très souvent en collaboration avec d'autres services de la CNIL : le service de l'expertise technique pour être appuyée sur des aspects techniques des plaintes, les services des contrôles pour proposer des missions de vérification et y participer ou encore le service des sanctions si une mesure correctrice s'avère nécessaire.

Porter ces dossiers, souvent au cœur de sujets d'actualité, me permet de contribuer, au même titre que les citoyens qui nous ont saisis, à cette prise de conscience sur la protection des données dans notre monde numérique.

UN NOMBRE DE PLAINTES QUI RESTE STABLE

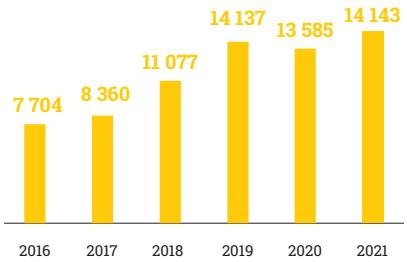
14 143

PLAINTES REÇUES EN 2021

+ 4 %

PAR RAPPORT À 2020

Nombre de plaintes par année



INFOSPLUS

Pour exercer ses droits, obtenir l'accès à ses données ou la suppression de contenus en ligne, la personne doit d'abord s'adresser 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.

Pour accompagner les personnes dans l'exercice de leurs droits, et si la plainte est recevable, la CNIL peut notamment transmettre les bons liens, contacts et procédures.

En 2021, **5 848** plaintes ont fait l'objet d'une réponse rapide (ou « de premier niveau », c'est-à-dire en 10 jours en moyenne) 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 notamment reçu et traité rapidement 253 plaintes concernant la **vidéosurveillance** mise en œuvre par des particuliers.

Par exemple, des personnes constatent l'installation, par un voisin, d'une caméra sur un mur, le toit ou un balcon de leur résidence, qui filmerait au-delà du domicile de l'installateur. La CNIL rappelle dans ces cas, par courrier, la règlementation applicable à la vidéosurveillance au domicile[14].

8 295 plaintes ont nécessité un traitement plus approfondi.

Après un examen de l'objet de la plainte, d'éventuelles vérifications informelles ou des demandes de complément d'information auprès du plaignant, la CNIL intervient par écrit auprès du responsable du fichier mis en cause.

Lorsqu'un organisme ne répond pas aux demandes de la CNIL, une procédure de sanction peut être engagée pour absence de coopération. Ainsi, en 2021, un office notarial a été sanctionné d'une amende de 3 000 € avec une injonction sous astreinte de répondre à la CNIL.

Dans certains cas, des plaintes peuvent faire l'objet de modalités de traitement différentes. Par exemple, elles peuvent directement faire l'objet d'un contrôle, notamment si leur sujet porte sur une thématique prioritaire de contrôle de la CNIL.

LE TRAITEMENT DES PLAINTES

Un traitement rapide pour un certain nombre de plaintes

Certaines plaintes reçues par la CNIL peuvent être traitées rapidement par un rappel de la règlementation applicable. C'est notamment le cas de plaintes concernant un cas individuel qui ne laisse, à priori, pas présager d'un manquement structurel ou mettant en cause des organismes disposant d'un délégué à la protection des données.

Au-delà de la résolution du cas individuel, ces plaintes sont également analysées pour identifier des problématiques communes à des organismes régulièrement mis en cause.

Ainsi, en 2021, plusieurs contrôles ont eu lieu dans le secteur de l'énergie concernant la prospection commerciale téléphonique : la prospection commerciale est ainsi devenue, en 2022, une des trois thématiques prioritaires de contrôle de la CNIL[15].

Les plaintes nécessitant un traitement plus long

Certaines plaintes nécessitent des analyses juridiques ou technologiques plus poussées. Des investigations auprès des organismes mis en cause sont alors nécessaires et peuvent conduire à échanger plusieurs courriers, à convoquer les organismes ou effectuer des contrôles.

14 « La vidéosurveillance, vidéoprotection – chez soi », mis à jour le 13 décembre 2019, cnil.fr
15 « Thématiques prioritaires de contrôle 2022 : prospection commerciale, cloud et surveillance du télétravail », 15 février 2022, cnil.fr

UNE ACTIVITÉ ENCORE MARQUÉE PAR L'ÉPIDÉMIE DE COVID-19

Ainsi en 2021, malgré les difficultés pour réaliser des contrôles sur place en raison de la pandémie, **31 % des contrôles réalisés par la CNIL ont fait suite à des plaintes et des signalements.**

L'année 2021 a notamment été marquée par un investissement notable sur le sujet des cookies et autres traceurs : plus de 250 plaintes reçues ont mis en cause des sites web ne respectant à priori pas les règles en la matière.
La CNIL reçoit également des plaintes contre des organismes établis uniquement dans des États situés hors de l'Union européenne (Royaume-Uni, Suisse, États-Unis d'Amérique, Canada, Russie, Australie, Corée du Sud, Chine). Ces plaintes portent principalement sur la diffusion de données sur internet. Après avoir vérifié si le RGPD est applicable aux traitements de données en cause, la CNIL intervient auprès de ces sociétés, lorsqu'il est possible de les identifier et de trouver un moyen de contact.

Enfin, lorsque la plainte porte sur un traitement mis en œuvre par un organisme établi dans un autre État membre de l'Union européenne, la CNIL doit généralement transmettre cette plainte à l'autorité du pays concerné et coopérer avec celle-ci.

Histoires vécues...

Monsieur V. Après un achat en ligne, Monsieur V. est déçu du service client de la boutique et décide de le faire savoir dans un avis publié sur son site web.

Le gérant de la boutique répond à l'avis de Monsieur V. en mentionnant ses numéros de commande, adresse de courriel et numéro de téléphone. Malgré ses demandes, le gérant refuse d'effacer les données concernant Monsieur V.

Saisie par M. V., la CNIL intervient auprès de la boutique pour lui rappeler que les données personnelles des clients ne doivent pas être divulguées. Le gérant de la boutique supprime les données concernant M. V. et ne publie plus d'informations sur ses clients en réponse aux avis en ligne.

Histoires vécues...

Plusieurs assurés sociaux rencontrent des difficultés pour faire **rectifier l'orthographe de leur nom ou prénom dans leur passe sanitaire** dans le cadre de l'épidémie de COVID-19.

Leurs demandes auprès de leur caisse locale d'assurance maladie ou de leur médecin ou du centre de vaccination ne permettent pas systématiquement de régler leurs difficultés.

L'intervention de la CNIL auprès des délégués à la protection des données (DPO) des caisses primaires concernées a permis de faire rectifier les données.

Au cours de l'année 2021, la CNIL a reçu des plaintes posant des questions juridiques et organisationnelles complexes, dans un contexte d'urgence sur le terrain, avec des organismes publics et privés chargés d'appliquer des textes suscitant beaucoup d'interrogations.

Ainsi, que ce soit dans le monde du travail, au sein des établissements scolaires ou universitaires, dans les associations notamment sportives, dans les établissements médicaux et médico-sociaux ou encore dans les commerces, **des responsables de traitement sont allés bien au-delà de ce que le législateur permettait**, souvent en pensant bien faire ou dans un souci de pragmatisme.

La centaine de plaintes reçues par la CNIL en 2021 liées à la pandémie a conduit la CNIL à rappeler à leurs obligations plusieurs organismes, dont des employeurs, au sujet du passe sanitaire ou de l'obligation vaccinale.

LES IRRITANTS DU QUOTIDIEN

Comme chaque année, certains sujets du quotidien numérique ont généré de nombreuses plaintes auprès de la CNIL.

La prospection commerciale, associative et politique

973 plaintes reçues en 2021 concernent la publicité par courrier électronique (38 %), SMS (29 %), voie postale (20 %) et téléphone (13 %). Les personnes rencontrent le plus généralement des difficultés pour ne plus recevoir de prospection alors qu'elles ont exprimé leur opposition à ces envois. Elles rencontrent également des difficultés à identifier qui a transmis leurs coordonnées aux organismes à l'origine de la prospection.

DÉFINITION

L'*open data*

L'*open data* désigne un mouvement d'ouverture et de mise à disposition des données produites et collectées par les services publics (administrations, collectivités locales...).

En 2019, la CNIL et la CADA ont publié un guide[16] pour accompagner les organismes publics à mettre en place de l'*open data* dans le respect des règles sur la protection des données.

16 « Publication en ligne et réutilisation des données publiques (« *open data* ») », cnil.fr

Histoires vécues...

Madame Y. s'adresse directement à la CNIL afin de faire supprimer des informations qui la concernent sur un réseau social.

La CNIL lui a indiqué **les moyens d'agir directement sur le réseau social** pour supprimer le contenu.

Le réseau social a supprimé rapidement les informations souhaitées.

LE DROIT À L'OUBLI SUR INTERNET

1 906 plaintes reçues en 2021 concernent principalement l'effacement de données de dirigeants de sociétés publiées sur des sites web de type annuaires d'entreprises ayant collecté les informations auprès de l'INPI ou de l'INSEE au titre de l'*open data* du registre du commerce et des sociétés. Certaines plaintes concernent également la publication de données mettant en cause ou dénigrant les plaignants sur des réseaux sociaux ou des blogs.

La CNIL a également reçu plus de 175 plaintes relatives à des demandes d'effacement de contenus concernant des articles de presse publiés en ligne faisant suite à des condamnations pénales (retrait de l'article, anonymisation, désindexation).

Enfin, la CNIL a reçu **292 nouvelles plaintes en matière de déréférencement** (- 23,5 %) qui concernent principalement le moteur de recherche Google, très majoritairement utilisé par les internautes français. Pour l'instant, elle a obtenu ce déréférencement dans 87 % des cas transmis à Google (certains dossiers étant toujours en cours).

Surveillance des employés

83 % des plaintes reçues en 2021 relatives à la surveillance des salariés concernaient des dispositifs de vidéosurveillance au travail. En général, ces plaintes visent des entreprises de taille réduite qui ne disposent ni d'un service juridique ni du soutien d'un délégué à la protection des données. L'action de la CNIL vise donc à les informer de leurs obligations afin qu'elles se mettent en conformité. Lorsque cette action ne suffit pas, des contrôles sur place peuvent avoir lieu et donner lieu à des mises en demeure ou des sanctions.

Les autres sujets

Le droit d'accès

Concernant le **droit d'accès, la CNIL a reçu 1 436 plaintes, dont 28,7 % concernent le secteur du travail.** En outre, elle a reçu 112 plaintes concernant des difficultés dans l'exercice du droit d'accès à son dossier médical auprès d'un professionnel de santé (dentiste, médecin généraliste ou spécialisé, établissement de santé public ou privé).

Le fichage bancaire

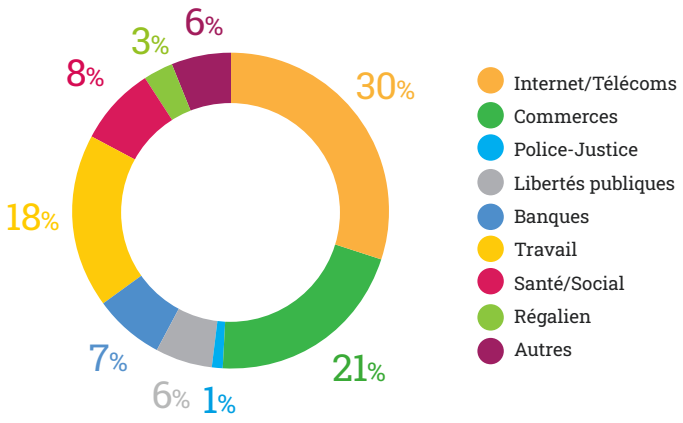
La CNIL a encore reçu plus de 200 plaintes concernant l'inscription par les établissements bancaires et de crédit de personnes dans les fichiers d'incidents de la Banque de France, notamment le fichier d'incidents de remboursement des crédits aux particuliers (FICP)[17] et le fichier central des chèques (FCC)[18].

Histoires vécues...

Après avoir quitté leur entreprise, plusieurs anciens employés sollicitent, en vain, la suppression de leur ancienne messagerie professionnelle et de photographies les représentant diffusées sur le profil LinkedIn et le site web de la société.

La CNIL est intervenue auprès de l'ancien employeur qui a procédé aux suppressions demandées.

Répartition des plaintes par secteur en 2021



17 « FICP : Fichier national des Incidents de remboursement des Crédits aux Particuliers », 10 juillet 2018, cnil.fr
18 « FCC : Fichier central des chèques et des retraits de cartes bancaires (CB) », 10 juillet 2018, cnil.fr

FOCUS

Les 101 plaintes noyb concernant Google Analytics et Facebook Connect

LE CONTEXTE

En août 2020, la CNIL a reçu 6 plaintes à l'encontre d'éditeurs de sites français par l'association autrichienne noyb (Centre européen pour les droits numériques). Celles-ci concernaient le transfert des données[19] des visiteurs de la version française de ces sites web vers les États-Unis d'Amérique, via la mise en œuvre d'un outil Facebook Business (Facebook connect) ou de la fonctionnalité Google Analytics.

Ces plaintes s'inscrivent dans la stratégie de noyb consistant à déposer 101 plaintes à l'encontre d'entreprises européennes qui poursuivent le transfert de données de visiteurs européens vers les États-Unis d'Amérique malgré l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 16 juillet 2020 ayant invalidé le *Privacy Shield*.

Dans cette décision, la CJUE a analysé la législation américaine en matière d'accès aux données des fournisseurs de services internet et entreprises de télécommunications par les services de renseignement américains. Elle en a conclu que les atteintes portées à la vie privée des personnes dont les données sont traitées par les entreprises et opérateurs États-uniens soumis à cette législation sont disproportionnées au regard des exigences de la Charte des droits fondamentaux. En conséquence, elle a invalidé le *Privacy Shield*, accord entre les États-Unis et l'Union européenne qui permettait d'encadrer juridiquement les transferts de données.

La CNIL et les autres autorités de protection des données européennes concernées par ces plaintes ont constitué un groupe de travail pour examiner ces plaintes de manière conjointe.

Elles ont procédé en parallèle à l'instruction des plaintes reçues. La CNIL a ainsi échangé à plusieurs reprises avec les sociétés mises en cause par noyb, ainsi qu'avec les autres autorités européennes.

Dans le cadre des travaux du groupe de travail européen, les autorités de protection des données ont conjointement considéré que les services mis en œuvre via le service Google Analytics n'étaient pas conformes au RGPD et ont établi un canevas commun de décision.

INFOSPLUS

ARRÊT « SCHREMS II » : UNE IDENTIFICATION NÉCESSAIRE DES TRANSFERTS DE DONNÉES

Les organismes européens et leurs sous-traitants doivent identifier leurs transferts de données concernés et **évaluer au cas par cas les éventuelles mesures supplémentaires**[20] à prendre pour assurer une protection effective et satisfaisante des données des européens.

LA DÉCISION DE LA CNIL

Le 10 février 2022, une semaine après son homologue autrichien, la CNIL a publié sa décision[21] : **elle estime que les transferts de données dus à Google Analytics sont illégaux et a imposé à un gestionnaire de site web français de se conformer au RGPD**, y compris en arrêtant d'utiliser cet outil dans les conditions actuelles.

De manière plus générale, le Comité européen sur la protection des données (CEPD) a adopté des recommandations pour tirer les conséquences de l'arrêt de la CJUE. Les organismes sont ainsi invités à recenser leurs transferts, à évaluer la législation du pays tiers vers lequel les données sont transférées et si nécessaire, à mettre en œuvre des mesures supplémentaires pour assurer un niveau de protection des données suffisant.

19 « Les transferts de données hors UE », cnil.fr
20 « *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* » (PDF, 1,3 Mo) [en anglais], edpb.europa.eu
21 « Utilisation de Google Analytics et transferts de données vers les États-Unis : la CNIL met en demeure un gestionnaire de site web », 10 février 2022, cnil.fr

LES PLAINTES EUROPÉENNES

La CNIL reçoit, directement par les plaignants ou par l'intermédiaire de ses homologues européens, des plaintes contre des acteurs principalement établis en France mais également établis dans d'autres États membres ou dont les fichiers contiennent des données relatives à des personnes résidant dans d'autres États membres.

Certaines plaintes, de par l'ampleur des manquements dénoncés et de par la taille des organismes concernés, font l'objet d'une coopération poussée entre la CNIL et ses homologues.

Ainsi, la CNIL a reçu plus de 200 plaintes de clients de la société Vinted. Après avoir traduit puis transmis ces plaintes à l'autorité lituanienne « chef de file » sur ce dossier, la CNIL participe à un groupe de travail avec cette autorité et l'autorité polonaise de protection des données afin de déterminer les actions à mener et analyser les réponses apportées par la société Vinted[22].

DROIT D'ACCÈS INDIRECT : 2021, UNE ANNÉE DE TRÈS FORTE ACTIVITÉ

Une augmentation des demandes de 35 % en un an

5 882

DEMANDES D'EXERCICE INDIRECT DES DROITS REÇUES PAR LA CNIL

+ 35 %

PAR RAPPORT À 2020

La CNIL a été très sollicitée par les usagers qui souhaitaient exercer leurs droits d'accès, de rectification ou d'effacement par son intermédiaire.

Les usagers ont ainsi adressé **5 882 courriers** ou courriels afin que la CNIL intervienne au titre de l'exercice indirect des droits, soit 35 % de plus qu'en 2020.

Plus de 5 300 demandes (90 %) ont été jugées recevables et suffisamment complètes pour permettre à la CNIL d'effectuer les vérifications nécessaires.

DÉFINITION

Qu'est-ce que le droit d'accès indirect ?

Pour la plupart des fichiers publics et privés, toute personne a le droit d'accéder aux informations qui la concernent en interrogeant directement l'organisme qui les détient.

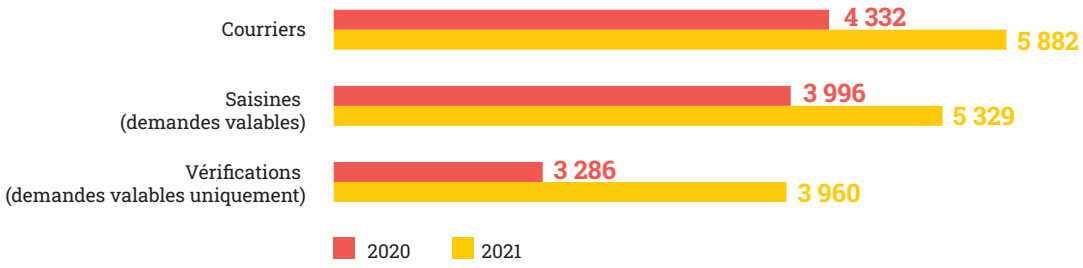
Cependant, ce droit est différent concernant certains fichiers de police, de gendarmerie ou de renseignement, pour lesquels l'accès n'est possible que par l'intermédiaire de la CNIL : **c'est le droit d'accès indirect**[23].

En pratique, le droit d'accès indirect n'offre pas un droit systématique à communication des données. Elles ne peuvent être communiquées qu'avec l'accord du responsable du fichier, qui peut s'y opposer pour des motifs liés à l'objectif du fichier, la sûreté de l'État, la défense ou la sécurité publique.

En cas de refus de communication, la CNIL indique les voies de recours qui sont ouvertes pour contester cette décision.

Dans tous les cas, la CNIL ne détient aucun fichier et ne peut apporter une réponse immédiate.

22 « Les pratiques de la plateforme Vinted contrôlées par des autorités de protection des données européennes », 18 novembre 2021, cnil.fr
23 « Le droit d'accès aux fichiers de police, de gendarmerie et de renseignement », cnil.fr

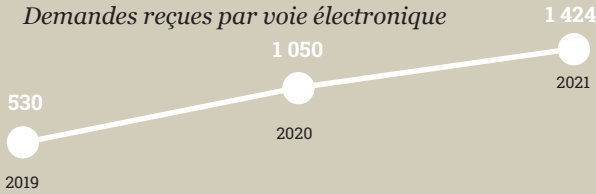


FOCUS

Vers un nouveau téléservice pour recueillir les demandes d'exercice indirect des droits

Depuis 2020, la CNIL a constaté que la proportion des sollicitations adressées par voie électronique est de plus en plus importante. Après avoir doublé entre 2019 et 2020, le nombre de ces demandes a encore augmenté de plus de 35 % en 2021.

Demandes reçues par voie électronique



Afin de répondre à cette évolution, la CNIL a engagé dès 2020 le travail nécessaire pour mettre à la disposition des usagers un téléservice dédié. Celui-ci devrait être déployé avant la fin de l'année 2022.

Histoire vécue...

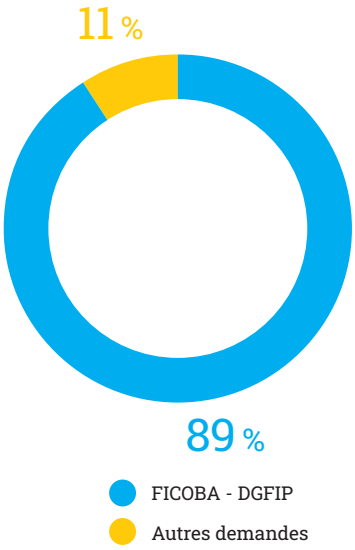
Monsieur G., à la recherche d'un emploi, souhaite orienter sa carrière vers des fonctions dans la sécurité incendie. En se renseignant, il a appris que le traitement d'antécédents judiciaires (TAJ) pouvait être consulté pour l'exercice de telles fonctions.
Il s'est alors souvenu qu'il avait fait l'objet de deux procédures judiciaires, l'une ancienne de 15 ans, l'autre ancienne de 3 ans. Ces deux affaires pouvaient alors bloquer sa réorientation professionnelle. Faute de réponse du ministère de l'Intérieur qu'il venait d'interroger, Monsieur G. s'est adressé à la CNIL pour savoir si des informations relatives à ces faits figuraient toujours dans le TAJ. Au terme des actions conduites par la CNIL, la première affaire a été supprimée sur accord du procureur de la République, la deuxième a été complétée par une mention concernant un classement sans suite dont Monsieur G. avait bénéficié.
Les éléments contenus dans le TAJ ne pouvaient alors plus porter préjudice au nouveau choix de carrière de Monsieur G.

D'autres correspondances n'ont en revanche pas pu être traitées par la CNIL. Il peut s'agir :

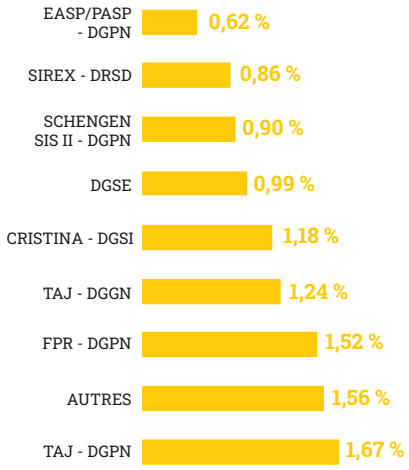
- de demandes ne relevant pas de la compétence de la CNIL ;
- de demandes incomplètes (défaut de copie d'un titre d'identité, absence de mention d'un fichier précis, etc.) : plus de 400 demandes ont ainsi été closes en l'absence de réponse aux courriers adressés par la CNIL afin d'obtenir le ou les éléments nécessaires à son action.

Le FICOBA reste le fichier le plus sollicité par les usagers

Proportion des demandes d'accès au FICOBA par l'intermédiaire de la CNIL



Répartition des autres demandes



En 2021, comme en 2020, le fichier des comptes bancaires et assimilés (FICOBA) est de loin le traitement pour lequel la CNIL est le plus souvent saisie. L'augmentation déjà identifiée en 2019 et 2020 se poursuit donc avec une nouvelle croissance de 40 % en un an.

4 753

Demandes concernant le fichier des comptes bancaires et assimilés (FICOBA)

+ 40 %

PAR RAPPORT À 2020

Des vérifications toujours en hausse

La croissance du nombre de demandes a conduit la CNIL à engager de plus en plus d'actions pour répondre aux usagers.

Elle a ainsi multiplié les échanges avec les gestionnaires des fichiers. Elle a en particulier conduit environ 4 000 vérifications (en croissance de 20 % par rapport à 2020).

Le traitement des demandes : un processus à plusieurs étapes nécessitant des actions auprès de plusieurs intervenants

Au cours de l'année 2021, la CNIL a instruit jusqu'à leur terme plus de 4 900 demandes. Pour les traiter, elle a dû engager des actions diverses impliquant parfois une ou plusieurs autres administrations.

La CNIL examine tout d'abord la recevabilité de la demande : celle-ci doit en effet relever de sa compétence et contenir l'ensemble des informations requises. Au besoin, elle s'adresse à l'usager ou aux gestionnaires de fichiers afin de compléter la demande.

La CNIL organise ensuite les vérifications. Elle doit notamment communiquer diverses informations à certains gestionnaires de fichiers afin qu'ils puissent rassembler les éléments nécessaires à la conduite des vérifications.

Elle effectue par la suite les vérifications afin de :

- déterminer si des données concernant l'usager sont ou non présentes dans le fichier ;
- d'examiner la conformité ; des traitements mis en œuvre ;
- de déterminer, avec le responsable de traitement, si le résultat des vérifications peut être communiqué à l'usager.

Ce n'est qu'à l'issue de ces démarches, qui nécessitent parfois plusieurs mois, que la CNIL répond de manière définitive à la demande d'accès, de rectification ou d'effacement adressée par un usager.

La contestation d'un refus de communication : la compétence de deux juges différents pour certains fichiers

Le gestionnaire du fichier peut s'opposer à la communication du résultat des vérifications opérées par la CNIL, que des données relatives à l'usager fassent ou non l'objet d'un traitement. Dans cette circonstance, la CNIL ne peut qu'informer l'usager qu'elle a procédé aux vérifications nécessaires et qu'il peut saisir le juge administratif afin de contester la décision du gestionnaire du fichier.

Pour certains fichiers, l'usager devra saisir deux juges administratifs : le tribunal administratif et la formation spécialisée du Conseil d'État. C'est ce qu'a récemment rappelé ce dernier concernant le fichier STARTRAC mis en œuvre par le service TRACFIN.

Histoires vécues...

Madame Y. avait le souvenir d'un livret A ouvert par ses grands-parents à sa naissance, au début des années 2000. Au cours de ses déménagements, elle avait cependant égaré les documents concernant ce compte qu'elle n'avait par ailleurs jamais utilisé.

Une fois majeure, elle souhaitait retrouver les références de ce compte pour deux raisons : utiliser l'argent que ses grands-parents y avaient déposé et ouvrir un nouveau livret A (en effet, tant que ce premier livret était ouvert, elle ne pouvait en ouvrir un autre auprès de la nouvelle banque dans laquelle elle entendait rassembler toute son épargne).

Elle a ainsi adressé une demande à la CNIL afin que lui soient communiquées les références de ce livret A « perdu ».
La CNIL a alors effectué des vérifications auprès du responsable de traitement. Celui-ci s'est cependant opposé à la communication de la liste complète des comptes figurant dans le FICOBA. Selon lui, une telle communication pouvait en effet nuire aux finalités du traitement, fragilisant notamment un contrôle fiscal de Madame Y. alors en cours.

Au regard des éléments apportés dans la demande, la CNIL a cependant sollicité du responsable de traitement qu'il accepte la communication des références du livret A évoqué par Madame Y.

Le responsable de traitement a finalement accepté l'envoi de ces informations, lesquelles ont permis à Madame Y. d'engager les démarches qu'elle envisageait.

CONSEILLER
les pouvoirs publics et le Parlement

La CNIL est amenée à 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.

Aurore,
Juriste au service de la santé, Direction de la conformité

Le service accompagne différentes catégories d'autorités publiques intervenant dans le domaine de la santé (ministère, autorité administrative indépendante, établissement public, agence, etc.).

L'année 2021 a été marquée par des projets numériques en santé d'envergure nationale qui ont eu - ou vont - avoir un impact significatif sur les acteurs publics et privés ainsi que sur la société dans son ensemble. Entre la crise sanitaire qui a nécessité d'adapter en continu les systèmes d'information créés pour lutter contre l'épidémie, le déploiement de la feuille de route du numérique en santé, les divers projets de recherche en santé, les sujets ont été variés et sources de défis majeurs.

Au service santé de la CNIL, conseiller les pouvoirs publics c'est notamment :

- *répondre aux interrogations des parlementaires ;*
- *analyser des projets de texte au regard de la règlementation « données personnelles » tout en prenant en considération les règlementations sectorielles applicables ;*
- *identifier les évolutions nécessaires de la doctrine de la CNIL au regard des besoins de ces acteurs ;*
- *formuler des recommandations opérationnelles en associant les différentes expertises des agents de la CNIL.*

Pour l'année 2022, nous avons comme objectif de poursuivre notre mission de conseil et d'accompagnement des pouvoirs publics ainsi que des acteurs privés, notamment par l'adoption de référentiels et la publication de guides et de recommandations.

LES ACTIVITÉS AU PARLEMENT

22

auditions

13

contributions écrites

Une nouvelle année marquée par la crise sanitaire

Comme en 2020, la crise sanitaire a occasionné de nombreuses sollicitations afin d'éclairer les travaux législatifs consacrés aux recours aux outils numériques dans la gestion de l'épidémie de COVID-19.

Ainsi, la CNIL a été auditionnée au mois de mars par la commission des affaires sociales de l'Assemblée nationale afin de faire un **bilan complet sur les conditions de mise en œuvre des systèmes d'information liés à la lutte contre l'épidémie**, sur la base de ses avis trimestriels rendus au Parlement[24].

La CNIL a également été auditionnée par les rapporteurs, dans les deux chambres, des projets de loi (gestion de la sortie de crise sanitaire, adaptation des outils de gestion de la crise sanitaire).

Elle a enfin envoyé une contribution écrite demandée par la commission des affaires sociales du Sénat au sujet de la proposition de loi visant à la création d'une plateforme de référencement et de prise en charge des malades chroniques de la COVID-19.

Sécurité intérieure et données personnelles : une première saisine de la CNIL sur une proposition de loi

Cette année, la CNIL a également été particulièrement sollicitée par les deux assemblées sur les questions de sécurité.

La proposition de loi relative à la sécurité globale intéressait directement la protection des données personnelles, notamment par la modification du cadre juridique applicable en matière de vidéo et de la réglementation des caméras aéroportées (drones). Le 30 novembre 2020, le président de la commission des lois du Sénat a ainsi demandé l'avis de la CNIL en faisant usage, pour la première fois, de la faculté qui lui permet de la saisir de toute proposition de loi relative à la protection ou au traitement des données personnelles. La commission des lois du Sénat a également auditionné la présidente de la CNIL, le 3 février 2021.

Par ailleurs, la CNIL a été entendue en audition par les rapporteurs de la commission des lois de l'Assemblée et du Sénat dans le cadre de l'examen de deux projets de loi : prévention d'actes de terrorisme et renseignement, et Responsabilité pénale et sécurité intérieure (voir focus page 53).

Enfin, dans le cadre des échanges avec des parlementaires nommés en mission, la CNIL a contribué aux travaux de réflexion confiés à M. Jean-Michel Mis, député de la Loire, sur les nouvelles technologies dans le domaine de la sécurité.

DÉFINITIONS

Le *Digital Services Act*

La proposition de règlement européen sur les services numériques ***(Digital Services Act)*** modernise la directive sur le commerce électronique et définit les obligations et responsabilités des fournisseurs de services intermédiaires en ligne, par exemple les plateformes numériques.

Le *Digital Markets Act*

La proposition de règlement européen législation sur les marchés numériques ***(Digital Markets Act)*** est un autre texte proposé par la Commission européenne qui a pour objectif d'encadrer les pratiques des très grands acteurs en ligne, qualifiés de contrôleurs d'accès, mieux réguler les grandes sociétés du numérique, telles que les GAFAM, afin d'assurer l'équité et la contestabilité des marchés numériques. En particulier, le projet de texte prévoit que ces grands acteurs ne pourront plus réutiliser librement les données personnelles collectées via la fourniture de leurs services de plateforme essentiels.

24 « Les avis de la CNIL sur les dispositifs de lutte contre la COVID-19 », cnil.fr

La réforme de la loi Informatique et Libertés pour simplifier les procédures de sanction

La CNIL a étroitement collaboré avec le Parlement afin d'aboutir à une simplification des procédures relatives au prononcé des mesures correctrices prévues par le RGPD et la loi Informatique et Libertés en cas de manquement à ces dispositions.

Cette adaptation permettra d'augmenter les capacités coercitives de la CNIL dans un contexte d'augmentation constante et substantielle du volume de plaintes.

Cette réforme a été définitivement adoptée dans la loi relative à la responsabilité pénale et à la sécurité intérieure n° 2022-52 du 24 janvier 2022.

L'expertise de la CNIL sur les dossiers européens

Les commissions des affaires européennes des deux chambres parlementaires se sont penchées en 2021 sur plusieurs sujets liés à l'actualité des institutions de l'Union européenne.
Dans ce contexte, l'éclairage de la CNIL par des contributions écrites a été sollicité au sujet des projets de textes européens *Digital Services Act* et de *Digital Markets Act*. (voir encadré Définitions, page précédente).

La CNIL a aussi été auditionnée par la rapporteure de la commission des affaires européennes sur les effets des jurisprudences de la CJUE du 6 octobre 2020 (sur les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a.) à propos de la question de la conservation des données de connexion par les fournisseurs de services de communication téléphoniques et électroniques.

Enfin, la CNIL a contribué en audition et par écrit aux travaux de la mission commune d'information de l'Assemblée sur la souveraineté numérique nationale et européenne.

L'ACCOMPAGNEMENT DES ACTEURS PUBLICS

Les actions de sensibilisation préélectorales

En matière de vie politique, la CNIL poursuit son action entamée il y a trente ans, avec sa première recommandation sur la communication politique. Cette année encore, elle a mis en œuvre de nombreuses actions afin d'accompagner l'ensemble des parties prenantes du processus électoral.

L'année 2021 a été particulièrement riche du fait de la tenue des élections régionales et départementales puis de la préparation des élections présidentielle et législatives qui auront lieu en 2022.
La CNIL s'est mobilisée pour sensibiliser aux enjeux de la protection des données dans le cadre électoral, qu'il s'agisse de campagne électorale ou de la tenue de scrutins.

Une mise à jour des contenus sur la vie politique et la protection des données personnelles

La CNIL a procédé à la mise à jour des contenus disponibles sur son site web[26], au regard notamment des mauvaises pratiques, plaintes et signalements constatés.

Le cadre juridique y est présenté ainsi que des conseils pratiques pour que les traitements de données personnelles des candidats et des partis politiques soient les plus respectueux possibles de la vie privée des électeurs.

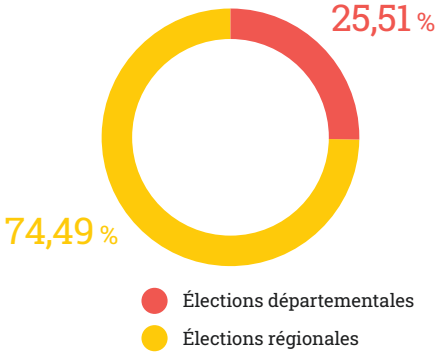
La CNIL a également actualisé les renseignements qu'elle délivre aux électeurs concernant leurs droits. À son habitude, la CNIL a mis à disposition une plateforme de signalements spécifique aux élections sur son site.

L'accompagnement des acteurs

Dans sa démarche d'accompagnement, la CNIL a également prodigué des conseils à divers acteurs de la vie politique, comme des équipes de campagne ou des élus lors du Salon des maires et des collectivités territoriales organisé du 16 au 18 novembre 2021 à Paris.

En vue des élections 2022, la CNIL a entamé des opérations de sensibilisation et d'accompagnement des partis et leurs candidats. Une action de sensibilisation a été menée auprès des équipes de campagne le 14 octobre 2021, lors d'une journée organisée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), sur la protection des données personnelles. Elle poursuivra son action dans cette lignée pour les échéances électorales de l'année à venir.

Répartition des 1 023 signalements en 2021



26 « Vie politique et citoyenne », cnil.fr

FOCUS

L'avis de la CNIL sur la proposition de loi « sécurité globale »

Saisie par le président de la commission des lois du Sénat, la CNIL a rendu son avis sur la proposition de loi « sécurité globale » le 26 janvier 2021. Cette proposition de loi visait notamment à permettre à un grand nombre d'acteurs tant publics que privés d'être associés à la mise en œuvre de la politique de sécurité sur le territoire national, en modifiant les prérogatives et les missions qui leur sont confiées. Le texte contenait plusieurs dispositions qui concernaient directement la protection des données personnelles à travers, en particulier, la modification du cadre juridique applicable en matière de vidéo et l'édiction d'une nouvelle réglementation des caméras aéroportées (drones).

Dans son avis, **la CNIL a notamment souligné les implications éthiques attachées au déploiement d'outils qui, par essence, présentent des risques d'atteintes aux libertés publiques et à la vie privée des individus**. Elle a ainsi alerté sur les spécificités des drones, qui sont des dispositifs mobiles, discrets par nature, et dont la position en hauteur permet de filmer des lieux jusqu'ici difficiles d'accès, voire interdits aux caméras classiques. La captation d'images qu'ils permettent est considérablement élargie et, surtout, peut être individualisée avec un suivi des personnes dans leurs déplacements, à leur insu et sur une durée qui peut être longue.

D'autres observations ont par ailleurs été formulées par la CNIL sur les dispositions de proposition concernant les caméras individuelles, les caméras embarquées dans certains véhicules, ainsi que la vidéoprotection, en particulier sur la transmission en temps réel des images aux forces de l'ordre.

De manière générale, la CNIL a souligné dans cet avis que le cadre normatif tel qu'envisagé, et les évolutions qui en découlent, ne permettaient toujours pas, selon elle, d'aboutir à un encadrement juridique suffisamment protecteur des droits des personnes. Elle a, dans ce contexte, rappelé qu'**elle se montrerait particulièrement vigilante quant aux conditions effectives de mise en œuvre** des traitements de données personnelles lorsqu'elle examinera les dispositions réglementaires qui lui seront soumises en application de la loi. Le projet de loi a substantiellement évolué à la suite de cet avis, au cours du débat parlementaire.

Les avis de la CNIL sur les projets de loi relatif à la prévention d'actes de terrorisme et au renseignement

La CNIL s'est prononcée en urgence, dans trois avis en date du 8 avril, du 15 avril et du 3 mai 2021, sur certaines dispositions du projet de loi relatif à la prévention d'actes de terrorisme, dans leur version alors envisagée par le gouvernement[27].

Dans la continuité de la loi de 2015 relative au renseignement, le projet de loi visait à adapter les outils dont disposent actuellement les services de renseignement aux évolutions de la menace et des technologies de l'information. Ce texte comprenant plusieurs dispositions qui intéressent la protection des données personnelles ainsi que la vie privée, le gouvernement en avait donc saisi la CNIL pour avis.

Dans ses avis, la CNIL a relevé que le gouvernement a encadré ces dispositifs de garanties importantes, dans la continuité de l'encadrement des techniques de renseignement en 2015. Elle a néanmoins estimé qu'afin d'assurer un juste équilibre entre les impératifs de sécurité et les atteintes portées à la vie privée des personnes concernées, des garanties supplémentaires devaient être prévues.

S'agissant de la technique de renseignement dite de « l'algorithme » – créée pour détecter automatiquement les connexions téléphoniques ou sur internet susceptibles de révéler une menace terroriste – **la CNIL a estimé ne pas disposer des éléments nécessaires pour lui permettre d'apprécier la nécessité de sa pérennisation**. Elle a demandé que l'éventuelle extension de cette technique aux URL fasse l'objet d'une nouvelle expérimentation, sans être suivie sur ce point par le Parlement.

Concernant les autres techniques de renseignement, la CNIL a relevé que des garanties importantes étaient mises en œuvre (limitation pour certaines finalités, durées de conservation, accès limités, etc.). **Elle a néanmoins recommandé que certaines mesures complémentaires soient prévues par le projet de loi** (limitation des finalités permettant de recourir à certaines techniques et précisions quant aux conditions de mise en œuvre, par exemple). Le projet de loi rectificatif a donné suite à certaines de ces recommandations.

Comme en 2015, la CNIL a également rappelé sa demande que ses pouvoirs de contrôle puissent être mis en œuvre concernant les fichiers de renseignement alimentés par ces techniques de manière adaptée à leurs spécificités. Elle a rappelé que les fichiers des services de renseignement sont soumis à la loi Informatique et Libertés mais que leurs conditions de mise en œuvre effectives ne font l'objet d'aucun contrôle de sa part.

27 « Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement : la CNIL publie ses avis », cnil.fr

L'ANALYSE DE LA CNIL

COVID-19 : GARANTIR LE RESPECT DE LA VIE PRIVÉE ET DES LIBERTÉS EN TEMPS DE CRISE

Dans le contexte de la crise sanitaire, l'utilisation des technologies de communication à distance et de dispositifs de surveillance pour essayer de ralentir l'épidémie ou pour s'adapter aux mesures de distanciation physique n'a cessé d'augmenter. Tout au long de l'année, la CNIL a conseillé activement les pouvoirs publics afin de contribuer à garantir que la mise en œuvre des systèmes d'information sanitaires (TousAntiCovid, SI-DEP, Contact Covid, Vaccin Covid) soit respectueuse des droits des personnes concernées.

16

avis rendus sur des traitements de données mis en œuvre dans le cadre de la lutte contre l'épidémie en 2021

29

contrôles effectués sur ces traitements de données en 2021

L'accompagnement de la CNIL

En 2021, la CNIL a **rendu 16 avis**[28], **la plupart portant sur des projets de texte soumis par le gouvernement** :

- 3 avis publics sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 ;
- 5 avis portant sur SIDEP et Contact Covid, dont quatre portant également sur le SI Vaccin Covid ;
- 5 avis sur le passe sanitaire ;
- un avis sur un décret prévoyant un traitement de données relatif au suivi et au contrôle du respect des mesures de quarantaine et d'isolement (non publié) ;
- un avis sur la constitution d'un « Portail autotest Covid » ;
- un avis sur l'application TousAntiCovid.

D'une manière générale, ces avis ont été l'occasion pour la CNIL de **rappeler la nécessité de porter à sa connaissance des éléments concrets permettant d'évaluer l'efficacité de ces dispositifs dans la lutte contre l'épidémie de COVID-19 et ainsi de lui permettre d'apprécier pleinement leur nécessité et leur proportionnalité** dans le cadre de la politique sanitaire du gouvernement.

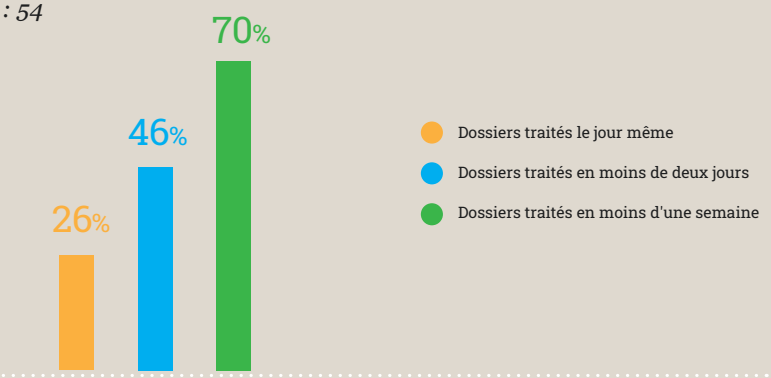
La CNIL a alerté, tant les pouvoirs publics que ses concitoyens, sur le **risque d'accoutumance et de banalisation** de ces dispositifs dérogatoires et donc d'un **glissement vers une société où de tels contrôles deviendraient la norme et non l'exception**. En effet, ces mesures exceptionnelles ne peuvent être justifiées que si leur efficacité est prouvée, leur application limitée en termes de durée, de personnes ou de lieux concernés, et si elles sont assorties de garanties de nature à prévenir efficacement les abus.

La CNIL a également eu l'occasion de rappeler, au vu de la sensibilité des données recueillies, du contexte justifiant leur mise en œuvre ainsi que de leur ampleur, la nécessité d'améliorer l'information déjà disponible pour le grand public et les utilisateurs de ces dispositifs, notamment lorsque des modifications y sont apportées. Elle a ainsi invité le ministère des Solidarités et de la Santé à diffuser une information concise, transparente, compréhensible et aisément accessible, afin que l'ensemble de la population puisse avoir connaissance de l'existence des différents traitements liés à ces dispositifs et appréhender leur étendue ainsi que leurs éventuelles interconnexions.

Outre les avis rendus sur des projets de textes, la CNIL s'est fortement **investie en conseillant** les pouvoirs publics et les responsables de traitement impliqués dans la lutte contre l'épidémie.

Ainsi, elle a eu l'occasion d'échanger de manière régulière avec les ministères concernés s'agissant, par exemple :

Autorisations de recherche en lien avec la COVID-19 en 2021
Total : 54



28 « COVID-19 : tous les avis de la CNIL », cnil.fr

- de la mise en œuvre du passe sanitaire, devenu passe vaccinal ;
- de la mise en œuvre du contrôle de l'obligation vaccinale ;
- des modalités de mise en œuvre du protocole sanitaire dans les écoles.

Enfin, la CNIL s'est fortement mobilisée pour se prononcer, dans des délais les plus courts possibles, sur **plusieurs projets de recherche dans le domaine de la santé dont la mise en œuvre suppose le traitement de données de santé** et nécessite, dans certains cas, l'obtention d'une autorisation de sa part.

Apporter des réponses et contribuer à la transparence des dispositifs

La CNIL s'est particulièrement attachée à garantir la transparence des dispositifs mis en œuvre dans le cadre de la lutte contre l'épidémie et à améliorer leur compréhension, par les professionnels et les personnes concernées. En 2021, elle a ainsi mis à disposition des outils et des publications sur son site web, dans un objectif pédagogique.

+ de 40 000 vues

pour le communiqué « La CNIL rappelle les principes à respecter pour diffuser aux médecins la liste de leurs patients non vaccinés[29] » publié en juillet 2021 sur cnil.fr

En 2021, elle a également proposé et mis à jour des contenus afin de diffuser largement ses recommandations (FAQ, communiqués de presse, etc.). Elle a notamment apporté des réponses et des éclaircissements sur :

- le passe sanitaire et l'obligation vaccinale ;
- la collecte de données personnelles sur le lieu de travail ;
- les règles et bonnes pratiques à suivre en matière de télétravail ;
- la continuité pédagogique et le quotidien dans les établissements scolaires (tests salivaires, organisation des examens, etc.) ;
- les traitements mis en œuvre par les collectivités territoriales ;
- le contrôle qualité à distance des données dans les essais cliniques (recommandations provisoires).

Elle poursuivra, d'une manière générale, ses actions d'accompagnement à destination des professionnels de santé, notamment par la production de référentiels et de contenus sectoriels adaptés à leurs activités, **ainsi que la diffusion d'informations à destination du grand public**.

Dans l'Union européenne, une intensification des échanges quotidiens

Enfin, au niveau européen, la CNIL a activement participé aux travaux du Comité européen de la protection des données (CEPD) en lien avec la gestion de l'épidémie. Elle a ainsi pu contribuer à l'élaboration de l'avis sur la proposition de règlement relatif au certificat vert numérique (*Digital Green Certificate*) de la Commission européenne[30]. Cet avis a été l'occasion de revenir sur les garanties que ce dispositif doit apporter pour les droits et libertés fondamentaux des personnes, à savoir disposer d'une base légale qui respecte les principes de nécessité et de proportionnalité et qui contienne les garanties essentielles pour éviter tout risque de discrimination et d'atteinte aux droits et libertés fondamentaux des personnes concernées.

Par ailleurs, la crise sanitaire actuelle a conduit à la désignation de « points de contacts » au sein de chaque autorité et à la mise à disposition d'un espace collaboratif en ligne dédié aux sujets relatifs au COVID-19. Les échanges avec les homologues européens ont permis d'éclairer les réflexions et travaux de la CNIL et d'assurer une approche harmonisée des régulateurs face à des questions, souvent inédites.

Les contrôles : vérification du respect des principes du RGPD et du cadre réglementaire

Outre les modalités selon lesquelles les opérations de contrôles s'effectuent, la situation sanitaire a fortement impacté le choix des contrôles menés par la CNIL : les missions portant sur les traitements liés à l'épidémie de COVID-19

DÉFINITION

Les traitements mis en place par l'État pour lutter contre l'épidémie

Le fichier **SI-DEP** (système d'information de dépistage) 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 de dépistage de la COVID-19 réalisés par des laboratoires publics ou privés et certains professionnels de santé habilités, comme les pharmaciens.

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 :

- Les médecins de ville/établissements de santé/centres de santé.
- Le personnel habilité de l'assurance maladie.
- Les agences régionales de santé (ARS).

TousAntiCovid (anciennement StopCovid) est une application mobile de **suivi de contacts**, basée sur le **volontariat** des personnes et utilisant la technologie Bluetooth. Mise à disposition par le gouvernement, elle permet d'alerter les utilisateurs d'un risque de contamination lorsqu'ils ont été à proximité d'un autre utilisateur ayant été diagnostiqué ou dépisté positif à la COVID-19. L'application fournit également des informations factuelles et sanitaires sur l'épidémie et permet le stockage du passe sanitaire et du statut vaccinal.

Le fichier **Vaccin COVID**, géré conjointement par la Direction générale de la santé et de la Caisse nationale d'assurance maladie (CNAM) a pour objectif la **mise en œuvre**, le **suivi** et le **pilotage des campagnes vaccinales** contre la COVID-19. Il comprend des informations sur les personnes invitées à être vaccinées ou déjà vaccinées afin notamment d'organiser la campagne de vaccination, le suivi et l'approvisionnement en vaccins et consommables (seringues, etc.), et la réalisation de recherches et du suivi de pharmacovigilance. Ce fichier n'a pas vocation à s'étendre à d'autres vaccinations que celle contre la COVID-19.

29 « La CNIL rappelle les principes à respecter pour diffuser aux médecins la liste de leurs patients non vaccinés » sur cnil.fr
30 « COVID-19 : le CEPD et le Contrôleur européen de la protection des données rendent un avis sur la proposition de certificat vert numérique », cnil.fr

FOCUS

COVID-19 : mise en demeure de la société Francetest pour sécurisation insuffisante des données de santé

Le 4 octobre 2021, la CNIL a mis en demeure la société Francetest de sécuriser les données de santé qu'elle collecte pour le compte des pharmacies à l'occasion de tests de dépistage à la COVID-19.

LE CONTEXTE

Le 27 août 2021, la CNIL a reçu un signalement anonyme indiquant l'existence d'une violation de données affectant la sécurité du site web francetest.fr.

Cette violation portait sur les données exploitées par la société Francetest dans le cadre d'un service qu'elle propose aux pharmacies pour simplifier la collecte des données des patients faisant des tests antigéniques et pour faciliter leur transmission vers la plateforme SI-DEP (fichier mis en œuvre par le ministère des Solidarités et de la Santé pour centraliser les résultats des tests).

La base de données exposée concernait 386 970 personnes et comportait leur nom, prénom, adresse e-mail, numéro de téléphone, date de naissance, résultat du test (positif ou négatif) et numéro de sécurité sociale.

LES CONTRÔLES ET LE MANQUEMENT CONSTATÉ

La CNIL a mené des contrôles afin de connaître les circonstances de cette violation de données et vérifier les mesures prises pour assurer la sécurité des données. Elle a constaté que la société avait pris certaines mesures pour remédier à la vulnérabilité à l'origine de la violation de données mais que son service présentait toujours plusieurs insuffisances en matière de sécurité (données de santé hébergées sans agrément adéquat - « Hébergement des données de santé » (HDS) - processus d'authentification pas assez robustes, procédés cryptologiques faibles et absence de journalisation des activités des serveurs).

En conséquence, la présidente de la CNIL a mis la société en demeure, dans un délai de deux mois, de prendre les mesures nécessaires pour garantir la sécurité des données de santé qu'elle traite pour le compte de centaines de pharmacies.

Dans ce cadre, la société a démontré qu'elle avait mis fin aux insuffisances constatées. La mise en conformité étant atteinte, la procédure a été close par une décision du 26 janvier 2022.

ont représenté 10 % de la totalité des contrôles réalisés durant l'année 2021 (TousAntiCovid, TousAntiCovid Vérif, SI-DEP, Contact-Covid, Vaccin Covid et passe sanitaire).

Afin de s'assurer du respect du cadre réglementaire, de la prise en compte des recommandations qu'elle a pu émettre dans ses avis et de réagir efficacement aux différentes plaintes qui lui ont été adressées, la CNIL a poursuivi la vérification des traitements mis en œuvre. Ces contrôles ont été diligentés auprès des différents organismes participant à ces traitements :

- 3 agences régionales de santé ;
- un rectorat ;
- 2 pharmacies ;
- 2 centres de vaccinations ;
- l'AP-HP ;
- la direction générale de la Santé (ministère des Solidarités et de la Santé) ;
- l'INRIA ;
- plusieurs établissements mettant en œuvre des traitements relatifs à la vérification du passe sanitaire (par exemple : restaurant, aéroport, musée, fédération sportive).

Dans le cadre de ces contrôles, la CNIL a porté une attention particulière :

- aux modalités de mise en œuvre et d'utilisation des dispositifs, notamment s'agissant de leurs évolutions ;
- aux modalités d'information des personnes ;
- à la sécurité des systèmes d'information ;
- aux flux de données et aux destinataires ;
- aux modalités de conservation des données ;
- à la réalisation d'analyses d'impact relatives à la protection des données.

Au total, depuis le début de la pandémie, la CNIL a réalisé **53 opérations de contrôle sur les dispositifs** mis en place dans le cadre de la crise sanitaire, **dont 29 en 2021**, et a adressé plus de 200 courriers à des organismes dans le cadre de ces contrôles.

Cette mobilisation perdurera, notamment afin de s'assurer de la suppression des données traitées dans ces dispositifs lorsque ceux-ci ne seront plus nécessaires.

31 Les traitements de données personnelles mis en œuvre à des fins de recherche, étude ou évaluation dans le domaine de la santé peuvent être mis en œuvre si le responsable de traitement déclare être conforme à une méthodologie de référence. Dans le cas contraire, il devra faire une demande d'autorisation spécifique de la CNIL.
Les méthodologies de référence sont publiées sur cnil.fr.

La parole à Lauren DEMERVILLE

Responsable du pôle Partenariats et Expertises de la Direction de la Recherche Clinique et de l'Innovation de l'AP-HP

Comment collaborez-vous avec les services de la CNIL dans le cadre de la mise en œuvre des projets de recherche de l'AP-HP ? Cette collaboration a-t-elle évolué pendant la crise sanitaire ?

La collaboration entre la Direction de la Recherche Clinique, de l'Innovation et des relations avec les universités et les Organismes de Recherche (DRCI) de l'AP-HP et la CNIL s'inscrit principalement dans le cadre des demandes d'autorisation soumises aux services de la CNIL pour la mise en œuvre de traitements de données de projets de recherche non conformes à une méthodologie de référence . Cette collaboration s'est extrêmement intensifiée pendant la crise sanitaire. Les services de la CNIL ont fait preuve d'une grande adaptation et d'une extrême réactivité. Le mécanisme de pré-instruction mis en place pour les études portant sur la COVID-19 a régulièrement permis d'obtenir l'autorisation de la CNIL le jour même de la transmission de l'avis favorable du CPP, tout en garantissant le niveau d'exigence applicable à tout traitement.

Quel est selon vous l'apport de l'instruction par la CNIL des demandes d'autorisation relatives aux projets de recherche qui ne sont pas conformes à des référentiels ?

La très grande majorité des recherches conduites par l'AP-HP sont conformes à des référentiels, notamment les méthodologies de référence, qui permettent une mise en œuvre rapide des traitements peu sensibles, en inversant la responsabilité puisqu'il incombe au responsable de traitement de s'assurer du respect de la réglementation. Seuls sont donc soumis à la CNIL pour autorisation les traitements les plus sensibles, pour lesquels l'instruction de la CNIL permet de garantir que ces traitements sensibles satisfont aux plus hautes exigences de protection des données des participants aux recherches promues par l'AP-HP, préoccupation partagée par la CNIL et l'AP-HP.

Pouvez-vous nous parler d'un projet de recherche pour lequel l'accompagnement de la CNIL vous a semblé particulièrement utile ?

En mai 2021, dans le cadre d'un concert expérimental, l'AP-HP a conduit un projet de recherche intitulé SPRING, dont le but était d'évaluer les risques de transmission du virus SARS-CoV-2, lors d'un concert à grande échelle en configuration debout, non distancié, dans une salle fermée. L'organisation d'un tel projet, dans des délais extrêmement courts, constituait un réel challenge sur le plan réglementaire. En termes de réglementation informatique et libertés, les sujets sensibles étaient nombreux : un site de pré-inscription en ligne, les coordonnées pour recontacter les participants sélectionnés pour le concert, la vérification des résultats PCR négatifs, le recours à la technologie de Datakalab pendant l'expérimentation. Les services de la CNIL ont été particulièrement à l'écoute et constructifs pour rendre cela possible dans des délais extrêmement contraints, tout en garantissant le respect des droits des participants en matière de protection des données.

ANTICIPER, innover et développer la réflexion éthique

Anticiper et innover représentent une des missions principales de la CNIL. Elle participe ainsi à la constitution d'un débat de société sur les enjeux éthiques des données, constitue un point de contact et de dialogue avec les écosystèmes d'innovation du numérique (chercheurs, startups, laboratoires) et contribue au développement de solutions technologiques protectrices de la vie privée.

Antoine,
Sociologue du numérique au Laboratoire d'innovation numérique, Direction des technologies et de l'innovation

J'ai rejoint le laboratoire d'innovation numérique de la CNIL (LINC) en 2019 en tant que sociologue du numérique. Le LINC est composé de profils variés, dont les parcours vont de l'expertise technique à celle des sciences sociales, en passant par le design. Son rôle est d'appréhender les innovations, d'explorer les usages numériques, de proposer une réflexion prospective, de mener des expérimentations et de construire des outils à destination de la CNIL, des organismes et des particuliers.

En 2021, nous avons notamment mené un travail pour mieux connaître les personnes adressant des plaintes à la CNIL et comprendre les difficultés qu'elles ont pu rencontrer dans l'exercice de leurs droits. En mobilisant des techniques d'enquête et des concepts issus des sciences sociales, l'objectif était de compléter les analyses juridiques et techniques de la CNIL pour améliorer la protection des données au quotidien et accompagner les personnes dans la mise en œuvre de leurs droits.

Parallèlement, une de mes fonctions est également de contribuer à renforcer les liens avec le secteur académique, notamment en participant à des conférences et en invitant des chercheurs à présenter leurs travaux auprès des agents de la CNIL. L'approche offerte par les sciences sociales constitue, pour la CNIL, une expertise complémentaire pour assurer et renforcer ses missions de régulation.

LA CRÉATION DU SERVICE LINC

La pluridisciplinarité a toujours été un des facteurs du succès du Laboratoire d'innovation numérique (LINC). Depuis sa création en 2016, le LINC est animé par l'équipe Innovation, Études et Prospective de la CNIL et des agents du service de l'expertise technologique. Il s'agit d'un dispositif de réflexion, d'information et de partage sur les tendances émergentes donnant lieu à de nombreuses publications. Il contribue également à des expérimentations et au développement d'outils (CookieViz, logiciel PIA[32], etc.), à l'étude des nouveaux défis techniques et à l'impact du design.

En mai 2021, le LINC est devenu un service à part entière de la CNIL, rattaché à la direction des technologies et de l'innovation. Il regroupe désormais des profils très divers : chargés d'études prospectives, designers, sociologues et ingénieurs qui collaborent quotidiennement autours de différents projets.

Les missions du LINC s'articulent autour de trois actions :

- **l'anticipation :** au travers d'ateliers prospectifs qui permettent une ouverture à de nouveaux enjeux, d'analyser de nouvelles technologies, d'étudier de nouveaux usages ;
- **l'échange :** pour être à l'écoute des différents écosystèmes d'innovation (académique, startup, associatif) et notamment bénéficier du point de vue de chacun. Ces échanges peuvent se dérouler de façon informelle (par exemple lors de séminaires de recherche interne) ou, plus officiellement, lors de conférences organisées par la CNIL ;
- **l'expérimentation :** qu'il s'agisse de développer des outils techniques, des nouvelles modalités d'échanges ou de design, les expérimentations permettent des tests des preuves de concept (ou *proof of concept* – PoC en anglais) en interne ou en externe.

Les projets conduits en 2021

En 2021, le LINC a travaillé à l'amélioration de l'outil CookieViz (voir focus page 66) et son adaptation en extension de navigateurs. Différents projets sont en cours d'élaboration. Par ailleurs, dans la lignée des recommandations faites dans son cahier Innovation et Prospective *Scènes de la vie numérique*, le LINC a réalisé une enquête sociologique auprès des personnes qui contactent la CNIL. Sur la base de ces résultats, la CNIL travaille également à la conception d'outils permettant de faciliter l'exercice des droits.

Le LINC a également mené des études sur les incitations économiques des responsables de traitements à se mettre en conformité.

À venir en 2022

En 2022, le LINC s'intéressera à la chaîne de la donnée captée via les applications mobiles. Tout d'abord, il analysera et mettra en avant des outils permettant d'analyser des applications avant d'étudier la diffusion et la revente des données collectées depuis les applications mobiles. Cette étude permettra de mettre en lumière la chaîne de la donnée, de sa collecte à sa réutilisation.

Le LINC poursuivra également l'étude des « *dark patterns* » en analysant les bandeaux cookies ainsi que les autres types de services qui influent sur le choix des utilisateurs.

Enfin, une série d'ateliers sera organisée avec des syndicats, des associations et des développeurs dans le cadre du partenariat pour un gouvernement ouvert.

LES PARCOURS DU DROIT EN MATIÈRE DE PROTECTION DES DONNÉES

En avril 2021, la CNIL a publié son 8e cahier Innovation et Prospective, *Scènes de la vie numérique,* qui propose une réflexion sur la protection des données des individus au quotidien.

Cette publication comprend une analyse des plaintes reçues par la CNIL, mettant en évidence quatre situations principales conduisant les individus à se mobiliser 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 ; et enfin
- concernant leur inscription dans des fichiers nationaux (accidents bancaires, antécédents judiciaires).

Cette analyse issue des plaintes reçues par la CNIL a mis en évidence les trois étapes que doivent franchir les personnes pour transformer une expérience individuelle en un litige pour lequel ils vont mobiliser leurs droits :

- l'infrastructure de données doit être rendue visible ;
- la personne se considère comme une victime du traitement de données ; et
- elle doit être dans une situation sociale asymétrique qui l'empêche de résoudre le problème par elle-même.

32 « Outil PIA : téléchargez et installez le logiciel de la CNIL », cnil.fr
33 « Cahier IP8 : Scènes de la vie numérique - Une exploration du rapport quotidien à la protection des données et de la vie privée », 13 avril 2021, linc.cnil.fr

Pour compléter ces premières analyses sur l'exercice des droits du point de vue des personnes, le LINC a conduit au printemps 2021 une enquête auprès des plaignants s'adressant à la CNIL. L'objectif était de mieux cerner le profil socio-économique de ces personnes et de comprendre ce qui les a conduit à exercer leurs droits concernant leurs données personnelles.

284 personnes, soit environ 20 % des plaintes reçues entre mars et avril 2021, ont répondu au questionnaire proposé à l'issue du formulaire de plaintes en ligne. Cette enquête quantitative a été complétée par la réalisation d'entretiens qualitatifs, par téléphone, avec les personnes volontaires. 105 entretiens téléphoniques de 15 à 60 minutes ont ainsi été menés par l'équipe du LINC.

Qui est le plaignant type ? Un homme, diplômé et cadre

Cette enquête statistique permet de dresser le profil majoritaire des plaignants. Ceux-ci sont majoritairement des hommes (62 %), entre 30 et 49 ans (54,2 %), diplômés d'un master ou plus (48,6 %). **Le niveau de diplôme et la catégorie socioprofessionnelle semblent bien discriminants dans le recours au droit en matière de protection des données personnelles. Les cadres supérieurs et les diplômés de master et plus sont ainsi surreprésentés parmi les répondants**.

Par ailleurs, la CNIL observe une nette surreprésentation des plaignants habitants en Île-de-France (32,48 % des plaignants alors qu'ils représentent 18,30 % de la population française) ainsi qu'une sous-représentation marquée des plaignants des Hauts-de-France (4,58 % des plaignants alors qu'ils représentent 9 % de la population française).

En croisant ces informations sociodémographiques avec le motif de la plainte, les seules variables significatives sont le niveau de diplôme et la catégorie professionnelle. Le genre, l'âge ou encore la taille de la commune de résidence n'ont pas d'incidence sur le motif de la plainte adressé à la CNIL.

> **« On a beaucoup de droits, ok, mais pour les faire valoir, c'est compliqué. »**
>
> ***Plaignant interrogé par le LINC***

Si les retraités déposent plus de plaintes relatives à la prospection commerciale que la moyenne (25 % contre 15 %), la surveillance sur le lieu de travail est le seul motif de plainte pour lequel la surreprésentation d'un groupe social est statistiquement significative. Les ouvriers déposent 7 fois plus de plaintes relatives à la surveillance au travail que l'ensemble de la population, alors que les cadres en adressent 5 fois moins.
Si la représentativité parfaite du corps social dans l'exercice des droits n'est pas attendue, ce manque de diversité interroge. **Qu'est-ce qui explique ces inégalités sociales dans le recours aux droits de protection des données personnelles ?**

Tout d'abord, la notoriété de la CNIL diffère selon l'âge, la profession et le niveau de diplôme. En outre, le profil particulier des plaignants peut également s'expliquer par les différences socialement marquées en équipements et pratiques numériques. Selon le baromètre du numérique 2021[34], le sentiment de manquer de maîtrise ou de compétences dans l'utilisation des outils numériques varie selon le niveau de diplôme : 33 % des non-diplômés ne maîtrisent pas suffisamment ces outils, contre 8 % seulement des diplômés du supérieur. Une autre explication à cette inégalité réside dans les différences de représentations et pratiques relatives à la protection des données au sein des divers groupes sociaux. Si le souci de la protection des données et de la vie privée est partagé dans toutes les classes sociales, le baromètre du numérique pointe que les cadres et les professions intellectuelles sont légèrement plus précautionneuses dans leurs pratiques effectives, ce qui peut conduire à un recours plus important aux droits par ces groupes sociaux.

Enfin, les inégalités sociales face aux droits ne sont pas spécifiques à la protection des données personnelles. Les caractéristiques sociales des personnes, leur dotation inégale en capitaux économiques, scolaires ou symboliques, sont des variables qui expliquent les différences d'accès au droit, au langage juridique et aux subtilités des procédures.

Les entretiens menés avec les plaignants témoignent en effet des difficultés et obstacles que rencontrent les personnes dans l'exercice de leurs droits. **Un certain nombre d'étapes, par lesquelles les personnes doivent passer avant de s'adresser à la CNIL, peuvent être identifiées : parvenir à contacter l'entreprise, attester de son identité, dépasser les obstacles matériels de la procédure, investir un temps conséquent, connaître la CNIL**, se constituer un dossier de preuves et, enfin, adresser sa plainte à la CNIL. Chacune de ces étapes peut conduire les personnes à se résigner et abandonner le processus d'exercice de leurs droits. À l'inverse, exercer ses droits conduit à un apprentissage progressif des procédures et des techniques. Une fois ce « capital procédural » constitué, certains plaignants deviennent des *« repeat players »*[35] ayant l'habitude des procédures et tirant davantage profit du droit que les *« one shooters »* qui y ont un recours occasionnel. Ils exercent alors plus fréquemment leurs droits de protection de leurs données personnelles. Sur les 284 plaignants ayant répondu à notre questionnaire, plus qu'un quart d'entre eux (27 %) avait déjà adressé une plainte à la CNIL.

Ces difficultés rencontrées par les personnes dans l'exercice de leurs droits se justifient, souvent, par de « bonnes raisons organisationnelles » pour les organismes. Le traitement des demandes exige de mettre en place des procédures pour s'assurer de l'identité du demandeur, faciliter leur traitement et respecter des mesures de sécurité des données personnelles. Au sein des organisations, la demande de droits doit passer à travers

34 « Baromètre du numérique, édition 2021 » (PDF, 3,6 Mo), arcep.fr
35 « « Pourquoi c'est toujours les mêmes qui s'en sortent bien ? » : réflexions sur les limites de la transformation par le droit », Droit et société 2013/3 n°85, cairn.info

des circuits de validation et des chaînes de traitement plus ou moins formalisées. Toutefois, certaines entreprises jouent sciemment sur ces difficultés pour entraver l'exercice des droits. Or, comme le rappelait une des personnes interrogées, « il devrait être aussi simple de supprimer un compte que de le créer ».

Dans son travail de contrôle, la CNIL analyse les processus d'exercice des droits : elle peut être amenée à sanctionner les entreprises en cas de parcours de droit volontairement sinueux, conduisant à l'absence de droits effectifs pour les personnes.

DONNÉES ET MOYENS DE PAIEMENT : LE POINT SUR LES PRINCIPAUX ENJEUX ÉCONOMIQUES, JURIDIQUES ET SOCIÉTAUX

Les données de paiement, des actifs stratégiques

Paiement sans contact, porte-monnaies électroniques, cryptomonnaies : les opérations de paiement du quotidien sont aujourd'hui au centre de trois révolutions, que la pandémie n'a fait qu'accélérer :

- technologique, avec l'arrivée de nouvelles solutions de paiement en ligne et le déclin des paiements en espèces ;
- concurrentielle, avec l'irruption dans le domaine des grands services du numérique et des acteurs Fintechs aux côtés des banques ; et
- réglementaires, avec l'entrée en vigueur récente de plusieurs législations qui doivent parfois s'articuler.

Comme l'illustre le recours à l'authentification forte, le recours à tel ou tel moyen de paiement soulève d'importantes questions en matière de vie privée et de protection des données personnelles. En effet, les données de paiement peuvent permettre de tracer des activités personnelles ou de cerner les comportements des personnes. L'anonymat des transactions, les transferts internationaux de données, les risques associés à la numérisation croissante des paiements, les futures monnaies numériques, sont autant de questions clés pour les entreprises, comme pour les personnes.

Cependant, les paiements et les enjeux qui y sont associés sont méconnus du grand public. Domaine complexe, mettant en jeu des acteurs multiples, **sa bonne compréhension est pourtant un préalable à l'établissement d'une relation de confiance dans les usages innovants**. De même, pour les professionnels assujettis au RGPD, il y a un besoin de sécurité juridique sur certains points d'application de cette réglementation.

Un Livre blanc pour comprendre et accompagner

Dans ce contexte, la CNIL a souhaité apporter des éclairages sur les principaux enjeux économiques, juridiques et sociétaux des données et des moyens de paiement, en publiant en octobre 2021 un nouveau Livre blanc[35] apportant mises en perspective, synthèses et pistes de travail. Cette publication s'adresse :

- **au grand public :** pour une meilleure compréhension des enjeux de vie privée relatifs aux données et moyens de paiement ;
- **aux professionnels :** pour des développements sur les points de vigilance de la CNIL en la matière, ainsi que des priorités qu'elle souhaite se donner en termes d'accompagnement.

Intitulé « Quand la confiance paie », le Livre blanc aborde des sujets d'actualité très variés : du jeu d'acteurs avec des dynamiques concurrentielles nouvelles à la circulation internationale des données de paiement - enjeu de souveraineté pour l'Europe - en passant par la question de l'anonymat et de l'usage des espèces, les nouveaux risques nés de la numérisation croissante des opérations de paiement, les enjeux du futur euro numérique préparé par la Banque centrale européenne, la déclinaison concrète des grands principes du RGPD dans le domaine des paiements, etc.

Ce Livre blanc, réalisé après une consultation publique, est pour la CNIL la première étape d'une feuille de route d'accompagnement des professionnels dans ce domaine. Elle structurera les travaux nationaux pour les années à venir. La CNIL entend travailler en partenariat avec les autres régulateurs concernés et en s'adaptant aux besoins du terrain. En particulier, elle appelle les professionnels (banques, commerçants, prestataires) à s'organiser pour mettre au point un code de conduite RGPD.

35 « La CNIL publie un nouveau Livre blanc sur les données et moyens de paiement », 6 octobre 2021, cnil.fr

Enfin, la CNIL souhaite développer un cadre de référence, en matière de conformité au RGPD, pour l'ensemble des acteurs du domaine et ainsi contribuer à l'égalité concurrentielle sur le marché français et à la conformité de tous les acteurs de la chaîne des paiements.

LES 8 MESSAGES CLÉS

1
Préserver un espace d'anonymat et le libre choix du moyen de paiement

2
L'euro numérique : « *privacy by design* » ?

3
Le paiement sur mobile : anticiper sa généralisation à terme

4
Fintechs et innovation : le RGPD comme atout de confiance

5
Points d'attention RGPD : RT/ST, minimisation, limite des finalités, fraude

6
Sécurité et tokenisation des données de paiement

7
Vers la localisation des données de paiement en Europe ?

8
European Payments Initiative **(EPI) : la conformité RGPD comme marqueur**

La parole à Maya ATIG

Directrice générale de la Fédération bancaire française

Quel regard la profession bancaire porte-t-elle sur les évolutions récentes en matière de paiements, sur lesquelles la CNIL est revenue dans son dernier Livre blanc ?

La profession bancaire a toujours intégré des innovations dans ses offres afin de répondre à l'évolution des comportements des clients, en particulier dans le domaine des paiements : transactions en temps réel, paiement mobile, sans contact, renforcement de la sécurité… La sécurité des données financières constitue un défi permanent pour tous, banques comme clients. L'investissement pour assurer la sécurité cyber et financière n'est pas négociable ! Les Français ne s'y trompent pas ; comme le révèle l'étude IFOP annuelle sur les attentes à l'égard des banques, c'est à notre profession que les Français dans leur très grande majorité (70 %) font confiance en matière de sécurisation de leurs données personnelles, loin devant les GAFA.

Que va apporter ce Livre blanc de la CNIL à vos réflexions et travaux ?

Compte tenu de l'essor des usages numériques et du commerce en ligne, le sujet de la protection et du partage des données clients est sans cesse travaillé. Le Livre blanc rappelle les différents enjeux à concilier, éclaire sur les spécificités des paiements et pose les bonnes questions. Pour nous, l'intérêt légitime est applicable dans le cadre de l'utilisation des données de paiement, notamment à des fins de lutte contre la fraude ou de marketing.

Comment la Fédération bancaire française peut-elle contribuer à la feuille de route d'accompagnement que s'est donnée la CNIL ?

La FBF salue la volonté de la CNIL de se doter d'une feuille de route favorisant la connaissance de la réglementation et des risques pour les citoyens, l'accompagnement des acteurs de l'écosystème dans la conformité au RGPD et la cohérence de l'ensemble de l'action publique.

Dans le cadre de cette feuille de route, le principe « mêmes activités, même risque, même régulation et même supervision » doit s'appliquer afin de maintenir un haut niveau de résilience au niveau européen. Notre objectif est de mettre en place un cadre équilibré pour une égalité des conditions de concurrence (le fameux « level playing field ») en termes de sécurité et de conformité RGPD.

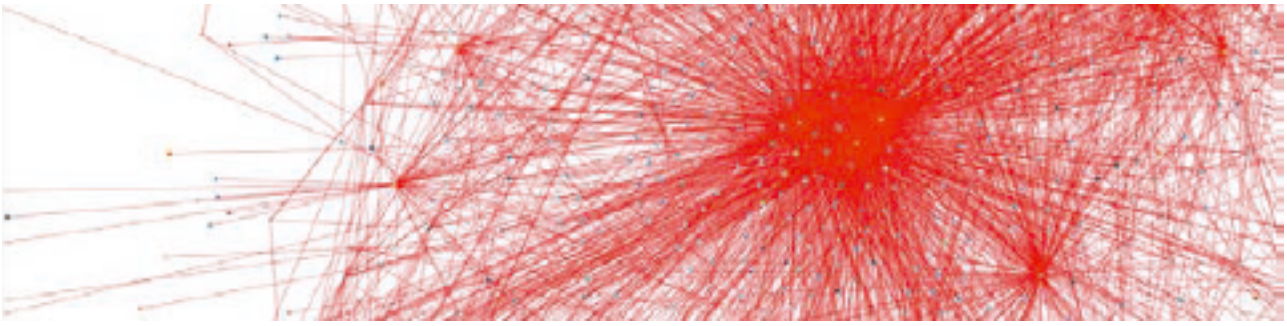
Dans cette optique, une action cohérente et coordonnée de différentes juridictions est nécessaire et pourrait se faire via un dialogue renforcé entre les différents régulateurs, comme proposé par la CNIL. La FBF peut apporter à la CNIL sa vision sur les nouveaux risques liés aux opérations bancaires.

Sur un autre plan, la CNIL entreprend une démarche pédagogique à destination de l'ensemble des acteurs des paiements (banques, clientèles particuliers et entreprises, institutions publiques…) afin de sensibiliser aux enjeux de la sécurisation des données. La FBF apporte tout son soutien à cette idée, et agit déjà fortement : outre toutes les actions des banques en direction de leurs clients, il existe un programme d'éducation financière « Les clés de la banque » qui informe tous les publics, notamment en matière de cybersécurité, pour accompagner chacun dans ses pratiques quotidiennes.

LES OUTILS DÉVELOPPÉS PAR LA CNIL POUR ACCOMPAGNER LA MISE EN CONFORMITÉ ET SENSIBILISER

En 2021, la CNIL a poursuivi le développement d'outils à destination du grand public et des développeurs. Ainsi, elle a publié en décembre **une mise à jour majeure de son guide à destination des développeurs** en y ajoutant de nouvelles recommandations.

La CNIL élabore également des outils permettant de sensibiliser les éditeurs et les internautes au suivi sur le web tel qu'un outil de gestion des cookies et une nouvelle version de son logiciel CookieViz (voir focus).



FOCUS

Global Privacy and Data Protection Awards 2021 : la CNIL récompensée pour son logiciel et les analyses de CookieViz 2.0

CookieViz est un logiciel développé par le Laboratoire d'innovation numérique de la CNIL (LINC). Il permet de visualiser les cookies déposés depuis des domaines tiers lors de la navigation sur un site web. Son code source est librement accessible et peut être enrichi par les développeurs.

Fin 2020, la CNIL a mis à jour ce logiciel et a publié un observatoire sur l'usage des cookies par les sites avec les plus fortes audiences en France. Ces travaux ont été conduits parallèlement à l'adoption des lignes directrices et de la recommandation de la CNIL sur les cookies et autres traceurs.

Cookieviz a ainsi permis de détecter les cookies déposés sur la première page vue par un internaute. Sur la base de ces résultats et pour les sensibiliser aux risques encourus en cas de non-conformité, la CNIL a décidé d'adresser un courrier à une sélection de sites web qui déposent des cookies provenant de plus de 6 domaines tiers sans consentement préalable des utilisateurs.

Cette démarche s'inscrit dans le cadre des missions d'accompagnement et de conseil de la CNIL. L'objectif était d'inciter les organismes publics et privés à procéder rapidement à un audit de leurs sites web et applications mobiles afin d'engager, si nécessaire, des actions permettant d'informer les internautes sur le dépôt de cookies et de recueillir leur consentement.

Cette initiative a été récompensée le 20 octobre 2021 lors de la 43e Assemblée mondiale sur la protection de la vie privée accueillie par l'Institut national pour la transparence, l'accès à l'information et la protection des données personnelles (INAI), autorité mexicaine de la protection des données.

AIR2021 : ENTRE PARTAGE ET PROTECTION, QUELLE ÉTHIQUE POUR L'OUVERTURE DES DONNÉES ?

Le lundi 8 novembre 2021 s'est tenu l'évènement de la CNIL « avenirs, innovations, révolutions », qui portait cette année **sur le thème de l'ouverture et du partage des données**. Tous les interlocuteurs de la CNIL étaient invités à prendre part à ce débat éthique dont l'organisation trouve son origine dans la loi pour une République numérique de 2016. Au total, **plus de 1 200 personnes étaient réunies, physiquement et en ligne**. Parmi elles, une grande diversité d'acteurs du milieu scientifique, du secteur privé et des administrations, ainsi que les réseaux d'éducation au numérique, les autorités de régulation compétentes et le grand public.

Des expertises terrain, politiques et scientifiques pour appréhender ce thème au travers du prisme de l'éthique

Cet évènement a montré, grâce à la qualité des interventions, l'intérêt majeur de l'ouverture et de la réutilisation des données (transparence de la vie publique, enjeu d'amélioration des politiques publiques, meilleure information des citoyens etc.), en même temps que des risques réels pour la protection des données personnelles avec une difficulté particulière à anonymiser ces données.

- Après une ouverture de l'évènement par Marie-Laure Denis, présidente de la CNIL, **Amélie de Montchalin**, la ministre de la Transformation et de la Fonction publiques, a tout d'abord présenté la stratégie gouvernementale en matière d'ouverture des données.
- **Axelle Lemaire,** ancienne secrétaire d'État au numérique, et **Éric Bothorel** (voir l'entretien page suivante), député des Côtes-d'Armor en charge du rapport sur la politique publique de la donnée, sont revenus sur la structuration progressive du cadre règlementaire français.
- **Malte Beyer-Katzenberg**, de la Commission européenne, a poursuivi en présentant les discussions en cours à l'échelle européenne dans le cadre du *Digital Governance Act*.
- **Éric Salobir**, du Conseil national du numérique, a fait le lien entre l'évolution du glissement sémantique des « données d'intérêt général », vers des données dites « altruistes », et l'apparition d'une nouvelle « morale » européenne de la donnée.
- **Stéphane Gigandet**, le fondateur d'Open food facts, une base de données collaborative et ouverte, a ensuite partagé son expérience, exemple de commun numérique.

Une table ronde a également porté sur l'impact de l'épidémie de COVID-19 sur les pratiques d'ouverture de données dans le champ de la santé. Elle a réuni **Nathalie Mesny**, de l'association de patients Renaloo, **Martin Daniel**, à l'origine de Covidliste et **Julien Marchal**, co-directeur de l'Innovation de l'Agence régionale de Santé d'Île-de-France.

Enfin, un dernier temps de réflexion a été consacré à l'approche méthodologique nécessaire de la donnée. Le chercheur **Yves-Alexandre de Montjoye** a détaillé les enjeux d'anonymisation et de pseudonymisation, tandis qu'**Anne Bouverot** de la fondation Abeona est revenue sur les risques de discriminations liés à l'intelligence artificielle. **Pierre Romera**, CTO de l'*International Consortium of Investigative Journalists* a détaillé l'importance de la data dans les nouvelles pratiques journalistiques et **Caroline Goulard de Dataveyes** a terminé la journée par un moment inspirant de datavisualisation.

Le lancement de nouveaux travaux sur l'ouverture et le partage des données

L'évènement air 2021 a mis en lumière la nécessité de clarifier le cadre juridique au regard des exigences et des possibilités offertes par le RGPD. Cette clarification est d'autant plus indispensable aujourd'hui qu'une ouverture plus large des données est prônée tant au niveau national qu'au niveau européen.

En France, quatre ans après la création du service public de la donnée par la loi du 7 octobre 2016 pour une République numérique, le rapport de la mission Bothorel, rendu le 11 décembre 2020 pose le constat général de **la nécessité d'une ouverture plus large des données publiques et fait des propositions concrètes pour permettre cette ouverture**. Au niveau européen, la directive 2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public donne une nouvelle impulsion au mouvement de l'*open data*, mouvement que les pro-

FOCUS

Revoir l'évènement air 2021

Dans la continuité de cet évènement, la CNIL a publié, le 11 mars 2022, le cahier air2021, qui revient sur les principaux échanges de cette journée de débat .

La rediffusion de l'évènement air2021 est également disponible sur le site web de la CNIL : cnil.fr/air2021.[36]

jets européens relatifs au *Data Governance Act* et au *Data Act* devraient encore accélérer.

Cette accélération ne peut toutefois se faire que dans un cadre respectueux de la protection des données et la CNIL comme la CADA sont très souvent saisies des interrogations des différents acteurs sur l'équilibre à respecter entre ouverture et protection. Les deux autorités ont déjà commencé à travailler sur ce sujet dans le cadre du Guide commun sur l'*Open Data*, publié en 2019, mais un approfondissement de ces travaux est aujourd'hui indispensable.

C'est la raison pour laquelle **Marie-Laure Denis, la présidente de la CNIL a annoncé à l'occasion de l'évènement air2021 la création d'un groupe de travail interne sur l'ouverture et le partage des données**. Piloté par Anne Debet, membre du Collège de la CNIL, il aura pour mission d'aboutir, en partant de cas très concrets, à la rédaction d'un guide et de fiches pratiques à l'intention tant des diffuseurs que des réutilisateurs des données. Ces productions, co-créées avec la CADA, seront soumises à la consultation pour contribuer à créer davantage de prévisibilité et de sécurité juridique pour les acteurs économiques.

La parole à Éric BOTHOREL

Député des Côtes-d'Armor en charge du rapport sur la politique publique de la donnée

Quelles ont été les grandes étapes de l'ouverture des données en France ?

Derrière ces enjeux de libération de la donnée, il peut aussi y avoir un sujet polémique ou mal interprété. Mais nous avons tout à gagner à mettre à disposition la DATA ! Pourquoi ? Parce qu'en rendant public un grand nombre de données, on crée les conditions d'un débat très large, qui empêche de se saisir d'éléments non publiés pour déformer la réalité. Par ailleurs, nous l'avons vu avec la pandémie, il est important d'enrichir les données publiques avec les données privées. Superposer les données entre elles a permis aux puissances publiques de mieux comprendre l'impact du COVID-19 sur la population.

Comment définir les données d'intérêt général ?

Tout peut être qualifié d'intérêt général. Les enjeux sanitaires et environnementaux qui nous attendent vont mobiliser des jeux de données très différents : météo, automobile… On ne peut pas savoir à l'avance quels jeux de données seront indispensables. Pour moi, permettre à la puissance publique de réquisitionner des données qu'elle qualifie « d'intérêt général », c'est prendre le risque de nier les réalités économiques de ceux qui produisent et collectent cette donnée. Il faut clarifier ce « droit à la réquisition » de la donnée, comme on l'a fait pour les biens et services. Demain, nous aurons besoin de HUBS sectoriels (agriculture, santé…) qui soient pensés avec de l'interopérabilité. On ne peut plus réfléchir en silo, ni de façon verticale, tout comme on ne peut plus ignorer ce qui se fait ailleurs. L'interopérabilité sera déterminante pour permettre de servir les besoins de la population.

Interview extraite des cahiers air2021

L'ANALYSE DE LA CNIL

INTELLIGENCE ARTIFICIELLE : LA NÉCESSITÉ DE TRACER DES LIGNES ROUGES ET D'ACCOMPAGNER LES NOUVEAUX USAGES

Depuis plusieurs années, le déploiement de technologies d'intelligence artificielle (IA) s'est très largement intensifié. Sortant des laboratoires, ces nouvelles approches ont bouleversé les façons de faire et posent des questions cruciales, nouvelles et complexes, en particulier en termes de protection des données. En effet, certains des grands principes de la loi Informatique et Libertés et du RGPD sont mis en tension par les présupposés fondateurs de l'IA. La CNIL mène donc d'importants travaux[37] afin de préciser la manière d'assurer la conformité des traitements de données recourant à ces systèmes tout en prenant part aux discussions sur le futur règlement européen consacré à l'IA en cours d'élaboration.

Se poser les bonnes questions pour assurer une conformité au RGPD.

Respect des principes de finalité et de minimisation, définition de durées de conservation des données, information des personnes concernées et exercices de leurs droits, cas des systèmes d'IA apprenant de façon continue, etc. les questions posées par l'application de la règlementation aux systèmes d'IA sont nombreuses. Forte de son expérience de régulateur à 360°, la CNIL a déjà eu l'occasion de se positionner sur un certain nombre d'entre elles et d'apporter des éléments de réponse dans les domaines de la santé, des affaires régaliennes, du recrutement, ou encore de la biométrie.

À la suite de ces travaux, et afin de permettre aux organismes d'évaluer par eux-mêmes la maturité de leurs systèmes d'IA au regard du RGPD et des bonnes pratiques dans le domaine, la CNIL a élaboré une grille d'analyse des systèmes d'IA. Il s'agit d'inviter les organismes prévoyant de mettre en place un traitement utilisant des technologies d'IA, ou ayant déjà initié cette démarche, à se poser les questions en matière de données personnelles et d'éthique qui leur permettront d'assurer leur conformité au RGPD.

37 « Intelligence artificielle », cnil.fr

FOCUS

Les nouvelles publications du LINC

Les systèmes d'IA engendrent des risques de sécurité spécifiques en comparaison avec des systèmes d'information classiques. En effet, les nouvelles capacités introduites par l'apprentissage automatique (*machine learning*) augmentent la « surface d'attaque » de ces systèmes en introduisant de nombreuses (et nouvelles) vulnérabilités. Le LINC propose un triptyque d'articles visant à :

- présenter les attaques pouvant être menées sur un système d'IA,
- détailler comment mener une analyse de risque sur un système d'IA prenant en compte les enjeux de sécurité et de protection des données,
- donner les bonnes pratiques pour la sécurisation d'un système d'IA.

Les équipes du LINC se sont également entretenues avec des chercheurs travaillant à la croisée des sujets d'IA et de protection de la vie privée. Reconnus internationalement, Nicolas Papernot, Catuscia Palamidessi, Aurélien Bellet et Marc Tommasi présentent leurs travaux de recherche respectifs et livrent leur sentiment sur l'évolution de la prise en compte des impératifs de protection des données dans le domaine de l'apprentissage automatique.

La CNIL suit également avec grand intérêt le développement des technologies d'IA protectrices de la vie privée. Dans le cadre de son « bac à sable » données personnelles 2021, la CNIL a ainsi eu l'occasion d'accompagner le CHU de Lille dans le cadre de la mise en œuvre de méthodes d'apprentissage fédéré (*federated learning*) appliquées aux études cliniques. Cette technique permet de réaliser l'entrainement de modèles d'IA de façon distribuée sans nécessiter la circulation des données. Un avantage de poids en faveur de la confidentialité !

Un règlement européen pour l'IA

La Commission européenne a adopté, le 21 avril 2021, une proposition de règlement sur l'IA[38]. Celle-ci suit une approche fondée sur les risques, différenciant les utilisations de l'IA qui crées un risque inacceptable pour les valeurs de l'Union européenne et les droits et libertés fondamentaux, un risque élevé, un risque limité et un risque faible ou minime.

La liste des pratiques interdites comprend tous les systèmes d'IA dont l'utilisation est considérée comme inacceptable car contraire aux valeurs de l'Union. Il s'agit des dispositifs ayant un potentiel important de manipulation des personnes par des techniques subliminales, de la notation sociale basée sur l'IA effectuée par les autorités publiques, et de l'utilisation de systèmes d'identification biométrique à distance « en temps réel » dans des espaces accessibles au public à des fins de contrôle du respect de la loi. Des règles spécifiques devant principalement être mises en œuvre par le fournisseur du système d'IA sont définies pour les systèmes qui crées un risque élevé pour la santé et la sécurité ou les droits fondamentaux des personnes physiques. Ces règles doivent aussi être accompagnées de procédures d'évaluation de la conformité. Les usages à faible risque, quant à eux, ne sont soumis qu'à des obligations de transparence.

Au niveau national, les États membres devront désigner une ou plusieurs autorités nationales compétentes et, parmi elles, l'autorité de contrôle nationale disposant d'un pouvoir de sanction afin de veiller au bon respect de ces règles. Au niveau de l'Union, la proposition prévoit la création d'un comité européen de l'intelligence artificielle (CEIA) composé de représentants des autorités de contrôle nationales et de la Commission européenne.

Les fournisseurs de certains systèmes d'IA auront une obligation de surveillance post-commercialisation et de transmettre, aux autorités de surveillance du marché, des rapports et enquêtes sur les incidents et dysfonctionnements liés à leurs systèmes. Le règlement européen pour l'IA ne sera toutefois pas adopté définitivement avant la fin 2022.

38 « Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle », eur-lex.europa.eu

FOCUS

L'avis du CEPD sur le règlement IA

À l'invitation de la CNIL, le Comité européen de la protection de données (CEPD) et le Contrôleur européen de la protection des données ont publié un avis conjoint sur le projet de règlement[39].

Les autorités de protection des données ont salué la volonté de la Commission européenne de préciser les usages interdits afin de construire une IA éthique et de confiance au sein de l'UE.

Cependant, compte tenu des risques extrêmement élevés posés par cette technique, les autorités de protection des données européennes proposent que soient retirées les exceptions visant à permettre l'identification biométrique à distance des personnes dans les espaces publics. L'avis recommande également une interdiction des systèmes biométriques utilisés aux fins de classer les individus dans des groupes basés sur l'ethnicité supposée, le sexe, ou l'orientation politique ou sexuelle. L'utilisation de systèmes d'IA pour déduire les émotions d'une personne physique est par ailleurs considérée comme hautement indésirable et devrait également être soumise à une interdiction de principe. Enfin, les systèmes utilisés pour la notation sociale (« social scoring ») doivent être systématiquement interdits.

La CNIL et ses homologues ont par ailleurs relevé que les systèmes dit « à haut risque » seraient, dans une écrasante majorité des cas, appelés à exploiter des données personnelles, impliquant donc un enjeu majeur d'articulation du règlement sur l'intelligence artificielle avec le RGPD et la directive « Police-Justice »[40].

L'avis conjoint rappelle également que les autorités de protection des données pourraient être chargées de réguler les usages de l'IA, dans la mesure où elles régulent déjà ces dispositifs sous l'angle de la protection des données.

39 « Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) », edpb.europa.eu
40 « Directive « Police-Justice », de quoi parle-t-on ? », 20 février 2019, cnil.fr

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 nombreux travaux et 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.

Délia
Chargée de mission au service des affaires européennes et internationales, Secrétariat général

Le service des affaires européennes et internationales (SAEI) a pour mission principale de développer et de promouvoir, en synergie avec les autres services, la doctrine de la CNIL sur les sujets ayant une dimension européenne et internationale au sein de différentes enceintes dédiées.

C'est ainsi que je suis amenée à représenter la CNIL au sein de sous-groupes thématiques mis en place au sein du Comité européen de la protection des données (CEPD) et à porter ses positions dans le cadre de l'élaboration de la doctrine européenne en matière de protection des données.

Les questions de transferts de données hors de l'Union européenne et des accès par les autorités étrangères aux données stockées sur notre territoire nous occupent aussi, comme le sujet majeur de la coopération européenne en matière répressive.
En effet, la CNIL participe quotidiennement à renforcer l'efficacité des mécanismes de coopération entre autorités de protection des données comme celui du guichet unique. Ce système comporte des avantages importants, d'uniformisation, de prévisibilité et de cohérence. Ainsi, plus de 300 décisions ont été prises et 800 dossiers sont en cours d'instruction. Cependant, nous devons encore améliorer son efficacité, par exemple par la mise en place d'un système renforçant la coordination au plan européen du traitement des cas transfrontaliers. De nombreux défis nous attendent encore, tant sur les questions de fond que sur les aspects de procédure. Mais c'est ainsi que se construit, étape par étape, ce nouveau modèle de gouvernance, unique en son genre. Rendez-vous l'année prochaine avec de nouvelles décisions !

LES COLLABORATIONS DE LA CNIL AVEC SES HOMOLOGUES EUROPÉENS

Le RGPD a instauré un mécanisme inédit afin d'assurer la coopération et la cohérence entre les autorités de protection des données européennes. Si sa mise en place depuis 2018 s'est accompagnée d'une certaine « courbe d'apprentissage » pour les autorités, le système est aujourd'hui opérationnel :

- **Plus de 809 procédures de coopération** ont été mises en œuvre entre 2018 et 2021, à l'issue desquelles près de 300 décisions finales ont été adoptées.
- **La CNIL est « autorité chef de file » pour 94 de ces dossiers** et **« autorité concernée » pour 400 dossiers** (un dossier correspond généralement à une typologie de manquement pour un organisme donné, il peut comporter plusieurs plaintes).

La coopération entre autorités est donc une réalité concrète et quotidienne pour la CNIL et ses homologues. Les échanges sont précieux, tant pour veiller à la cohérence d'application du RGPD, qu'au souci de protection renforcée des citoyens.

Néanmoins, des obstacles à cette coopération entre autorités demeurent. La CNIL poursuit donc son implication au niveau européen afin de remédier, à droit constant, aux difficultés identifiées, en particulier concernant les obstacles procéduraux à la coopération et la définition d'une compréhension commune des concepts et termes clé du guichet unique du RGPD et de la procédure de coopération. La CNIL est ainsi à l'initiative de plusieurs procédures de coopération spécifiques d'assistance mutuelle. En outre, les travaux au sein du Comité européen de la protection (CEPD) des données pour finaliser des lignes directrices sur une approche commune des procédures et des notions clés couvrent ainsi désormais de nombreux aspects liés à la coopération (par exemple les exigences en matière d'objections pertinentes et motivées ou la procédure en matière de résolution des différends devant le CEPD dans le cadre d'un dossier de coopération spécifique[41]).

Par ailleurs, la CNIL s'investit dans plusieurs initiatives pour partager son expérience et son expertise, et pour s'assurer que les plaintes qu'elle a reçues sont traitées avec diligence par ses homologues.

Plus globalement, sur le plan de la doctrine et de la coopération européenne, la CNIL reste également très engagée dans les travaux du Comité européen de la protection des données et a participé à la rédaction de plus d'une trentaine de documents du Comité en 2021, par exemple dans le cadre de la coordination sur les 101 plaintes transmises par l'association noyb concernant les transferts vers les États-Unis de plusieurs opérateurs (voir focus page 45).

DE L'ARRÊT « SCHREMS II » À LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNEE

L'arrêt Schrems II (voir encadré page suivante) est directement lié à la problématique des transferts de données hors de l'Union européenne (UE) mais pose également, en creux, **la question de l'accès par des autorités étrangères à des données protégées par le RGPD.** Ce point soulève de nouvelles questions concernant le recours à des prestataires de services qui, bien que situés dans l'UE, restent soumis au droit américain et doivent permettre l'accès aux données en cas de requête, y compris, en l'absence de transfert vers les États-Unis. Ces analyses ont notamment conduit la CNIL à formuler en 2020, pour certains traitements particuliers, la recommandation de recourir à des sous-traitants soumis aux seules juridictions de l'Union européenne.

Ce sujet de l'immunité aux lois extra-territoriales s'invite dans le débat plus large sur la souveraineté numérique européenne. En effet, dans le cadre de sa stratégie sur le numérique, l'UE souhaite créer les conditions qui permettront à l'Europe de développer et déployer ses propres capacités critiques, de réduire sa dépendance technologique à l'égard des pays tiers, et de renforcer son aptitude à définir ses propres règles et valeurs, comme en témoigne le projet de cloud européen Gaïa-X.

Au niveau national, la stratégie du gouvernement en matière de cloud contribue également à promouvoir la souveraineté numérique européenne. Elle s'articule autour de 3 grands axes.

Un nouveau label cloud de confiance qui doit garantir :
- la sécurité technique (à travers la qualification SecNumCloud de l'ANSSI[42]) ;
- la sécurité juridique des données (notamment l'immunité aux applications extraterritoriales de droit hors UE).

Pour se voir attribuer le label, un service cloud devra remplir les exigences de sécurité SecNumCloud et offrir une localisation et une identité européenne (localisation obligatoire des infrastructures et systèmes en Europe et portage commercial et opérationnel du service par une entité européenne).

41 Article 65, paragraphe 1, a) du RGPD
42 Voir l'interview de Guillaume Poupard, directeur de l'ANSSI, page 94.

- La mise en œuvre de la doctrine « cloud au centre » de l'État[43], dans le contexte de la transformation numérique des administrations publiques et qui deviendra le mode d'hébergement par défaut des projets numériques de celles-ci.
- Des investissements, notamment dans la R&D, et des projets dans le cadre de France Relance (plan économique de la France entre 2020 et 2022 à la suite de la crise sanitaire) et également au niveau européen avec Gaïa-X (projet de développement d'une infrastructure cloud européenne).

Les actions menées par la CNIL

En 2021, la CNIL a mené plusieurs actions, notamment dans le secteur du cloud.

Les « suites collaboratives pour l'éducation » de sociétés américaines

La CNIL a été saisie par la Conférence des présidents d'université et la Conférence des grandes écoles sur l'utilisation des « suites collaboratives pour l'éducation » proposées par des sociétés américaines, **plus particulièrement sur la question des transferts internationaux de données personnelles**.

Dans sa réponse, publiée le 27 mai 2021 sur son site web[44], la CNIL a rappelé la nécessité de mettre en place des mesures supplémentaires ou de justifier le transfert de données au regard des dérogations autorisées par l'article 49 du RGPD[45], à la suite de l'invalidation du *Privacy Shield*.

Par ailleurs, la CNIL a alerté sur les risques d'accès illégaux par les autorités américaines aux données stockées dans l'UE (voir plus haut), tout en prenant en compte les contraintes liées à la crise sanitaire et la nécessité que les établissements concernés assurent la continuité de leurs missions.

DÉFINITION

Du *Privacy Shield* à l'arrêt « Schrems II »

Le *Privacy Shield* (Bouclier de protection des données en français), était un mécanisme d'auto-certification pour les sociétés établies aux État-Unis d'Amérique. Ce dispositif avait été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données personnelles transférées depuis une entité européenne vers des sociétés établies aux États-Unis. Le *Privacy Shield* UE-États-Unis était entré en vigueur le 1er août 2016. **Cependant, la décision d'adéquation de la Commission européenne validant le *Privacy Shield* a été annulée par la Cour de justice de l'Union européenne (CJUE) le 16 juillet 2020** (arrêt dit « Schrems II »). **Il ne constitue donc plus une garantie juridique suffisante** pour transmettre des données personnelles de l'Union européenne vers les États-Unis.

Les autres échanges concernant le cloud

La CNIL a rencontré tout au long de l'année 2021 les acteurs ayant annoncé des projets de **partenariat en matière de cloud de confiance** (OVH/Anthos Google, Bleu (Orange/Capgemini/MicrosoftAzure) et GOTH (Thalès/Google Cloud) dont le développement ne peut se faire sans intégrer la protection des données personnelles et les mesures spécifiques à mettre en place suite à l'invalidation du *Privacy Shield* et écarter tout risque d'accès illégal aux données par des autorités étrangères.

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

Fin 2020, l'Agence de l'Union européenne pour la cybersécurité (ENISA) a lancé une consultation publique sur un projet de certification intitulé *European Cybersecurity Certification Scheme for Cloud Services (EUCS)*. Plusieurs échanges ont eu lieu avec l'ENISA.
Le CEPD lui a adressé un courrier en novembre 2021 indiquant que le niveau d'assurance de ce projet de certification devrait inclure des critères spécifiques pour garantir la protection contre les menaces que représente l'accès par des autorités non soumises à la législation de l'UE et n'offrant pas un niveau de protection des données personnelles essentiellement équivalent à celui garanti par le RGPD, tel que rappelé par la CJUE.
Par ailleurs, dans le cadre de la mise en place d'un cadre d'application coordonné *(coordinated enforcement framework)*[46], le CEPD a décidé de lancer en octobre 2021 sa première action coordonnée sur le thème de l'utilisation des services de cloud dans le secteur public. Cette action, à laquelle participe la CNIL, doit permettre de mieux comprendre le sujet, d'assurer un suivi ciblé au niveau national et européen et, le cas échéant, de prendre les mesures nécessaires à la mise en conformité des acteurs contrôlés.

43 « Le cloud pour les administrations », numerique.gouv.fr
44 « La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche », 27 mai 2021, cnil.fr
45 « Transferts de données hors UE - dérogations pour des situations particulières », cnil.fr
46 Il s'agit pour le CEPB d'organiser une action mobilisant de manière coordonnée les autorités de surveillance sur un sujet précis - « Document du comité européen de la protection des données sur le cadre d'application coordonné en vertu du RGPD », adopté le 20 octobre 2020 (PDF, 139 ko), edpb.europa.eu

FOCUS

Schrems II : les mesures supplémentaires pour respecter le RGPD lors d'un transfert de données

En 2021, la CNIL a continué de participer aux travaux du CEPD sur l'analyse et la prise en compte de l'arrêt Schrems II. Elle a ainsi contribué à la finalisation des recommandations du CEPD concernant les mesures supplémentaires qui peuvent ou doivent compléter les outils de transfert pour assurer le respect du niveau européen de protection des données personnelles[47]. Ces recommandations, qui tirent les enseignements de l'arrêt Schrems II, étaient très attendues. **Elles doivent permettre, en pratique, aux acteurs de se mettre en conformité concernant leurs transferts de données hors UE**.

Ainsi, par exemple, si le chiffrement peut être considéré comme une mesure supplémentaire effective dans certains cas, celle-ci pourrait ne pas être effective pour l'ensemble des transferts vers les États-Unis, notamment si les services fournis impliquent un déchiffrement des données une fois transférées, ou lorsque les destinataires sont directement soumis aux lois américaines en matière d'accès par les services de renseignement (FISA 702, Executive Order 12333).

Ces recommandations ont été reflétées dans des **FAQ et autres documents pratiques publiés par la CNIL**[48]. Ces éléments de réponse pratiques ont vocation à être précisés ou complétés si besoin, en lien avec les homologues de la CNIL avec lesquels des échanges réguliers ont lieu.

Les recommandations du CEPD ont également vocation à être prises en compte dans le cadre du développement de solutions techniques, y compris dans le cadre de la certification de ces solutions, par exemple en matière d'informatique en nuage. C'est le sens du courrier transmis par le CEPD à **l'Agence de l'Union européenne pour la cybersécurité (ENISA)** en novembre 2021.

La CNIL a également eu à répondre à des sollicitations variées concernant la mise en œuvre concrète de cet arrêt, y compris dans le contexte de plaintes. Des décisions seront ainsi adoptées dans le courant de l'année 2022.

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.

RÉGULATION DU NUMÉRIQUE & GOUVERNANCE

Avec ses homologues du CEPD, la CNIL s'est impliquée dans les discussions en cours sur les initiatives législatives européennes en matière de marché unique européen, à savoir la législation sur la gouvernance des données (DGA), la législation sur les services numériques (DSA), la législation sur les marchés numériques (DMA) et la législation sur l'intelligence artificielle (AIA), qui contribueront à renforcer la souveraineté numérique de l'Union.

À la demande de la CNIL, le CEPD et le Contrôleur européen de la protection des données ont notamment produit un avis conjoint sur la proposition de législation sur la gouvernance des données (DGA) qui vise à renforcer la confiance dans le partage de données au sein de l'Union. Cet avis a permis de souligner la nécessité de développer une économie de la donnée fondée sur les valeurs et principes de l'Union, et de rappeler à ce titre que le cadre juridique européen de protection des données personnelles devait rester le fondement du modèle de gouvernance européenne des données. La CNIL, ses homologues et le Contrôleur européen de la protection des données ont également adopté un avis sur la proposition de règlement sur l'intelligence artificielle (voir L'analyse de la CNIL page 68) et se sont félicités de cette proposition

47 « Invalidation du Privacy Shield : les travaux du CEPD », cnil.fr
48 « Transférer des données hors de l'UE », cnil.fr

visant à construire un écosystème européen de l'intelligence artificielle respectueuse des libertés et droits fondamentaux.

Il est indispensable que les co-législateurs assurent la cohérence de ces différents textes avec le cadre juridique européen de protection des données personnelles. Celle-ci permettra de garantir le droit fondamental à la protection des données de façon générale, mais aussi d'assurer la bonne application de ces textes à l'avenir s'agissant des éléments où il pourrait exister des recoupements (transparence, ciblage, conditions de recueil du consentement, évaluation des risques systémiques pour la vie privée, etc.).

L'application de ces nouveaux textes devra également se faire dans le cadre d'une gouvernance intelligente de la régulation, avec la désignation d'autorités compétentes en capacité d'agir sur la base d'une expertise et d'une connaissance pratique des acteurs et enjeux. La CNIL et ses homologues ont ainsi rappelé aux co-législateurs que le Traité sur le fonctionnement de l'Union européenne, et la Charte des droits fondamentaux de l'Union européenne exigeaient que le respect des règles relatives à la protection des données personnelles soit soumis au contrôle d'autorités indépendantes. À cet égard, les différents textes manquent à ce stade d'éléments clairs et précis s'agissant des mécanismes d'inter-régulation entre les nouvelles autorités en charge de la supervision des nouveaux textes et les autorités de la protection des données. La CNIL et ses homologues ont ainsi estimé que les autorités de protection des données devraient être désignées comme autorités de contrôle nationales pour le DGA et le règlement sur l'intelligence artificielle compte tenu de l'enjeu majeur d'articulation de ces textes avec le cadre juridique européen de protection des données.

Ces recommandations favoriseront la cohérence d'action et une gouvernance intelligente et permettront d'atteindre les trois objectifs suivants :

- garantir la protection des droits fondamentaux des personnes dans l'application de la régulation européenne du numérique ;
- assurer la capacité de la CNIL à faire appliquer de façon efficace et effective les principes et normes dégagées dans l'écosystème numérique ;
- assurer la lisibilité de l'environnement réglementaire pour les citoyens et les acteurs économiques concernées qui ne sont pas seulement les GAFAM.

LES GRANDES DÉCISIONS DU CEPD EN 2021

809

procédures de coopération
La CNIL est autorité chef de file pour

94

dossiers
Et autorité concernée pour

400

dossiers

Cette année, le CEPD a adopté deux décisions majeures dans le cadre du mécanisme de la cohérence et du guichet unique :

- la première décision issue de la procédure d'urgence (article 66 du RGPD) à l'encontre de Facebook ;
- la seconde décision contraignante adressée à l'autorité irlandaise concernant un projet de décision à l'égard de WhatsApp.

Une première décision dans le cadre de la procédure d'urgence

En juillet 2021, l'autorité de protection des données de Hambourg a adopté une mesure d'urgence provisoire (article 66.1 du RGPD) à l'encontre de Facebook pour suspendre le transfert de données entre WhatsApp et Facebook. Elle a ainsi considéré que l'urgence était caractérisée et donc qu'elle pouvait agir, sans pour autant être autorité chef de file sur ce dossier. Elle a ensuite demandé au CEPD une décision contraignante d'urgence (article 66.3 du RGPD) prévoyant des mesures définitives sur cette question. Le CEPD a estimé que les conditions de l'urgence n'étaient pas réunies en l'espèce. Par conséquent, il a rejeté la demande de l'Allemagne. Cependant, la décision reconnaît que les éléments présentés permettaient de considérer que sur certains aspects, des infractions au RGPD semblaient constituées.

En conséquence, le Comité a estimé que cette affaire nécessitait des enquêtes complémentaires rapides. Il a donc invité l'autorité irlandaise, la DPC, à mener en priorité une enquête sur WhatsApp et sur Facebook pour déterminer si Facebook agissait en tant que sous-traitant ou en tant que responsable de traitement conjoint. Cette décision était en partie liée à la procédure parallèle de résolution des différends (procédure prévue par l'article 65 du RGPD) qui a abouti quelques semaines plus tard contre WhatsApp.

Une nouvelle décision contraignante adressée à l'autorité irlandaise

Toujours en juillet 2021, le CEPD a adopté sa seconde décision contraignante sur le fondement de l'article 65 du RGPD. Cette procédure concernait les politiques de vie privée de Whatsapp et notamment les modalités d'information des personnes concernées et la transparence de ses politiques de vie privée. Cette décision a enjoint l'autorité irlandaise d'ajouter des manquements à son projet de décision de sanction initiale, de modifier le calcul du montant de l'amende en prenant une assiette plus large et en tenant compte de l'ensemble des manquements (et pas seulement du plus grave), et d'imposer une amende plus élevée tenant compte de tous ces aspects.

Au cours de l'été, l'autorité irlandaise a ainsi adopté une amende de 225 millions d'euros contre la société.

LA CNIL DANS LE MONDE

La 43e réunion de la *Global Privacy Assembly*

Au-delà de l'Union européenne, la CNIL a participé à la 43e réunion annuelle de l'Assemblée mondiale de la vie privée, la *Global Privacy Assembly*, sous la présidence du Mexique, et qui a réuni plus de 80 pays sur des sujets d'intérêt commun en lien avec la protection de la vie privée. À cette occasion, l'Assemblée a adopté cinq résolutions importantes dont deux pour lesquelles la CNIL était co-auteur.

La résolution sur l'encadrement de l'accès par les gouvernements aux données détenues par le secteur privé

Cette résolution est le premier texte international posant des principes pour le respect de la vie privée lorsqu'un gouvernement accède à des données personnelles pour des raisons de sécurité nationale ou de sécurité publique. La CNIL est co-auteur de ce texte, aux côtés de l'autorité du Canada (OPC) et de l'autorité du Japon (PPC). Ce sujet majeur fait l'objet de nombreuses initiatives aux niveaux national et international, en particulier au sein de l'OCDE, du G7 et du G20. Partant du constat qu'il ne peut en effet avoir de libre circulation des données sans confiance, la résolution prône l'application de grands principes pour l'accès des gouvernements aux données personnelles. Cette résolution établit ainsi les conditions permettant de garantir que tout type d'accès légitime d'autorités publiques à des fins liées à la sécurité nationale ou à la sécurité publique s'effectue de manière licite et proportionnée au regard des exigences de préservation de la vie privée et de l'état de droit en général.

La résolution sur la protection des droits numérique des enfants

Cette seconde résolution rappelle l'importance de développer des politiques dédiées à la protection des mineurs, population particulièrement vulnérable mais fortement présente sur internet. Cette protection doit passer par des réglementations adaptées, des campagnes de sensibilisation et d'éducation, ou encore des outils dédiés (par exemple, des interfaces adaptées à l'information des mineurs, ou des outils qui assurent la sécurité des enfants en fonction de leur âge). Forte de ses travaux en la matière (voir page 36), la CNIL est également co-auteur de cette résolution avec l'autorité italienne.

Les autres actions de la CNIL au sein du GPA

La CNIL continue de participer activement à l'animation de ce réseau en assurant la coprésidence de deux groupes de travail (éducation au numérique et éthique : 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 travail se poursuivra en 2022, en se concentrant plus particulièrement sur les outils de transferts.

Une participation active de la CNIL dans les discussions internationales

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 2021 se sont concentrées sur la mise à jour de la Recommandation de l'OCDE sur la protection des enfants dans l'environnement numérique.

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. Dans ce cadre, la CNIL suit avec attention le processus de ratification par la France de la Convention 108+, et participe activement aux différents travaux du comité, notamment l'élaboration de lignes directrices sur l'identité numérique et sur les échanges de données entre autorités publiques à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme.

Pour finir, la CNIL a pu accueillir quelques délégations étrangères, mais de manière limitée du fait du contexte sanitaire. Les contacts bilatéraux ont toutefois pu être maintenus, en attente d'une situation plus favorable qui permettra la reprise de ces échanges si importants.

La parole à Andréa JELINEK

Présidente du Comité européen de la protection des données - CEPD (European data protection board ou EDPB en anglais)

Quelles sont les décisions et étapes clés de l'année 2021 pour l'EDPB ?

En 2021, le CEPD a participé au débat global sur la protection des données et a tenu 380 réunions qui ont permis de faire d'importants progrès sur de nombreux dossiers impliquant une application cohérente de la législation européenne en matière de protection des données au sein de l'Espace Économique Européen (EEE). Au début de l'année 2021, l'EDPB a adopté son programme de travail 2021-2022 qui décline les priorités retenues dans sa stratégie définie pour 2021-2023. Il a également adopté de nombreuses lignes directrices.

Transferts internationaux de données

En 2021, le CEPD a fait une série de contributions importantes pour permettre des flux de données internationaux sécurisés et protecteurs : il a adopté des avis sur les projets de décisions d'adéquations de la Commission concernant le Royaume-Uni – dont il est souligné l'importance qu'elles soient temporaires - et la Corée du Sud, ainsi que sur les nouveaux modèles de clauses-types de la Commission européenne ; il a adopté la version finale de ses recommandations concernant les mesures supplémentaires suite à l'arrêt Schrems II après une consultation publique ; il a également adopté des lignes directrices sur les codes de conduite en tant qu'outils de transferts.

Politique numérique

Le CEPD a adopté, conjointement avec le Contrôleur européen de la protection des données, deux avis communs concernant les projets de règlements sur la gouvernance des données (Data Governance Act - DGA) et sur l'intelligence artificielle. Il a également adopté une déclaration sur le DGA, ainsi que sur le paquet relatif aux services numériques et la stratégie européenne en matière de données. Dans toutes ces contributions, il rappelle que les règles de protection des données sont fondamentales pour créer de la confiance et qu'elles s'appliquent à tout traitement de données personnelles.
Il fournit aussi des recommandations, notamment de confier la supervision aux autorités de protection des données, en consultation avec les autres autorités sectorielles concernées.

Cohérence et application du RGPD

En 2021, le CEPD a adopté 39 avis, 1 décision contraignante et 1 décision dans le cadre d'une procédure d'urgence. Il y a également eu 506 cas transfrontaliers, dont 375 sont issus de plaintes.

La coopération entre autorités fonctionne-t-elle bien ?

De l'expérience du CEPD, le modèle de coopération et de cohérence fonctionne bien. Des douzaines d'échanges ont lieu chaque jour entre les agents des autorités et de nombreux cas sont résolus chaque jour et chaque semaine. Le nombre d'actions répressives a augmenté ces dernières années, et le montant total des amendes imposées par les régulateurs depuis l'entrée en application du RGPD a atteint plus d'1,55 milliard d'euros.

Quelles sont les principales actions que vous entendez prendre collectivement en 2022 ? De quels sujets majeurs allez-vous vous saisir ?

Gouvernance et activités répressives

Les activités répressives au niveau national requièrent du temps et des ressources. En outre, le modèle de coopération doit faire face à d'autres challenges, notamment les différences de législations administratives dans les États membres. Le CEPD se concentre sur les solutions pratiques, pour renforcer les capacités des autorités. De plus, les autorités débattent sur la manière d'améliorer la coopération avec le cadre juridique actuel. Le CEPD a également mis en place un « pool d'experts » support et un cadre commun en matière répressive. Après un débat lors de sa séance plénière de janvier 2022, l'EDPB organisera une importante discussion au printemps.

Lignes directrices

En 2022, l'EDPB continuera à développer de la doctrine, notamment sur la base légale relative aux intérêts légitimes ou l'utilisation des technologies de reconnaissance faciale par les autorités répressives. Il développera également un outil spécifique pour les personnes travaillant dans des TPE/PME.

Dimension globale

La présidente de l'EDPB et les vice-présidents, de même que les membres du Comité, participent à de nombreux échanges internationaux et échanges des bonnes pratiques avec leurs homologues du monde entier, en particulier dans le cadre de la Global Privacy Assembly et du G7.

L'EDPB va également continuer à construire la boîte à outils des mécanismes de transferts vers des pays tiers avec notamment les codes de conduite, les mécanismes de certification, et les arrangements administratifs entre autorités publiques.

Enfin, l'EDPB travaille sur les différents outils permettant la coopération répressive avec les autorités de protection des données de pays tiers, dans l'objectif de développer là aussi une boîte à outils pour la coopération internationale.

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.

Marjorie
Juriste au service des délégués à la protection des données, Direction de la conformité

Le service des délégués, composé de neuf juristes et d'une assistante, est chargé d'accompagner les délégués de tous les secteurs dans leurs missions. Le service est le point de contact privilégié des délégués au sein de la CNIL.

Nous échangeons quotidiennement avec eux au travers de la permanence téléphonique, des demandes de conseil, des réseaux de délégués et des partenaires de la CNIL. Cette proximité nous permet de bénéficier d'une vision globale des sujets et d'une vision terrain, très précieuse pour nous.

Au sein de la direction, le service intervient également sur différents projets en lien avec les services sectoriels : élaboration de nouveaux référentiels, participation aux groupes de travail sectoriels ou thématiques, rédaction de fiches pratiques, etc. Les tâches sont donc très variées !

Notre activité de conseil et d'accompagnement des professionnels est très souvent marquée par l'actualité. Cette année encore, la crise sanitaire a généré de nombreuses interrogations. L'évolution, parfois très rapide, de la réglementation a nécessité d'être réactifs pour apporter des réponses adaptées à nos interlocuteurs.

Cette année 2021 a été aussi celle de la publication du guide DPO dont la rédaction a bénéficié de notre participation à l'élaboration des lignes directrices du CEPD sur le DPO et de trois ans de pratique d'accompagnement des délégués.

Nul doute que les prochains mois seront tout aussi stimulants !
En effet, le service va élargir son offre d'accompagnement courant 2022 : interventions en régions, programme de webinaires, « bac à sable » consacré aux « EdTechs », et accompagnement renforcé de certains acteurs.

L'ACCOMPAGNEMENT DES PROFESSIONNELS

Face à la complexité technique et juridique grandissante des textes relatifs à la protection des données personnelles, **la CNIL a fait le choix, depuis de nombreuses années, d'accompagner les professionnels** des organismes publics et privés dans leur diversité : les pouvoirs publics, les responsables de traitement ou leurs sous-traitants, les associations professionnelles ou encore les fournisseurs de solutions techniques, technologiques et méthodologiques.

Dans son champ d'intervention, **la CNIL a développé des outils prenant de plus en plus finement en compte les besoins des organismes.** Elle a produit de nombreux instruments de droit souple élaborés en concertation avec les acteurs intéressés. Depuis quelques années, la CNIL s'applique ainsi à réaliser des outils directement utilisables par les acteurs tel que son MOOC, des guides pratiques, des packs de conformité, des référentiels, etc[49].

L'année 2021 aura été particulièrement riche en matière d'élaboration d'outils d'accompagnements destinés aux professionnels.

4
référentiels

3
recommandations

2
guides

480
réponses aux consultations publiques[50]

UNE CHARTE D'ACCOMPAGNEMENT

L'accompagnement des professionnels dans leur démarche de conformité est l'une des missions de la CNIL. Dans une logique de transparence, et dans la mesure où ses ressources sont limitées, la CNIL a décidé d'afficher sa politique en publiant une charte d'accompagnement[51] en février 2021.

À qui s'adresse-t-elle ?

Cette charte d'accompagnement s'adresse aux cibles professionnelles de la CNIL, à savoir :

- les responsables de données personnelles ou leurs sous-traitants, ainsi qu'aux associations professionnelles qui les représentent, soumis aux réglementations en matière de données personnelles, qu'ils soient publics ou privés ;
- les fournisseurs de solutions techniques, technologiques ou méthodologiques dont les produits et services sont utilisés pour traiter des données, sans qu'ils soient eux-mêmes soumis directement aux réglementations.

Pourquoi cette charte ?

Avec le RGPD, le premier acteur de la conformité à la réglementation relative à la protection des données est le professionnel lui-même, les traitements de données (sauf pour certaines données sensibles) n'étant plus soumis à autorisation ou déclaration mais au contrôle à posteriori de la CNIL.

La CNIL a choisi de renforcer ses missions de conseil et d'accompagnement des professionnels pour les aider dans leur mise en conformité. Elle met à disposition différents outils (référentiels, recommandations, guides pratiques, modèles, fiches pratiques sur son site web, etc.) et offre, dans la limite de ses ressources, un accompagnement sectoriel et individuel.

Afin que les professionnels puissent avoir une vision claire du périmètre et des modalités de cet accompagnement, la CNIL a décidé d'afficher sa politique en la matière en publiant une charte.

Son objectif : présenter les grands principes et la méthodologie de la CNIL en matière d'accompagnement et fournir aux acteurs concernés des **réponses à leurs questions pratiques** sur le traitement de leurs demandes de conseil, le fonctionnement de la stratégie de « têtes de réseaux », ou encore la confidentialité de leurs échanges avec la CNIL.

Une nouvelle étape dans la politique d'accompagnement de la CNIL

La publication de cette charte s'inscrit dans la stratégie globale de la CNIL, visant à assurer un équilibre entre l'action répressive et l'accompagnement. Elle sera complétée par l'élaboration d'un programme de travail annuel sur les outils de droit souple, afin de donner aux professionnels une visibilité sur ces instruments innovants et leur permettre d'y participer grâce à des consultations publiques.

49 « Les outils de la conformité », cnil.fr
50 « Consultation », cnil.fr
51 « La CNIL publie sa charte d'accompagnement des professionnels », 12 février 2021, cnil.fr

LA CNIL COMPLÈTE SA BOÎTE À OUTILS

En 2021, la CNIL a mis à disposition des acteurs de nombreux outils d'accompagnement. Ils prennent des formes diverses pour s'adapter au mieux aux publics auxquels ils s'adressent et concernent des sujets variés (santé, social, logement, mesures de sécurité etc.).

En 2021, la CNIL a adopté plusieurs référentiels sectoriels[52] et recommandations [53] :

- référentiel relatif à l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes âgées, en situation de handicap et en difficulté ;
- référentiel relatif à la désignation des conducteurs ayant commis une infraction au code de la route ;
- référentiel relatif à la gestion locative ;
- référentiel relatif aux entrepôts de données de santé ;
- recommandation relative à l'exercice des droits par l'intermédiaire d'un mandataire ;
- recommandations provisoires pour le contrôle qualité des essais cliniques pendant la crise sanitaire ;
- recommandation relative aux mesures de journalisation.

La CNIL a également élaboré plusieurs guides :

- un guide de sensibilisation au RGPD pour accompagner les associations ;
- un guide consacré au délégué à la protection des données (DPO) regroupant les principales connaissances utiles et bonnes pratiques pour aider les organismes et accompagner les DPO déjà en poste.

52 « Les autres référentiels », cnil.fr
53 « Lignes directrices et recommandations de la CNIL », cnil.fr
54 « Consultation », cnil.fr
55 « Le secteur de l'assurance », 16 juillet 2021, cnil.fr

DÉFINITION

Les référentiels et recommandations

Les référentiels constituent des cadres de référence qui permettent à un organisme de mettre en conformité un traitement de données spécifique. Ils ont vocation à remplacer les autorisations uniques, normes simplifiées et packs de conformité qui existaient avant le RGPD. Instruments de régulation de droit « souple » essentiels, les référentiels ont vocation à donner davantage de sécurité juridique aux acteurs concernés en les accompagnant dans la mise en œuvre de leurs traitements.
Les recommandations quant à elles, sans être prescriptives ni exhaustives, jouent le rôle de **guides pratiques** destinés à éclairer les acteurs concernés.

INFOSPLUS

Une concertation publique systématique

Afin que ces outils puissent répondre au mieux aux préoccupations concrètes des acteurs, les référentiels et les recommandations sont systématiquement soumis à une phase de consultation publique qui permet à tous, organismes comme particuliers, de faire part de leurs observations sur les projets. Toutes les consultations de la CNIL sont référencées sur son site web[54].

L'ACCOMPAGNEMENT SECTORIEL

Assurance

Le secteur de l'assurance bénéficie, depuis de nombreuses années, d'un accompagnement spécifique de la CNIL compte tenu des enjeux liés aux traitements mis en œuvre, notamment en ce qu'ils impliquent souvent des données de santé. Dans ce cadre, la CNIL anime régulièrement des « clubs conformité » avec les principaux représentants du secteur (France assureurs, le Centre technique des institutions de prévoyance, la Fédération nationale de la mutualité française).

Afin de mettre à jour les principes inscrits dans son pack de conformité assurance de 2014, la CNIL a publié, en juillet 2021, des fiches pratiques pour aider les organismes à comprendre les principaux enjeux en matière de protection des données depuis l'entrée en application du RGPD[55]. Ces contenus reprennent l'essentiel du contenu du guide élaboré par le secteur de l'assurance, en association avec la Fédération française de l'assurance (FFA) : qualification des ac-

teurs, minimisation des données, bases légales, durée de conservation, etc.

Santé

Le 17 novembre 2021, **la CNIL a publié un référentiel sur les entrepôts de données de santé**[56]. Les entrepôts de données de santé sont des bases de données destinées à être utilisées notamment à des fins de recherches, d'études ou d'évaluations dans le domaine de la santé. Leur création peut être soumise à l'autorisation de la CNIL.

Ce référentiel s'inscrit dans une démarche de simplification des formalités dans le secteur de la santé tout en fournissant un cadre juridique et technique adapté aux pratiques et protecteur des données de santé. **Il permet aux organismes voulant mettre en œuvre un entrepôt de données conforme au référentiel de ne pas solliciter d'autorisation préalable auprès de la CNIL :** après vérification de la conformité de son projet d'entrepôt par rapport au référentiel, l'organisme peut déclarer sa conformité auprès de la CNIL.

Le référentiel ne s'applique toutefois qu'aux entrepôts de données de santé reposant sur l'exercice d'une mission d'intérêt public et ne concerne pas les entrepôts de données mis en œuvre par des entreprises privées à des fins de recherche sans exécution d'une mission d'intérêt public.

La CNIL a également publié de nombreux autres contenus visant à accompagner les professionnels de santé dans le cadre des traitements mis en œuvre dans leurs activités quotidiennes. Elle a notamment organisé une consultation publique sur un projet référentiel pour la gestion des pharmacies et mis à jour ses recommandations provisoires pour le contrôle qualité des essais cliniques pendant la crise sanitaire.

Le secteur associatif

La France dispose d'un tissu associatif particulièrement dense, recensant plus de 1,3 million d'associations aux profils, tailles et secteurs d'activité très hétérogènes (caritatif, politique, sportif, social, etc.).

Concentrées sur leurs missions, certaines structures n'ont pas toujours de ressources dédiées à la protection des données. Pourtant, la plupart d'entre elles collectent de nombreuses informations, parfois sensibles, qui concernent des publics variés (adhérents, éventuelles personnes accompagnées, salariés, bénévoles, donateurs).

Pour les aider à respecter le RGPD, la CNIL propose un nouveau guide dédié aux associations avec pour objectifs de leur **rappeler le cadre juridique de la protection des données et de leur donner des repères en termes d'organisation et de pratiques professionnelles.**

INFOSPLUS

Les clubs conformité

Les réunions dites « clubs conformité », initiées en 2014 avec le secteur de l'assurance, permettent d'échanger librement sur des problématiques identifiées par les professionnels ou par les services de la CNIL, y compris sur la base d'exemples de plaintes reçues.

UN ACCOMPAGNEMENT SPÉCIFIQUE DES TPE/PME

Une approche pragmatique

En 2021, la CNIL a poursuivi ses efforts de sensibilisation auprès des TPE et des PME afin de leur permettre de s'approprier le RGPD de façon opérationnelle et d'harmoniser les actions à mettre en place et les rendre plus transparentes. Son plan d'action repose, depuis quelques années, sur deux axes : la publication de fiches pratiques et d'outils adaptés à ces structures (FAQ à destination des TPE/PME, modèle de registre simplifié, exemples de mentions d'information des personnes, etc.) et une démarche d'accompagnement s'appuyant sur les têtes de réseaux et des partenariats structurants (avec notamment le médiateur des entreprises et l'ordre des experts-comptables).

Une contribution ambitieuse à l'innovation

La CNIL s'inscrit dans une logique de régulation moderne dans sa méthode et ouverte sur des problématiques innovantes. Afin d'apporter une contribution ambitieuse à l'accompagnement de l'innovation, la CNIL a eu recours à plusieurs méthodes :

- **elle déploie depuis 2017 une stratégie « start-up »** afin de poursuivre la mise en place d'interfaces d'échange et d'accompagnement des start-ups sur les sujets de protection des données ;
- **la CNIL a décidé, en 2021, de compléter ses outils traditionnels d'appui à l'innovation par la mise en place d'un**

56 « La CNIL adopte un référentiel sur les entrepôts de données de santé », 17 novembre 2021, cnil.fr

« bac à sable » (voir pages 86). L'objectif est d'apporter aux innovateurs des réponses pragmatiques et de la sécurité juridique sur des problématiques nouvelles. Ce dispositif, initié en 2021 sur la santé numérique, se poursuivra en 2022 sur le thème des outils numériques utilisés dans le secteur éducatif (EdTechs).

L'ACCOMPAGNEMENT DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Apparu en 2018 avec l'entrée en vigueur du règlement général sur la protection des données (RGPD), le délégué à la protection des données (DPD, ou DPO selon l'acronyme du titre anglais de ***Data Protection Officer*** couramment utilisé) occupe **un rôle central dans la gouvernance des données personnelles.** Il doit informer et conseiller le responsable de traitement, contrôler le respect des obligations légales par l'organisme et agir comme point de contact avec la CNIL. S'il n'est **pas responsable de la conformité de l'organisme**, il en est un rouage essentiel, capable d'allier expertise et conseil à toutes les étapes des projets impliquant l'utilisation de données personnelles.

En 2021, **28 810 personnes** exercent cette fonction en France (personnes physiques et morales confondues) pour **81 393 organismes** ayant désigné un DPO. Parmi ceux-ci, les secteurs de l'administration publique, de l'enseignement et de la santé sont les plus représentés.

Les obligations des organismes

Les autorités publiques et certains organismes privés dont l'activité de base implique un traitement à grande échelle de données sensibles ou de données permettant un suivi régulier et systématique de personnes doivent obligatoirement **désigner un DPO**[57]. Cette désignation doit être faite selon des critères, notamment de compétences, de connaissances et d'absence de conflit d'intérêts.

Les obligations des organismes ne s'arrêtent pas là : ils doivent également veiller à ce que le DPO ne reçoive pas d'instruction, qu'il soit associé en temps utile à toutes les questions relatives aux données personnelles et qu'il soit mis en capacité d'exercer ses missions. Ces exigences peuvent être contrôlées et, si nécessaire, sanctionnées par la CNIL.

Mais quelles sont les traductions concrètes de ces obligations ? Comment s'assurer que le DPO choisi puisse remplir ses missions de façon satisfaisante ? La CNIL propose depuis novembre 2021 un nouveau guide pratique dédié à la fonction de DPO et qui répond à ces questions.

Le premier guide pour les questions sur le DPO

Avec l'aide de nombreuses associations professionnelles, la CNIL a regroupé dans ce guide les **principales connaissances utiles sur le DPO**.

Cet outil est organisé en quatre parties :

1. Le rôle du DPO
2. La désignation du DPO
3. L'exercice de la fonction du DPO
4. L'accompagnement du DPO par la CNIL

Chaque thématique est illustrée par des cas concrets et les réponses aux questions fréquemment posées sur le sujet. Le lecteur peut également s'appuyer sur des outils pratiques tel qu'un modèle de lettre de mission.

De sa désignation à la fin de sa mission, ce guide permet d'obtenir rapidement des informations essentielles et précises sur le DPO. La CNIL a été particulièrement vigilante à apporter des éléments clairs sur la manière de s'assurer que le DPO peut effectuer ses missions en toute indépendance, sans conflit d'intérêt et avec une réelle efficacité pour l'organisme.

LES DPO EN FRANCE

81 393
organismes ont désigné un DPO

1/3
sont issus du secteur public

28 810
DPO (personnes physiques et morales)

4 131
appels reçus par la CNIL pendant la permanence juridique dédiée aux DPO

57 « Le délégué à la protection des données (DPO) », cnil.fr

L'activité dédiée à l'accompagnement des DPO

En consacrant une équipe à l'accompagnement des DPO, la CNIL est en prise directe avec les pratiques métiers.

Cette activité revêt plusieurs formes :

- des collaborations régulières avec les associations représentant les DPO ;
- une animation et un développement de partenariats impliquant la désignation et le développement de la fonction de DPO (voir focus) ;
- une permanence juridique téléphonique ;
- une adresse électronique spécifique pour les demandes de conseil des DPO.

Ces interactions quotidiennes et multisectorielles avec les professionnels de la protection des données que sont les DPO donnent l'opportunité à la CNIL de diffuser les bonnes pratiques tout en permettant d'enrichir sa doctrine.

Soucieuse du bon développement du métier de délégué, **la CNIL a participé aux travaux menés par la délégation générale à l'emploi et à la formation professionnelle (DGEFP) du ministère du Travail** sur la troisième édition de l'étude sur les délégués à la protection des données. Les résultats sont attendus courant 2022.

FOCUS

Un partenariat avec Déclic pour les DPO des petites collectivités territoriales

La CNIL, au titre de sa mission d'accompagnement des professionnels et Déclic, animateur d'un réseau de structures œuvrant en faveur du développement numérique des collectivités territoriales, ont signé une convention de partenariat le 25 janvier 2021. Cette coopération vise à soutenir les collectivités dans leur démarche de protection des données personnelles en favorisant le développement des services de délégués à la protection des données mutualisés.

Le contexte

Les collectivités territoriales et leurs groupements ont engagé la transition numérique de leur action (e-administration, télé services, *open data*, plateformes en ligne participatives, mobilité intelligente, etc.) alors que ne cesse d'augmenter le niveau de conscience des citoyens quant au besoin de protection des informations les concernant. Dans le même temps, se multiplient les cyber-attaques de nature à porter atteinte à l'intégrité, à la confidentialité et à la disponibilité de ces informations.

Pour garantir la protection des données personnelles de leurs usagers, les communes et intercommunalités doivent ainsi adopter des mesures techniques et organisationnelles et être en capacité de démontrer qu'elles offrent un niveau optimal de sécurité des données qui leur sont confiées.

Dans ce contexte, la CNIL, au titre de sa mission d'accompagnement des responsables de traitement, et Déclic, qui fédère des opérateurs publics de services numériques (OPSN), ont souhaité unir leurs efforts. Leur objectif commun : soutenir les collectivités dans leur démarche de mise en conformité au cadre juridique de la protection des données.

Les actions

Afin de contribuer le plus efficacement possible à la mise en œuvre du RGPD dans les communes et intercommunalités, en particulier dans les plus petites d'entre elles, plusieurs actions sont prévues dans les trois prochaines années.

L'association Déclic favorisera le développement des services de délégué à la protection des données mutualisés proposés par ses structures adhérentes :

- en formant les délégués désignés et en favorisant le travail collaboratif par l'animation du réseau ;
- en mettant à la disposition de celui-ci des ressources utiles, notamment documentaires ;
- en centralisant les problématiques structurantes ou questions récurrentes identifiées auprès de ses adhérents, et à y apportant un premier niveau de réponse.

Parallèlement, la CNIL soutiendra Déclic dans ses démarches :

- en contribuant à l'élaboration d'outils, de fiches pratiques et modèles pouvant être diffusés par Déclic ;
- en participant activement aux réunions d'information de portée nationale organisées par Déclic ;
- en lui apportant un soutien juridique et technique dans le traitement des problématiques dont elle est saisie.

LE MOOC « ATELIER RGPD »

Plus de 123 000 comptes ont été créés depuis 2019.

123 882
comptes créés

43 987
attestations de suivi délivrées

Avec la formation en ligne ouverte à tous (MOOC) intitulée « L'atelier RGPD », la CNIL propose une initiation au RGPD pour permettre aux professionnels de débuter la mise en conformité de leurs organismes.

Une évolution technique est en cours de réalisation depuis juillet 2021 afin de proposer en 2022 toujours plus de nouveaux contenus pour les utilisateurs.

LES NOUVEAUX OUTILS DE LA CONFORMITÉ

Un premier code de conduite européen pour les fournisseurs de solutions cloud

L'année 2021 aura été marquée par la **première approbation** par la CNIL d'un code de conduite européen dédié aux fournisseurs de services d'infrastructure cloud (IaaS)[58] et la **délivrance des premiers agréments** à des organismes de contrôle[59].

Ce code, porté par *Cloud Infrastructure Service Providers Europe* (CISPE), s'adresse aux fournisseurs de services d'infrastructure cloud *(« Infrastructure as a Service » ou « IaaS »)* situés sur le territoire de l'Union européenne.
Le recours à l'outil de conformité que constitue un code de conduite est particulièrement adapté : il aidera les adhérents à démontrer à leurs clients **qu'ils font uniquement appel à des sous-traitants qui présentent des garanties suffisantes au regard de l'article 28 du RGPD.**

De plus, le code de conduite porté par CISPE facilitera la mise en conformité de ce secteur d'activité : il apporte à la fois une **méthode de mise en conformité** et des **solutions pratiques** aux problèmes recensés par les professionnels concernés. Il donne ainsi une dimension opérationnelle aux principes de la protection des données énoncés dans le droit national et européen. Le contrôle de la bonne application de ce code par les adhérents sera assuré par trois organismes tiers sélectionnés par le porteur du code et agrées par la CNIL sur la base du référentiel adopté le 24 juillet 2020.

Document de référence
Les outils de la conformité

58 « La CNIL approuve le premier code de conduite européen dédié aux fournisseurs de services d'infrastructure cloud (IaaS) », 11 juin 2021, cnil.fr
59 « Code de conduite : la CNIL délivre un premier agrément à un organisme de contrôle », 16 juillet 2021, cnil.fr

DÉFINITION

Le code de conduite

Un code de conduite est un **outil de redevabilité (*accountability* en anglais)** car il permet aux adhérents de démontrer leur conformité en justifiant des bonnes pratiques mises en place. **Il prend en compte les exigences du RGPD mais peut éventuellement intégrer des préconisations qui vont au-delà.** Il résulte d'une **double démarche volontaire :** la décision par l'organisation représentative du secteur d'élaborer un code et l'adhésion des professionnels concernés.

Le mécanisme de contrôle développé par un code de conduite, qui incombe à un organisme dédié, ne se confond pas avec les missions de contrôle de la CNIL.

FOCUS

Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : le projet de position de la CNIL

La CNIL a constaté ces dernières années une augmentation significative des dispositifs de vidéo dite « intelligente » ou « augmentée » dans les lieux ouverts au public. Ces dispositifs sont constitués de logiciels de traitements automatisés d'images couplés à des caméras. **Ils permettent d'extraire diverses informations à partir des flux vidéo qui en sont issus.**

Ces dispositifs sont susceptibles d'être utilisés par tout type d'acteurs, publics comme privés, en particulier dans la rue ou des lieux ouverts au public, pour satisfaire des objectifs divers tels que la sécurité des personnes ou des biens, l'analyse de la fréquentation d'un lieu ou encore des opérations de publicité.

Face à la création et au déploiement de ces outils, parfois en dehors de tout cadre juridique spécifique, et face aux risques d'une surveillance et d'une analyse algorithmiques permanentes des espaces publics, **la CNIL a souhaité exposer sa compréhension, ses réflexions et ses analyses sur le sujet d'un point de vue éthique, technique et juridique.**

Elle a publié un projet de position concernant le déploiement de ces dispositifs dans les espaces publics et a soumis ce document à **consultation publique du 14 janvier au 11 mars 2022**[60]**.**

Ce projet de position poursuit 3 objectifs :

- présenter de manière pratique et concrète ce que sont les outils de vidéo « intelligente » ou « augmentée » et leur variété d'usages.
- mettre en avant les enjeux éthiques et sociétaux de cette technologie et les risques pour les droits et libertés des personnes.
- soumettre à consultation une interprétation du cadre juridique applicable à ces dispositifs en fonction de leurs objectifs, de leurs conditions de mise en œuvre et des risques qu'ils impliquent.

La CNIL étudiera les retours à cette consultation, désormais terminée, et publiera prochainement sa position définitive sur le sujet.

60 « Projet de position relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics », (PDF, 549 ko) 14 janvier 2021.

L'ANALYSE DE LA CNIL

« BAC À SABLE » D'ACCOMPAGNEMENT RENFORCÉ POUR LA SANTÉ NUMÉRIQUE : LE BILAN

Une procédure transparente, quatre lauréats

Les nouveaux usages de la donnée et de l'intelligence artificielle appliquée à la santé, portée par une vague d'innovation que la pandémie a mis sur le devant de la scène, sont en train de renouveler profondément ce domaine sensible. Pour accompagner ces progrès et promouvoir des solutions respectueuses de la vie privée et des données personnelles dès la conception, la CNIL a décidé de se doter en 2021 d'un « bac à sable » d'accompagnement pour 4 projets innovants utilisant des données en santé numérique.

Quatre critères de sélection ont été retenus pour cet appel à projets : le caractère innovant, le bénéfice pour le public, l'intérêt des questions posées pour la protection des données, et un engagement fort du porteur en la matière.

Cette première édition du « bac à sable » a connu un fort succès : une soixantaine de candidatures ont été déposées par des acteurs de divers statuts et régions, sur des cas d'usage variés. Les 7 porteurs de projets les plus prometteurs ont été auditionnés en avril 2021 afin de procéder à un classement des dossiers. Au final, la présidente de la CNIL a retenu 4 projets :

- le projet du CHU de Lille et de l'équipe Magnet de l'Inria concernant l'apprentissage fédéré en intelligence artificielle appliquée aux études cliniques ;
- le projet de la jeune pousse Resilience développant une solution d'aide au diagnostic en oncologie ;
- le projet Magellan du bureau d'études Clinityx visant à construire des indicateurs statistiques anonymes de description des populations en recherche médicale (cf. interview ci-contre) ;
- et le projet Vertexa du Centre hospitalier d'Arras proposant une solution de réalité virtuelle à visée thérapeutique pour lutter contre les troubles de l'alimentation des mineurs.

Un accompagnement agile et personnalisé

Dans le cadre de son « bac à sable », la CNIL a proposé aux lauréats un accompagnement renforcé tout au long de l'année 2021, fondé sur l'identification des difficultés à lever lors de l'expérimentation. L'accompagnement est centré sur le projet et non sur l'ensemble des activités du lauréat. Il ne conduit pas à une attestation de conformité, dont le lauréat reste entièrement responsable.

La méthode de travail déployée au sein du « bac à sable » est agile et proche des besoins des lauréats, sur la base de réunions mensuelles avec les services de la CNIL, de visites sur site et de conseils et vérifications des services sur les infrastructures et la documentation juridique du lauréat. Outre des réponses détaillées sur les questions à résoudre, dont les lauréats ont démontré la bonne prise en compte dans leurs opérations, la CNIL les a conseillés sur la qualité de leur étude d'impact de protection des données ou leur a fait gagner du temps dans l'instruction de leurs demandes d'autorisation.

L'expérimentation du « bac à sable » n'affecte pas les droits des personnes, puisqu'il ne porte que sur des projets qui n'étaient pas encore opérationnels. Autre avantage pour les lauréats, **les services des contrôles de la CNIL n'ont pas connaissance des projets du « bac à sable » pendant la durée de l'expérimentation ni accès au dossier par la suite.**

Outre les quatre lauréats retenus dans le cadre du « bac à sable », la CNIL a organisé des réunions personnalisées avec 6 autres projets innovants présentant un intérêt fort pour la protection des données personnelles en santé.

Deux projets se sont terminés avec succès à la fin de l'année 2021 ; deux autres sont encore accompagnés jusqu'à la fin mars 2022. L'accompagnement s'est également adapté au calendrier des innovateurs eux-mêmes. Certains souhaitent être guidés dans leurs **choix de conception**, d'autres recherchent de la **sécurité juridique** sur des points d'application précis du RGPD, d'autres encore veulent **développer des technologies protectrices de la vie privée** pour tout un écosystème. Le « bac à sable » permet de répondre à tous ces besoins.

> **« L'objectif était triple : mieux connaître le terrain, apporter des réponses à des questions juridiques et technologiques nouvelles, accompagner l'innovation en suivant le rythme des innovateurs eux-mêmes.**

Une restitution publique des leçons tirées du « bac à sable »

La CNIL a publié, sur son site web, les principales leçons tirées par les services des projets examinés dans le cadre du « bac à sable ». Dans le respect du secret des affaires, la CNIL entend restituer au grand public et aux écosystèmes innovants les solutions trouvées par ses services dans ce cadre, afin de faire progresser l'ensemble de l'écosystème (voir encadré ci-contre).

FOCUS

Quelques questions-réponses pour les innovateurs dans le domaine de la santé numérique

Un porteur de projet de droit privé, non chargé d'une mission de service public, peut-il poursuivre une finalité d'intérêt public ?
Un entrepôt de données fondé sur la base légale de l'intérêt légitime (cas le plus courant pour les acteurs privés du secteur de la santé) peut poursuivre une finalité d'intérêt public (par exemple pour permettre la réalisation de projets de recherche en santé) . Les données de santé pourront être traitées à des fins de recherche scientifique ou pour des motifs d'intérêt public dans le domaine de la santé. Si l'entrepôt est constitué à des fins de construction, de fonctionnement et d'amélioration continue d'un algorithme d'apprentissage par machine, il sera soumis à formalités préalables (conformité à un référentiel ou autorisation de la CNIL), sauf si la collecte du consentement des personnes concernées à cette fin est possible.

Est-il possible d'utiliser des données agrégées dans le cadre d'un apprentissage fédéré par machine ?
Il est préférable de constituer des agrégats anonymes. Sans démonstration d'une absence de risque de réidentification, les agrégats seront considérés comme des données personnelles. La nature de l'algorithme et sa complexité sont à prendre en compte pour évaluer la nature des agrégats. Lorsque ces derniers ne sont pas anonymes, il convient de limiter le risque de réidentification dans l'ensemble de l'entraînement et de chiffrer la communication des agrégats en appliquant des méthodes à l'état de l'art. De même, en pareil cas, il conviendra d'utiliser les modalités d'exportation des données prévues par l'autorisation d'entrepôt de données de santé.

Est-il possible de réutiliser des données de santé dans un entrepôt de données, hors fins de recherche ?
Une telle réutilisation de données ne peut concerner que les bases régulièrement constituées et conservées pour lesquelles le responsable de traitement initial a réalisé un test de compatibilité avec les nouvelles finalités. Dans ce cadre, le respect du principe de minimisation suppose une logique de « pas à pas » et une pseudonymisation à la source, mais le RGPD reste applicable à ces données pseudonymisées, susceptibles de droit d'accès. Les personnes concernées doivent être informées de la réutilisation de leurs données par le nouvel utilisateur, de manière loyale, neutre et aisément compréhensible.

La parole à Nicolas GLATT

Fondateur et directeur du bureau d'études Clinityx

Qu'est-ce qui vous a décidé à candidater au « bac à sable » données de santé de la CNIL ?

Clinityx ambitionnait de développer Magellan, une application destinée à produire, de façon automatisée et selon une méthode normalisée, des indicateurs de santé publique à partir des données du système national de données de santé (SNDS). Nous souhaitons rendre l'apport du SNDS accessible à tout l'écosystème alors que certains acteurs en sont aujourd'hui exclus pour des raisons financières, techniques ou méthodologiques.
Nous avions conçu un environnement qui s'appuyait sur le principe du On-Demand, du privacy by design sans toutefois parvenir à trouver un cadre réglementaire applicable suffisamment simple pour en préserver l'intérêt. Le bac à sable était finalement la dernière chance pour Magellan : un projet innovant, des difficultés règlementaires, des experts de la CNIL et une volonté commune d'aboutir.

Comment avez-vous collaboré avec les services de la CNIL à l'occasion du « bac à sable » ?

La collaboration s'est matérialisée par des échanges et réunions de travail avec les juristes et les experts techniques de la CNIL. Un plan de travail nous a permis en 6 mois de lever toutes les contraintes rencontrées par Magellan sur les plans juridiques et techniques.
Pour chaque sujet, nous avons pu échanger directement avec les experts concernés et ainsi mieux connaitre la doctrine de la Commission et les attentes techniques associées.
Nous avons ainsi pu affiner et formaliser nos propositions.

Au final, quel est pour vous l'intérêt de ce dispositif pour les innovateurs confrontés à des enjeux de protection des données personnelles ?

Ce dispositif permet une proximité et un accompagnement sur les sujets d'expertise juridique et technique, indispensable à une démarche d'innovation dans le secteur de la santé. L'innovateur bénéficie d'un éclairage pour établir le meilleur compromis entre la pertinence de l'innovation et la préservation de la vie privée des personnes concernées.
Pour nous, ce dispositif a également été l'opportunité d'explorer les possibilités ouvertes par la réglementation et son application à une solution innovante qui bouscule les paradigmes en s'appropriant pleinement les principes fondamentaux du RGPD.
Si le dispositif était une formidable opportunité pour Magellan, nous pensons qu'il permet aussi à la CNIL de recueillir de nouveaux cas d'usages pour ajuster sa doctrine et accompagner l'évolution des méthodes de traitement de données.

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 des 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.

Erik
Ingénieur expert en technologie de l'information - référent santé au service de l'expertise technologique, Direction des technologies et de l'innovation

Au sein du service de l'expertise technologique, nous sommes plusieurs experts spécialisés dans les systèmes d'information de santé. Les enjeux sont de taille, puisqu'il s'agit de garantir le secret médical pour tous et de protéger les personnes contre un usage malveillant de leurs données personnelles !

En tant qu'ingénieur référent santé, je coordonne le traitement des dossiers et j'harmonise les solutions techniques et juridiques apportées aux entités publiques et privées qui nous sollicitent.

Les systèmes d'information que nous expertisons sont très variés : les grands systèmes nationaux comme « Mon espace santé » ou le Dossier médical partagé, ceux dédiés à la recherche en santé comme le Health Data Hub et les « entrepôts de données » des hôpitaux français, mais aussi les dossiers des patients gérés par les acteurs de soins, ou encore tous les systèmes mis en place en urgence pour lutter contre la COVID-19, comme le suivi des tests de dépistage et de la vaccination.

À chaque fois, nous analysons les circuits de circulation des données et les conditions de leur stockage afin d'assurer le meilleur niveau de sécurité possible. Nous recommandons régulièrement certaines mesures très efficaces : le chiffrement des données et leur pseudonymisation (remplacement des noms et prénoms des personnes par un numéro technique), ainsi que l'authentification forte (par exemple avec un code temporaire ou une carte à puce) qui permet de protéger et de tracer les accès aux données.

LES VIOLATIONS DE DONNÉES PERSONNELLES

Un nombre record de notifications de violations de données personnelles

La CNIL a traité **6 158 notifications en 2021.** Ce total prend en compte les notifications complètes, les notifications initiales, les notifications complémentaires ainsi que les notifications annulées car ne correspondant pas à une notification au sens de l'article 33 du RGPD (environ 2,3 % des notifications).

En ne comptant que les notifications complètes et les initiales, la CNIL recense **5 037 notifications de violations reçues en 2021**, contre 2 821 notifications[61] en 2020, soit **une augmentation significative de 79 %**. En moyenne, près de **14 notifications** sont reçues **par jour,** soit **420 notifications par mois.**

Plusieurs raisons expliquent cette augmentation majeure :

- **une très forte croissance des attaques informatiques, notamment les attaques par rançongiciels**, constituant la première menace cyber pour les entreprises, les collectivités locales et les organismes publics ;
- **une meilleure appropriation de l'obligation de notification**, résultant d'une **meilleure prise en compte des enjeux de cybersécurité** au sein des organismes, ainsi que **la définition et la mise en œuvre de processus internes** permettant de détecter et de réagir face aux violations de données personnelles ;
- **des notifications par vague**, lorsqu'un sous-traitant est concerné par un incident de sécurité et informe ses nombreux clients qui procèdent ensuite eux-mêmes à la notification. Ainsi, la CNIL a pu recevoir jusqu'à **près de 300 notifications en une seule journée.**

La CNIL estime cependant que de nombreuses violations restent non notifiées. Elle continuera à développer son action de sensibilisation pour la prise en compte de cette obligation par les organismes.

Les organismes et les secteurs d'activité les plus concernés

Toutes les tailles de structure sont concernées

Les PME et les micro-entreprises représentent 69 % des notifications, qui font majoritairement l'objet de piratage informatique (68 %). Cette forte proportion s'explique pour deux raisons. Moins armées que les grandes entreprises face à cette menace, elles constituent des cibles privilégiées pour les acteurs malveillants. Par ailleurs, dans le cas d'une défaillance d'un de leurs sous-traitants, ces organismes peuvent être amenés à devoir notifier en nombre.

INFOSPLUS

Le RGPD est le seul texte à imposer des obligations de cybersécurité précises, de façon transversale, et soumises au pouvoir de contrôle et de sanction d'une autorité.

En cas de non-respect des règles, la CNIL peut infliger une amende administrative de 20 millions d'euros ou 4 % du chiffre d'affaires.

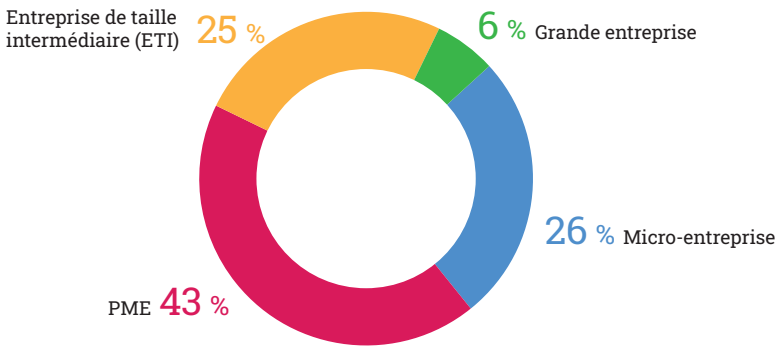
5 037

notifications reçues en 2021

+ 79 %

Par rapport à 2020

Part de notifications par taille de l'organisme



61 Le rapport annuel de 2020 recensait 2 825 notifications, nombre qui a été corrigé à 2 821 après sa publication (annulation de notifications).

Tous les secteurs d'activité concernés

Quatre secteurs d'activités représentent à eux seuls plus de 60 % des notifications reçues par la CNIL en 2021. Il s'agit :

- des organismes du secteur **« Activités spécialisées, scientifiques et techniques**[62] **»** (21 %),
- des organismes **du secteur de la santé humaine et de l'action sociale** (18 %),
- des **administrations publiques** (12 %) ; et
- des entreprises du **secteur financier et assurance** (10 %).

Les deux premiers secteurs connaissent la plus forte progression par rapport à 2020 : **le nombre de notifications reçues a pratiquement triplé en l'espace d'un an** (respectivement + 191 % et + 195 %). Ces augmentations majeures s'expliquent notamment par les vagues de notifications reçues au cours de l'année liées à des attaques ayant affecté des sous-traitants des organismes de ces deux secteurs.

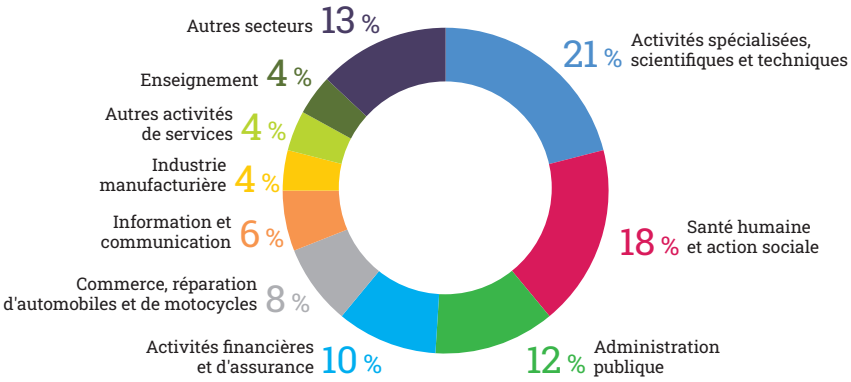
Par ailleurs, **24 % des notifications** effectuées en 2021 font état de la **compromission de données sensibles**, parmi lesquelles figurent les **données de santé** (23 % des notifications reçues en 2021).

Typologie des violations notifiées à la CNIL

Nature des violations

Comme les années précédentes, la CNIL reçoit majoritairement des notifications de violations en lien avec **une perte de confidentialité de données personnelles** (avec un total de 4 017 notifications, soit environ **80 %**). Les notifications liées à **une perte de disponibilité** et celles liées à **une perte d'intégrité** progressent fortement : **en 2021 leur nombre a plus que doublé.** Cela s'explique par une prise de conscience des organismes de la nécessité de notifier également ce type d'incidents et par l'augmentation des attaques de type rançongiciel.

Part de notifications par secteur d'activités

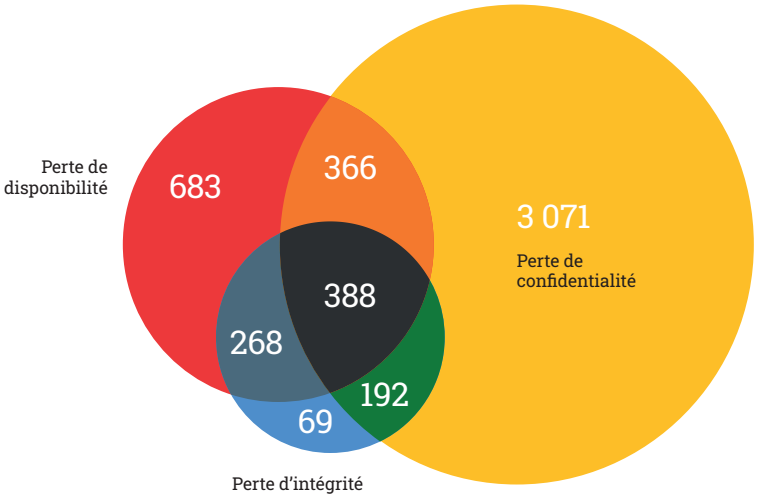


DÉFINITION

Perte de confidentialité, de disponibilité et d'intégrité

Les violations de données ne se limitent pas aux fuites de données. Elles peuvent entraîner **trois types de perte** qui peuvent toutes avoir de graves conséquences :

- **la perte de confidentialité** signifie que les données ont été rendues accessibles à une personne non autorisée ;
- **la perte de disponibilité** signifie que les données ont été rendues inaccessibles pendant un certain temps
- **la perte d'intégrité** signifie que les données ont été modifiées illégitimement.



62 Le code NAF M « Activités spécialisées, scientifiques et techniques » regroupe les organismes dont l'activité principale concerne des activités juridiques et comptables, des activités de sièges sociaux et de contrôle de gestion, des activités d'architecture, d'ingénierie, de contrôle et d'analyses techniques, des activités de recherche et développement scientifiques, des activités de publicité et d'études de marché, des activités vétérinaires ainsi que des activités telles que le design, la photographie ou la traduction et l'interprétation.

Causes des violations

En 2021, près de **63 % des violations notifiées à la CNIL sont causées par un acte externe** (accidentel ou malveillant), alors que les actes internes (accidentels ou malveillants) représentent 17 %.

Origines des violations

La CNIL a reçu **près de 3 000 notifications** résultant d'un **piratage informatique**, ce qui représente **environ 59 % des notifications, soit une hausse de 128 % par rapport à 2020.**

L'attaque la plus répandue reste **l'attaque par rançongiciel**, des programmes malveillants qui empêchent 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. 2021 a vu également la multiplication des rançongiciels opérant **l'exfiltration de données personnelles.** L'attaquant utilise alors le chantage à la divulgation des données pour faire peser une menace supplémentaire sur les victimes et les inciter ainsi à payer la rançon.

La CNIL a ainsi reçu plus de **2 150 notifications**, soit 43 % des notifications pour ce seul type d'attaque (contre 20 % en 2020). **Le quart de ces notifications** concerne le secteur de la santé et de l'action sociale.

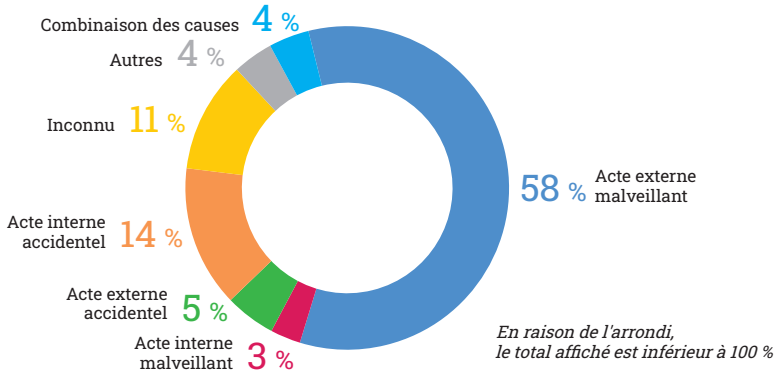
43 %

des notifications reçues en 2021 concernent une attaque par rançongiciel

INFOSPLUS

Le paiement de la rançon **ne garantit pas la récupération des données compromises et n'immunise pas** les organismes contre une nouvelle attaque de type rançongiciel.

Part des violations notifiées à la CNIL par cause



En raison de l'arrondi, le total affiché est inférieur à 100 %

FOCUS

Violations de données : les ressources utiles pour comprendre les attaques et s'y préparer

Au-delà des nombreux conseils pratiques disponibles sur son site web, la CNIL communique très régulièrement autour des enjeux liés à la cybersécurité.

Elle publie notamment « la violation du trimestre »[63]. Celle-ci permet de faire un retour d'expérience basée sur les violations majeures constatées par la CNIL dans le cadre des notifications faites par les responsables de traitement. Le but est ici de proposer des bonnes pratiques pour réduire les risques présentés par ces violations. Les sujets traités en 2021 concernaient les attaques par bourrage d'identifiants *(credential stuffing)*[64], les faux ordres de virement international (FOVI) ou « fraude au président »[65] ainsi que les attaques sur les messageries[66].

La CNIL a également participé au « Baromètre *Data Breach* » présenté lors du Forum International de la Cybersécurité (FIC) en 2021. Les données exploitées sont issues des publications de la CNIL sur la plateforme data.gouv.fr et permettent de donner les tendances en termes d'atteintes aux données personnelles.

Afin de répondre à l'augmentation des attaques de type rançongiciel mettant en œuvre l'exfiltration de données, la CNIL a également publié une communication concernant la recherche sur Internet de fuites d'informations (RIFI). La RIFI a pour objectif de détecter, au plus tôt, une fuite de données. La CNIL a ainsi souhaité préciser les règles à respecter, notamment le RGPD et le code pénal pour les organismes qui souhaitent y recourir, ainsi que pour les prestataires de RIFI eux-mêmes.

63 « Violation du trimestre », cnil.fr
64 « La violation du trimestre : attaque par credential stuffing sur un site web », 12 janvier 2021, cnil.fr
65 « Violation du trimestre : le faux ordre de virement international ou fraude au président », 9 avril 2021, cnil.fr
66 « Violation du trimestre : les attaques sur les messageries », 10 août 2021, cnil.fr

MOTS DE PASSE : UNE NOUVELLE RECOMMANDATION À VENIR

S'il existe aujourd'hui de multiples moyens de s'authentifier auprès d'un service en ligne, l'accès à de nombreux services numériques reste contrôlé par de simples mots de passe.

Or, d'après une étude de Verizon[67] de 2021, **81 % des notifications de violations de données mondiales seraient liés à une problématique de mots de passe.**

En France, presque **60 % des notifications reçues par la CNIL au cours de l'année 2021 sont liées à du piratage et un grand nombre de ces évènements auraient pu être évités par le respect de bonnes pratiques en matière de mots de passe.** L'authentification par mot de passe reste souvent utilisée car elle peut être mise en œuvre sans coût particulier pour les organismes et ne requiert pas de matériel dédié, mais mettre en place un système réellement sécurisé nécessite de traiter de nombreuses problématiques de sécurité pour être véritablement efficace et sûr.

Pour répondre à cet enjeu de sécurité, la CNIL avait publié en 2017 une première recommandation pour permettre aux professionnels et aux particuliers de disposer d'outils pratiques et à l'état de l'art[68]. **Cette recommandation définit des exigences techniques et organisationnelles minimales lorsque l'authentification par mots de passe est mise en œuvre pour un traitement de données personnelles.** Si le recours aux mots de passe pour gérer l'authentification lors de l'accès à un traitement de données personnelles est généralement acceptable, la CNIL a notamment considéré que d'autres moyens d'authentification, **comme par exemple l'authentification à double facteur ou les certificats électroniques**, offrent davantage de sécurité que le mot de passe et sont nécessaires pour sécuriser l'accès à certains types de traitements.

Forte de l'expérience acquise ces quatre dernières années au travers de ses actions d'accompagnement et de contrôle, la CNIL a souhaité mettre à jour sa recommandation afin d'y intégrer plus de souplesse et prendre en compte l'évolution des connaissances et des usages.

Ainsi, en octobre 2021, un nouveau projet de recommandation a été publié pour consultation afin de permettre à l'ensemble des parties prenantes de contribuer aux travaux de la CNIL sur le mode d'authentification le plus utilisé au quotidien.

Cette consultation a rencontré un vif succès : **53 réponses ont été reçues**, provenant de personnes travaillant dans le domaine de la cybersécurité (pour la moitié d'entre elles) et/ou de la protection de la vie privée (deux-tiers des retours) mais aussi de quelques acteurs de la vie civile (monde politique ou associatif). Ainsi 17 DPO, 10 RSSIs, 4 chercheurs en sécurité ainsi qu'une dizaine d'informaticiens de diverses spécialités ont répondu.

Une fois les réponses à cette consultation prises en compte, **une nouvelle version de cette recommandation sera publiée en 2022.**

FOCUS

Journalisation des traitements : une nouvelle recommandation

L'obligation de sécurité imposée par le RGPD et la loi Informatique et Libertés ne se limite pas aux critères de gestion des mots de passe. Suivant le même processus de consultation publique, la CNIL a publié en octobre 2021 une recommandation relative aux mesures de journalisation[69].

Le but de la journalisation est d'assurer une traçabilité des accès et des actions des différentes personnes accédant aux traitements de données personnelles mis en œuvre. Les données ainsi collectées peuvent constituer un outil efficace de détection et d'investigation en cas d'incident, d'intrusion dans les systèmes informatiques, ou de détournement d'usage des traitements de données par les personnes habilitées. En ce sens, la journalisation constitue une mesure de sécurité importante que la CNIL encourage de manière systématique.

Cependant de tels journaux contiennent également des données relatives aux utilisateurs habilités du système qui peuvent révéler des informations sur eux (par exemple liées à leur performances professionnelles). Il est donc nécessaire de trouver un juste équilibre entre la sécurité apportée par la journalisation et l'émergence de risques particuliers liés à une conservation trop longue de données. Comme souvent en matière de protection des données cette conciliation doit avoir pour objectif de limiter les risques pour les personnes concernées.

La publication de cette recommandation permet aux acteurs de mieux comprendre les mesures à mettre en œuvre afin de respecter des obligations qui découlent des textes applicables et donc de mieux protéger les données personnelles des citoyens.

67 « 2001 Data Breach Investigation Report » (en anglais), verizon.com
68 « Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers », 27 janvier 2017, cnil.fr
69 « La CNIL publie une recommandation relative aux mesures de journalisation », 18 novembre 2021, cnil.fr

LA PARTICIPATION DE LA CNIL À L'ÉCOSYSTÈME CYBER

La sécurité informatique, ou cybersécurité, est une obligation présente depuis 1978 dans la loi Informatique et Libertés et, encore renforcée avec l'entrée en application du RGPD en 2018. Elle fait partie des **principes fondamentaux** de la protection des données, en tant que mesure cardinale permettant de prévenir les risques pour les personnes dont les données sont traitées.

En 2022, pour renforcer son action, la CNIL a rejoint le **Campus Cyber**, qui rassemble les principaux acteurs du domaine en France. L'objectif est d'intensifier ses relations avec l'écosystème cyber et de participer à promouvoir l'excellence française en fédérant les différents talents et acteurs de ce secteur.

La CNIL s'investit dans de nombreuses autres initiatives du monde cyber. Elle participe depuis de nombreuses années au **Cybermoi/s** afin de participer à la diffusion des bonnes pratiques de sécurité. Ses relations se sont également intensifiées avec le **groupement d'intérêt public contre la cybermalveillance (GIP ACYMA)** dont le but est de lutter contre les actes de cybermalveillance par le biais, notamment, du dispositif **Cybermalveillance.gouv.fr.** Cette collaboration s'est traduite par l'adhésion de la CNIL au GIP en mars 2022.

La CNIL est également membre d'associations actives dans le domaine, telles que le **Club EBIOS**, le **CESIN** et participe aux principaux évènements liés à la Cybersécurité, comme le **Forum International de la Cybersécurité (FIC)**, démontrant ainsi son intérêt et sa place dans l'écosystème avec la volonté d'améliorer le monde cyber tout en préservant les droits et libertés de chacun.

CAMPUS CYBER

FOCUS

Les quatre piliers du Campus cyber

Les opérations : favoriser le partage de données pour renforcer la capacité de chacun à maitriser le risque numérique (détection, capacités de veille, réponse aux incidents, mise en commun de la connaissance sur la menace).

La formation : Soutenir la formation initiale et continue des différents publics (agents de l'État, salarié(e)s, étudiant (e)s, personnel en reconversion…) afin de favoriser une montée en compétence globale de l'écosystème (programmes communs, partage de ressources).

L'innovation : développer les synergies entre les acteurs publics et privés (industriels, start-up et centres de recherche) pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique.

L'animation : proposer un lieu ouvert, vivant dédié à la programmation d'évènements innovants, propice aux échanges et à la découverte des évolutions (conférences, webinaires, *showroom, jobdating*, etc.)

La parole à Guillaume POUPARD

Directeur général de l'ANSSI

Comment l'ANSSI agit-elle pour améliorer la sécurité numérique ?

L'ANSSI est l'autorité nationale de cybersécurité et de cyberdéfense française. Pour améliorer la sécurité numérique, elle agit en prévention : en diffusant des bonnes pratiques via des guides dont certains sont réalisés avec la CNIL, en accompagnant les grands projets numériques pour les sécuriser et en élaborant au niveau national et européen le cadre réglementaire applicable en matière de sécurité numérique. Elle évalue également des prestataires privés de confiance vers lesquels les organisations, privées comme publiques, peuvent se tourner pour mettre en œuvre leur démarche de cybersécurité. Mais elle agit également en réactif : en intervenant auprès de victimes de cyberattaques, en diffusant des alertes en cas de vulnérabilités[70] et en détectant des cyberattaques.

En quoi la conformité au RGPD peut aider les entreprises et administrations à prévenir les menaces cyber ?

Les menaces cyber sont multiples et peuvent avoir des finalités variées allant de l'espionnage au sabotage en passant par la déstabilisation et le profit financier. Cependant, les mesures à mettre en place pour s'en prémunir sont les mêmes : identifier les systèmes d'information critiques, notamment au regard des données qu'ils contiennent et mettre en place des mesures de sécurité essentielles que sont les mises à jour, les sauvegardes, la gestion des accès et le suivi des alertes. Ce travail d'identification et de sécurisation est d'ailleurs demandé par le RGPD pour protéger les données personnelles, directement aux responsables de traitement mais également à ses sous-traitants. Aussi, ***être conforme au RGPD est souvent synonyme d'un bon niveau de cybersécurité****, à même de résister aux menaces les plus opportunistes.*

Qu'est-ce que le référentiel SecNumCloud ? Comment peut-il être utilisé pour garantir la conformité en matière de transferts de données ?

Créé en 2016 par l'ANSSI, le référentiel SecNumCloud permet la qualification de prestataires de services d'informatique en nuage, plus couramment dénommés cloud pour que les administrations et entreprises souhaitant externaliser leurs données le fassent en confiance. La qualification évalue ainsi la robustesse de la prestation de services cloud et la compétence du prestataire qui la met en œuvre. Déjà modifié en 2018 avec l'aide de la CNIL pour tenir compte de l'entrée en application du RGPD, le référentiel SecNumCloud continue d'évoluer. Il intégrera ainsi prochainement de manière explicite des critères visant à garantir l'applicabilité exclusive du droit européen sur ces offres. Selon l'évaluation de la CNIL, ces critères attesteront également de la Conformité en matière de transferts de données, notamment au regard de la jurisprudence de la Cour de justice de l'Union européenne avec la décision « Schrems II ».

70 Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), cert.ssi.gouv.fr

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 et de l'instruction réalisée par les services, la présidente de la CNIL peut décider, selon l'importance des manquements constatés, de clôturer le dossier, de prononcer une mise en demeure ou de saisir la formation restreinte de la CNIL en vue de prononcer une sanction financière à l'encontre de l'organisme. Les mesures correctrices sont susceptibles d'être rendues publiques.

Marjolaine
Juriste au service des contrôles – RH, santé et affaires publiques, Direction de la protection des droits et des sanctions

Antoine
Auditeur des systèmes d'information au service des contrôles – affaires économiques, Direction de la protection des droits et des sanctions

Nous sommes auditeurs des systèmes d'information et juriste au service des contrôles de la CNIL. Nos missions sont variées et nous pouvons être amenés à contrôler les traitements aussi bien dans des entreprises privées que dans des ministères ou des établissements de santé.

Nous avons été impliqués sur des thématiques ayant de fort enjeux pour les personnes et pouvant avoir un retentissement dans l'actualité, par exemple quand il s'agit de violations de données, des dispositifs mis en œuvre pour lutter contre la COVID-19, ou des traitements européens comme le « SIS II - SCHENGEN » qui ont pour objet de permettre aux États membres de l'espace Schengen de mettre en place une politique commune de contrôle des entrées dans ce territoire.

Nous travaillons toujours en binôme, juriste et auditeur des systèmes d'information. L'un comme l'autre, cela permet de nous enrichir mutuellement et d'acquérir des connaissances sur des sujets parfois bien différents de nos formations initiales, ce qui est indispensable si nous voulons maîtriser tous les aspects des dossiers sur lesquels nous travaillons.

Les contrôles sur place sont toujours très enrichissants. Tous les organismes n'ont pas nécessairement conscience de leurs obligations au regard des traitements de données personnelles qu'ils mettent en œuvre et il nous appartient alors d'échanger avec eux pour bien comprendre leur activité. Le bon déroulement d'une mission de contrôle repose également sur notre capacité à gérer les relations humaines avec les salariés ou les agents des organismes contrôlés, qui s'attendent rarement à recevoir notre visite.

« COMMENT SE PASSE UN CONTRÔLE DE LA CNIL ? »

Une mission de contrôle a pour objectif de permettre une évaluation de la conformité d'un organisme tout en assurant à la CNIL une bonne compréhension de la nature et des finalités des traitements de données qu'il réalise. Lors de ces vérifications, un procès-verbal factuel reprenant l'ensemble des informations fournies et décrivant les constats effectués est rédigé par les contrôleurs qui le signent avec le représentant de l'organisme[71].

Les missions de contrôle sont notamment réalisées sur place, dans les locaux de l'organisme et généralement de façon inopinée, ou sur audition, le responsable de l'organisme étant convoqué et entendu dans les locaux de la CNIL. Il est également possible de réaliser des vérifications en ligne, directement sur un site web ou une application mobile, ou sur pièces, sur la base des réponses apportées par l'organisme à un questionnaire écrit.

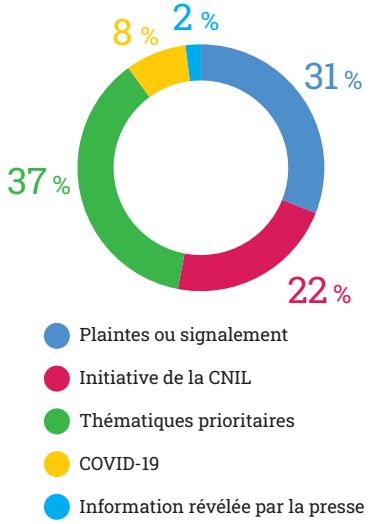
DES CONTRÔLES EN HAUSSE

La CNIL a procédé à 384 contrôles formels en 2021 (soit une augmentation de 55 % par rapport à l'année 2020 et de 28 % par rapport à l'année 2019). Le prolongement de la crise sanitaire en 2021 a conduit la CNIL à poursuivre l'adaptation de ses pratiques de contrôle afin d'être en mesure de réaliser un nombre plus conséquent de missions malgré les importantes contraintes liées à la situation.

Ainsi, lors de chaque rebond épidémique, les opérations de contrôle sur place ont été réduites au strict nécessaire. Dans le même temps, les contrôles des traitements liés à la vaccination ou au contrôle des passes sanitaires ont fortement mobilisé la CNIL (29 contrôles en 2021). Les phases de recul de la contamination ont néanmoins permis, en 2021, **une augmentation substantielle des contrôles sur place par rapport à l'année 2020 (+ 64 %), mais également des auditions (+ 47 %)**. Seuls les contrôles sur pièces, modalité de contrôle qui avait été privilégiée au plus fort de l'épidémie en 2020, voient leur nombre reculer légèrement en 2021 (- 12 %).

La réalisation de plusieurs vagues de contrôles au périmètre limité (cookies et autres traceurs, cybersécurité des sites web) a entraîné une augmentation très significative du nombre des contrôles en ligne pendant l'année 2021 (+ 110 % par rapport à 2020).

L'origine des contrôles



Afin de répondre toujours plus aux préoccupations quotidiennes et aux difficultés rencontrées par les particuliers dans leurs relations avec les responsables de traitement, la CNIL poursuit sa volonté d'effectuer plus de missions de contrôle ayant pour origine une plainte (31 % pour l'année 2021).

Outre les modalités de contrôle, la situation sanitaire a également fortement impacté le choix des contrôles menés, les missions portant sur les traitements liés à l'épidémie de COVID-19 représentent ainsi 10 % de la totalité des contrôles réalisés durant l'année 2021 (TousAntiCovid, TousAntiCovid Vérif, SI-DEP, Contact Covid, Vaccin Covid et passe sanitaire – voir L'analyse de la CNIL page 54).

Par ailleurs, comme les années précédentes, la CNIL a continué de porter une attention particulière à la sécurité des données personnelles. Elle a ainsi mené 49 vérifications à la suite de signalements de violations de données personnelles afin de les faire cesser dans un délai très restreint.

La CNIL a conduit environ 8 000 actes d'investigation en 2021. Ces vérifications peuvent s'effectuer dans le cadre de procédures formelles de contrôle (voir ci-dessous), notamment en réponse à des plaintes ou lors d'une procédure de sanction et comprennent également les demandes de droit d'accès indirect[71].

384
contrôles dont :

118
contrôles sur place

173
contrôles en ligne

65
contrôles sur pièces

28
contrôles sur audition

Auxquels s'ajoutent
49
signalements relatifs à des violations de données personnelles

71 Pour en savoir plus sur le droit d'accès indirect, voir page 46.

Bilan des thématiques annuelles prioritaires pour 2021

La sécurité des données de santé

La CNIL a poursuivi la thématique prioritaire de contrôle initiée en 2020 relative 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 service du domaine de la santé.

La CNIL a donc mené **30 nouvelles missions** de contrôle dans le domaine de la santé (laboratoires d'analyses médicales, hôpitaux, prestataires, *data brokers* en données de santé), et plus précisément sur la question de la sécurité des données de santé.

La CNIL a également poursuivi sa mission de contrôles des traitements mis en œuvre pour répondre à l'épidémie de COVID-19[72].

La cybersécurité du web français

Cette thématique prioritaire de contrôle a eu pour objectif d'évaluer le niveau de sécurité des sites web français les plus visités dans différents secteurs, aussi bien privés que publics. Dans ce cadre, trois séries de vérifications en lien avec la sécurité des données ont été menées.

La première a porté sur la robustesse du chiffrement des données en transit sur internet par l'analyse des versions du protocole TLS mises en place, la conformité du certificat et des suites cryptographiques autorisées par les serveurs des sites contrôlés.

La deuxième a concerné la sécurisation de l'accès aux comptes utilisateur à travers l'évaluation de la robustesse des mots de passe, de leur procédure de renouvellement, des modalités de leur transmission et conservation, et des mesures de traçabilité mises en œuvre.

La dernière a visé les mesures mises en place face aux rançongiciels (*ransomwares* en anglais) à la suite de violations de données. Une attention particulière a été portée sur les dispositifs de détection des consultations anormales et des accès non autorisés.

Au total, vingt-deux organismes ont été contrôlés dont quinze publics. Ces vérifications ont montré que le manquement le plus récurrent (recensé auprès de douze organismes) concerne l'utilisation de suites cryptographiques obsolètes qui rendent les sites web particulièrement vulnérables aux attaques. Le recours à un certificat de sécurité délivré par une autorité non qualifiée suivant les recommandations du règlement général de sécurité (RGS) a également été relevé auprès d'une dizaine d'organismes publics. De même, dix organismes ont recours à des versions obsolètes du protocole TLS (versions 1.0 et 1.1), c'est-à-dire qui ne sont pas conformes aux recommandations de sécurité de l'ANSSI. Enfin, les recommandations de la CNIL en matière de mot de passe sont insuffisamment suivies.

Les cookies et autres traceurs

Dans le prolongement de la publication des nouvelles lignes directrices de la CNIL sur les « cookies et autres traceurs » en 2020, une période d'adaptation avait été accordée aux acteurs. Pour vérifier la mise en conformité des organismes, **trois séries de contrôles en ligne ont été menées en 2021, visant 92 sites web à forte affluence**, afin de s'assurer notamment de **l'absence de dépôt de cookies sur le terminal de l'internaute avant tout accord et du respect de l'obligation de recueillir un consentement libre** ; refuser les cookies devant être aussi simple que de les accepter. Les vérifications ont porté sur des sites aux caractéristiques variées, bien que 93 % de ces contrôles aient visé le secteur privé. En outre, 58 % des entreprises éditant les sites web concernés étaient des entreprises étrangères et 42 % étaient des entreprises françaises. Si 43 % des sites relevaient du domaine du commerce, d'autres secteurs ont été ciblés, comme le transport (12 %), les nouvelles technologies (11 %), les loisirs (7 %), les services publics (7 %) ou la finance et l'assurance (6 %).

Ces vérifications se sont limitées à un ou deux points très spécifiques (présence d'un bouton permettant de naviguer sans consentir au dépôt des cookies et effectivité du refus) afin de pouvoir être réalisées rapidement sur une multitude de sites web. L'ensemble de ces contrôles a par la suite fait l'objet de mises en demeure sur ces exigences afin de conduire les acteurs à se conformer à la loi Informatique et Libertés (voir page 102).

72 Pour en savoir plus sur les contrôles relatifs à la crise sanitaire, voir page 30.

UNE FORTE HAUSSE DE L'ACTIVITÉ RÉPRESSIVE DE LA CNIL

2021 est une année sans précédent, tant par le nombre de mesures adoptées (18 sanctions et 135 mises en demeure) que par le montant cumulé des amendes, qui atteint plus de 214 millions d'euros.

18 sanctions visant des secteurs d'activités variés

En 2021, la formation restreinte de la CNIL a prononcé 18 sanctions, **pour un montant de 214 106 000 euros. Douze d'entre elles ont été rendues publiques.**

Ces sanctions comportent 15 amendes (dont 5 avec injonctions sous astreinte) et 2 rappels à l'ordre, avec injonctions. À cela s'ajoute la première décision de liquidation d'astreinte (c'est-à-dire le paiement d'une somme en raison du non-respect d'un ordre donné par la CNIL). En pratique, la société concernée, initialement sanctionnée d'une amende de 7 300 euros, a dû payer 65 000 euros supplémentaires car elle n'avait pas procédé aux modifications de son traitement demandées dans la décision de sanction.

Cette année, les décisions ont concerné **des secteurs d'activité et des acteurs très divers.** Parmi les manquements les plus fréquents figurent le défaut d'information des personnes et des durées de conservation excessives. Sur ces 18 sanctions, la moitié comporte un manquement en lien avec la sécurité des données personnelles, ce qui illustre deux choses :

- les mesures de sécurité prises par les organismes restent souvent insuffisantes ;
- la CNIL vérifie systématiquement la sécurité des systèmes d'information lorsqu'elle effectue un contrôle.

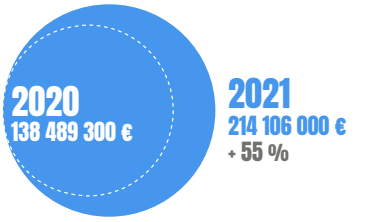
Enfin, 4 sanctions concernent une mauvaise gestion des cookies et autres traceurs.

18
sanctions

214
millions d'euros d'amendes

135
mises en demeure

Les sanctions de la CNIL en 2021



La moitié des sanctions concerne en partie une mauvaise sécurité des données

4 décisions de la CNIL en coopération avec d'autres autorités européennes

17 dossiers européens examinés par la CNIL

FOCUS

Les dossiers traités en coopération avec les autorités européennes de protection des données en 2021

En 2021, parmi les 18 sanctions imposées par la formation restreinte de la CNIL, 4 ont été adoptées en coopération avec des homologues européennes, dans le cadre du « guichet unique » prévu par le RGPD. Cette procédure a été suivie, par exemple, pour la sanction adoptée à l'encontre de Slimpay. Avant l'adoption de ces 4 décisions, la CNIL a coopéré avec les autorités concernées et leur a soumis les projets de décision afin de s'assurer de leur accord.

En parallèle, **la CNIL a examiné 17 projets de décision d'homologues**, à propos desquels elle a prononcé 6 objections en raison de divergences d'analyse, notamment sur le fait que certains manquements au RGPD n'avaient pas été retenus dans le projet de décision, sur la nature de la mesure correctrice proposée ou encore sur le montant de l'amende proposé par l'autorité chef de file.

En particulier, la CNIL ainsi que d'autres autorités européennes ont formulé des objections concernant un projet de sanction de l'autorité irlandaise dirigée contre la société WhatsApp. L'autorité irlandaise ayant rejeté l'ensemble des objections, l'affaire a été renvoyée devant le CEPD, conformément à l'article 65 du RGPD. Dans sa décision du 28 juillet 2021, le CEPD a suivi la majorité des objections formulées par les autorités concernées, dont celles de la CNIL, et a enjoint à l'autorité irlandaise de modifier son projet.

FOCUS

Deux sanctions publiques prononcées à l'encontre du ministère de l'Intérieur

UNE UTILISATION ILLICITE DE DRONES ÉQUIPÉS DE CAMÉRAS POUR SURVEILLER LE RESPECT DU CONFINEMENT

Le contexte

En 2020, lors du premier confinement, le ministère de l'Intérieur a utilisé des drones équipés de caméras, notamment pour vérifier le respect des mesures de confinement. Des drones étaient également utilisés pour surveiller des manifestations, pour des missions de police judiciaire (telles que la reconnaissance d'un lieu avant une interpellation ou la surveillance d'un trafic de stupéfiants) ou encore surveiller des rodéos urbains.

La loi Informatique et Libertés prévoit que les traitements mis en œuvre par l'État, notamment pour prévenir ou détecter les infractions pénales, mener des enquêtes ou se prémunir contre des atteintes à la sécurité publique, **doivent être prévus par un texte.** En outre, **une analyse d'impact**[73] **doit être réalisée** lorsque ces traitements présentent un risque élevé pour les droits et libertés des personnes, comme c'est le cas en l'espèce.

Or, aucun texte n'autorisait le ministère de l'Intérieur à recourir à des drones équipés de caméras captant des images sur lesquelles les personnes sont identifiables et aucune analyse d'impact n'avait été communiquée à la CNIL. Le public n'était pas non plus informé de l'utilisation des drones comme il aurait dû l'être.

La décision de la CNIL

Le 12 janvier 2021, la formation restreinte de la CNIL a donc rappelé à l'ordre le ministère de l'Intérieur pour avoir procédé à des vols de drones en dehors de tout cadre légal et lui a enjoint de cesser tout vol de drone jusqu'à ce qu'un cadre normatif l'autorise. Cette décision concernait l'utilisation des drones par l'ensemble des forces de l'ordre agissant sous l'autorité du ministère, qu'il s'agisse de services de police ou de gendarmerie, sur l'ensemble du territoire et quelles que soient les finalités poursuivies.

La loi du 24 janvier 2022 relative à la responsabilité et à la sécurité intérieure autorise à présent la police nationale, la gendarmerie nationale et les militaires des armées à utiliser des drones pour des finalités limitées dont la sécurité des rassemblements des personnes pouvant entraîner des troubles graves à l'ordre public.

UNE MAUVAISE GESTION DU FICHIER AUTOMATISÉ DES EMPREINTES DIGITALES (FAED)

Le FAED est un fichier de police judiciaire d'identification recensant les empreintes digitales de personnes mises en cause dans des procédures pénales. Ces empreintes sont principalement utilisées par les forces de l'ordre dans le cadre de leurs enquêtes.

À l'issue des contrôles effectués auprès des services de la police technique et scientifique et de juridictions (tribunaux judiciaires et cours d'appel), la CNIL a relevé de multiples manquements à la loi Informatique et Libertés. Ainsi, il a été relevé que le FAED contient des données non prévues par les textes telles que par exemple le nom d'une victime ou le numéro d'immatriculation d'un véhicule. En outre, **des données y sont conservées pour une durée excédant celle prévue par les textes et les mentions relatives à des personnes ayant bénéficié d'un acquittement, d'une relaxe, d'un non-lieu ou d'un classement sans suite y sont enregistrées** alors que les fiches les concernant devraient en principe être effacées.

De plus, aucune information n'est délivrée aux personnes concernées dont les empreintes sont prises puis versées au FAED. Enfin, le fichier s'est révélé insuffisamment sécurisé compte tenu de la faible robustesse des mots de passe permettant d'accéder au FAED.

Le 24 septembre 2021, la formation restreinte de la CNIL a donc rappelé à l'ordre le ministère de l'Intérieur et lui a enjoint de prendre les mesures nécessaires à la mise en conformité du FAED, notamment en supprimant les informations ne devant plus y figurer, en s'assurant de leur mise à jour effective, en informant correctement les personnes concernées et en sécurisant davantage le fichier.

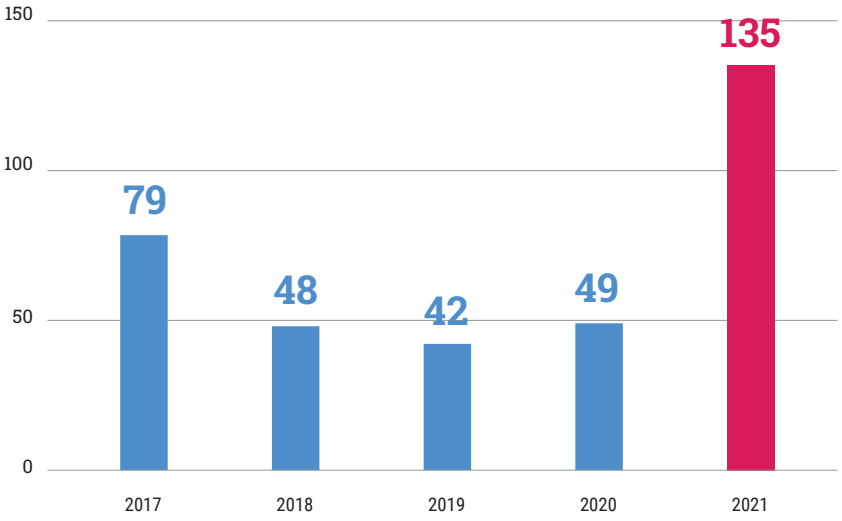
73 « L'analyse d'impact relative à la protection des données (AIPD) », cnil.fr

135 mises en demeure et de nombreuses mises en conformité

Le nombre de mises en demeure (décision de la présidente de la CNIL ordonnant à un organisme de se mettre en conformité) a également fortement augmenté en 2021, avec 135 décisions prononcées, dont 2 rendues publiques à l'encontre de Clearview et de Francetest (voir l'analyse de la CNIL page 101), et 3 adoptées dans le cadre de la coopération européenne.

Une part importante de ces mises en demeure a porté sur la thématique prioritaire des cookies : 89 décisions comportent un manquement en lien avec l'utilisation des traceurs (dont 84 sont pleinement consacrées à cette question).

En parallèle, **la CNIL a clos 123 dossiers** (procédures de sanction et de mise en demeure) à l'issue, notamment, de l'examen des actions prises par les organismes pour se mettre en conformité.



FOCUS

Reconnaissance faciale : mise en demeure de Clearview AI de cesser la réutilisation de photographies accessibles sur internet

La société Clearview AI, établie aux États-Unis, a développé un logiciel de reconnaissance faciale dont la base de données repose sur l'aspiration de photographies et de vidéos publiquement accessibles sur internet et les réseaux sociaux (par exemple, Twitter ou Facebook). Des images sont également extraites de vidéos disponibles en ligne quelles que soient les plateformes (par exemple, sur le site youtube.com). De cette manière, la société s'est appropriée plus de 10 milliards d'images à travers le monde. Ainsi plusieurs millions de personnes en France, y compris des personnes mineures, sont susceptibles d'être concernées par ce traitement dès lors que leur visage apparaît sur une photographie ou une vidéo publiquement accessible sur Internet et notamment sur un compte de réseau social.

Cette collecte permet à la société Clearview AI de commercialiser l'accès à son moteur de recherche où une personne peut être recherchée grâce à une photographie. La société offre notamment ce service à des forces de l'ordre, afin d'identifier des auteurs ou des victimes d'infraction.

À partir de mai 2020, la CNIL a reçu des plaintes de particuliers au sujet du logiciel de reconnaissance faciale de Clearview AI et a ouvert une enquête. En mai 2021, l'association *Privacy International* a également alerté la CNIL sur cette pratique. Au cours de cette procédure, la CNIL a coopéré avec ses homologues européens afin de partager le résultat des investigations, chaque autorité étant compétente pour agir sur son propre territoire en raison de l'absence d'établissement de la société Clearview AI en Europe.

Dans la mesure où le traitement en cause est lié au suivi du comportement des personnes concernées (article 3.2.b) du RGPD), le RGPD est applicable, même si la société n'est pas établie en Europe.

Les investigations menées ont permis de constater deux manquements au RGPD :

- un traitement illicite de données personnelles (article 6 du RGPD) car la collecte des photographies et l'utilisation des données biométriques s'effectuent sans base légale (en l'occurrence, sans le consentement des personnes concernées) ;
- l'absence de prise en compte satisfaisante et effective des droits des personnes, notamment des demandes d'accès à leurs données (articles 12, 15 et 17 du RGPD).

Le 26 novembre 2021, la présidente de la CNIL a mis publiquement en demeure la société Clearview AI de cesser ce traitement illicite et de supprimer les données personnelles des personnes concernées qui se trouvent sur le territoire français dans un délai de 2 mois.

FOCUS

L'action de la CNIL en matière de cookies

Dans le cadre de son plan d'action sur le ciblage publicitaire, la CNIL avait laissé aux organismes un délai de six mois pour mettre leurs pratiques en conformité avec les exigences de l'article 82 de la loi Informatique et Libertés suite à l'adoption, le 17 septembre 2020, de ses nouvelles lignes directrices et de sa recommandation portant sur l'usage des cookies et autres traceurs. Elle avait cependant pris soin de préciser qu'elle continuerait, pendant ce délai, à contrôler le respect des autres obligations relatives aux cookies n'ayant fait l'objet d'aucune modification. À l'issue de cette période d'adaptation qui s'est achevée fin mars 2021, la CNIL a réalisé de nombreux contrôles pour évaluer l'application de l'ensemble des règles relatives aux cookies. Ces contrôles ont donné lieu à des mises en demeure et à des procédures de sanction.
La CNIL a ainsi entendu répondre aux attentes des internautes de plus en plus sensibles aux problématiques de traçage sur internet, comme en témoignent les plaintes constantes qu'elle reçoit sur ce sujet.

Une campagne sans précédent de mises en demeure

Sur l'année 2021, la CNIL a ainsi mis en demeure près de 90 acteurs sur le sujet des cookies. Les vérifications en ligne initiées par la CNIL ont permis de constater, selon les cas, que :

- des cookies soumis à consentement sont automatiquement déposés sur le terminal de l'utilisateur avant acceptation de sa part, dès son arrivée sur le site ;
- des bandeaux d'information ne sont toujours pas conformes car ils ne permettent pas à l'utilisateur de refuser le dépôt de cookies aussi simplement que de l'accepter ;
- des bandeaux d'information offrent à l'utilisateur un moyen de refuser les cookies avec le même degré de simplicité que celui prévu pour les accepter, mais le mécanisme proposé n'est pas effectif car des cookies soumis à consentement sont tout de même déposés après le refus exprimé par l'utilisateur.

Les sanctions prononcées

Brico Privé et Le Figaro : l'internaute doit pouvoir accepter les cookies non essentiels avant leur dépôt

La formation restreinte de la CNIL a prononcé une amende de 500 000 euros à l'encontre de la société Brico Privé, qui édite le site de ventes privées bricoprive.com. Parmi les manquements retenus, la CNIL a notamment constaté que, lorsqu'un utilisateur se rendait sur le site bricoprive.com, plusieurs cookies étaient automatiquement déposés sur son terminal, avant toute action de sa part. Plusieurs de ces cookies étant utilisés à des fins publicitaires, la formation restreinte a considéré que le consentement de l'utilisateur aurait dû être recueilli avant leur dépôt. La société a modifié le fonctionnement de son site web durant la procédure, et plus aucun cookie publicitaire n'est désormais déposé avant que l'utilisateur n'ait donné son accord.

La Société du Figaro a également été sanctionnée d'une amende de 50 000 euros en raison du dépôt de cookies publicitaires sans consentement des internautes. La formation restreinte a considéré qu'en tant qu'éditrice du site web lefigaro.fr, cette société devait s'assurer que ses partenaires ne déposent pas sur son site de cookies soumis au consentement avant que les utilisateurs aient fait un choix et qu'ils respectent leur refus.

Google et Facebook : refuser les cookies doit être aussi simple qu'accepter

La formation restreinte de la CNIL a relevé que si les sites facebook.com, google.fr et youtube.com proposent un bouton permettant d'accepter immédiatement les cookies, ils ne mettent pas en place de solution équivalente (bouton ou autre) pour permettre à l'internaute de refuser facilement le dépôt de ces cookies. Plusieurs clics sont nécessaires pour refuser les cookies, contre un seul pour les accepter.
La formation restreinte a considéré que cela porte atteinte à la liberté du consentement : dès lors que, sur internet, l'utilisateur s'attend à pouvoir rapidement consulter un site, le fait de ne pas pouvoir refuser les cookies aussi simplement que de les accepter biaise le choix en faveur du consentement. Cela constitue une violation de l'article 82 de la loi Informatique et Libertés. S'agissant de Facebook, la formation restreinte a également considéré que le parcours informationnel mis en œuvre par la société n'est pas clair puisque, pour refuser le dépôt de cookies, les internautes doivent cliquer sur un bouton intitulé « Accepter les cookies » figurant dans la seconde fenêtre proposée pour paramétrer les cookies.

Elle a ainsi prononcé :

- deux amendes d'un montant total de 150 millions d'euros à l'encontre de Google (90 millions d'euros pour la société Google LLC et 60 millions d'euros pour la société Google Ireland Limited) ;
- une amende de 60 millions d'euros à l'encontre de la société Facebook Ireland Limited.

En complément des amendes, la formation restreinte a enjoint aux sociétés de mettre à disposition des internautes situés en France, dans un délai de 3 mois, un moyen permettant de refuser les cookies aussi simplement que celui existant pour les accepter, afin de garantir la liberté de leur consentement. À défaut, une astreinte de 100 000 euros par jour de retard devra être payée.


Refuser les cookies doit être aussi simple qu'accepter
La CNIL sanctionne GOOGLE et FACEBOOK
LES INVESTIGATIONS
La CNIL a reçu plusieurs plaintes dénonçant les modalités de **refus des cookies** sur les sites web **facebook.com, google.fr et youtube.com.**
Des contrôles en ligne ont été effectués sur ces sites.
LES MANQUEMENTS
Un bouton permet d'accepter immédiatement les cookies mais **il n'existe pas de solution équivalente pour les refuser aussi facilement**.
Ce procédé porte **atteinte à la liberté du consentement** des internautes et constitue une **violation de l'article 82 de la loi Informatique et Libertés.**
LA DÉCISION
La formation restreinte de la CNIL a prononcé :
- une amende de 60 millions d'euros à l'encontre FACEBOOK ;
- deux amendes pour un montant total de 150 millions d'euros à l'encontre de GOOGLE.
CNIL.

LA JURISPRUDENCE RELATIVE À LA PROTECTION DES DONNÉES PERSONNELLES

Les principales décisions des juridictions nationales et européennes en 2021

Plusieurs juridictions peuvent rendre des décisions qui permettent de préciser un point de droit relatif à la protection des données personnelles : l'ensemble de ces décisions constitue la jurisprudence.
Sans être exhaustive, cette frise revient sur les principales décisions en la matière pour l'année 2021.

2 mars 2021

COUR DE JUSTICE DE L'UNION EUROPÉENNE (ARRÊT DANS L'AFFAIRE H K./PROKURATUUR)

L'accès, à des fins pénales, à un ensemble de données de communications électroniques relatives au trafic ou à la localisation n'est autorisé qu'en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

4 mars 2021

TRIBUNAL JUDICIAIRE DE PARIS

À la suite d'une saisine de la CNIL, le tribunal judiciaire de Paris a demandé aux fournisseurs d'accès à internet (FAI) de bloquer l'accès à un site hébergeant des données de santé de près de 500 000 personnes mises à disposition par un pirate informatique.

12 mars 2021

CONSEIL D'ÉTAT

Le juge des référés rejette la demande de suspension du partenariat entre le ministère de la santé et Doctolib pour la gestion des rendez-vous de vaccination contre la COVID-19.

21 avril 2021

CONSEIL D'ÉTAT

À la suite de l'arrêt de la CJUE dit « LQDN » d'octobre 2020, le Conseil d'État juge que la conservation généralisée des données est aujourd'hui justifiée par la menace existante pour la sécurité nationale, mais ordonne au gouvernement de réévaluer régulièrement la menace qui pèse sur le territoire pour justifier de cette conservation.

25 mai 2021

COUR EUROPÉENNE DES DROITS DE L'HOMME (ARRÊT DANS L'AFFAIRE BIG BROTHER WATCH)

Dans l'affaire de Grande Chambre Big Brother Watch et autres c. Royaume-Uni, la Cour a conclu que certains aspects du régime britannique de surveillance de masse étaient contraires à la Convention européenne des droits de l'homme.

10 juin 2021

CONSEIL D'ÉTAT

Le Conseil d'État clarifie les conditions de publication d'informations relatives au recrutement des travailleurs handicapés dans la fonction publique en considérant que le maintien permanent sur le site internet d'un ministère de ces données personnelles excède ce qui est nécessaire au regard des finalités du traitement en cause et en demandant de prendre des mesures de nature à limiter le traitement des données en cause.

11 juin 2021

CONSEIL CONSTITUTIONNEL

Non-conformité des dispositions relatives à l'accès aux données médicales des fonctionnaires lors de l'instruction des demandes de congé pour incapacité temporaire imputable au service.

23 juin 2021

COUR DE CASSATION

Un dispositif de vidéosurveillance constante destiné à vérifier qu'un salarié exerçant seul son activité en cuisine respecte les règles d'hygiène et de sécurité est disproportionné.

LE CONTENTIEUX DE LA CNIL

Dans certains cas, il est possible de contester les décisions de la CNIL, par exemple des sanctions, devant le Conseil d'État. Dans d'autres cas, des recours peuvent être déposés devant des tribunaux administratifs. La CNIL revient sur les décisions qui ont marqué l'année 2021.

En 2021, 6 recours ont porté contre des délibérations de sanction de la formation restreinte de la CNIL et 7 recours ont été effectués par des plaignants contre des décisions de la présidente de la CNIL de procéder à la clôture de leurs plaintes.

Par ailleurs, la CNIL peut être informée de recours contre des actes réglementaires (arrêtés ou décrets) pris par le gouvernement concernant la mise en œuvre d'un traitement de données personnelles. Elle peut alors émettre des observations en tant qu'observateur. En 2021 elle a ainsi eu communication de 59 recours, notamment 15 contre les décrets prescrivant les mesures générales nécessaires à la gestion de la sortie de la crise sanitaire et 15 contre les décrets relatifs aux traitements de données personnelles dénommés « Enquêtes administratives liées à la sécurité publique » (EASP), « Prévention des atteintes à la sécurité publique » (PASP) et « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP).

Au total, la CNIL a produit 24 mémoires dont 5 en qualité d'observateur, 14 en tant que défendeur et 5 au titre de la mission de la personnalité qualifiée et relatifs au blocage de sites provoquant à des actes de terrorisme ou en faisant l'apologie.

15 juin 2021

COUR DE JUSTICE DE L'UNION EUROPÉENNE (ARRÊT DANS L'AFFAIRE FACEBOOK)

La CJUE précise les conditions d'exercice des pouvoirs des autorités nationales de contrôle pour le traitement transfrontalier de données.

17 juin 2021

COUR DE JUSTICE DE L'UNION EUROPÉENNE (ARRÊT DANS L'AFFAIRE MIRCOM/TELENET)

L'enregistrement systématique d'adresses IP d'utilisateurs et la communication de leurs noms et adresses postales au titulaire des droits intellectuels ou à un tiers afin de permettre d'introduire un recours en indemnisation sont admissibles sous certaines conditions.

22 juin 2021

COUR DE JUSTICE DE L'UNION EUROPÉENNE (ARRÊT DANS L'AFFAIRE LATVIJAS REPUBLIKAS SAEIMA)

Le droit de l'Union sur la protection des données s'oppose à la réglementation lettonne obligeant l'autorité de la sécurité routière à rendre accessibles au public les données relatives aux points de pénalité imposés aux conducteurs pour des infractions routières.

6 juillet 2021

CONSEIL D'ÉTAT

Le juge des référés estime que le passe sanitaire ne porte pas une atteinte grave et illégale au droit au respect de la vie privée ou au droit à la protection des données personnelles.

25 novembre 2021

COUR DE JUSTICE DE L'UNION EUROPÉENNE (ARRÊT DANS L'AFFAIRE STWL)

L'affichage dans la boîte de réception électronique de messages publicitaires sous une forme qui s'apparente à celle d'un véritable courrier électronique constitue une utilisation de courrier électronique à des fins de prospection directe au sens de la directive sur la vie privée et les communications électroniques.

30 décembre 2021

CONSEIL D'ÉTAT

Le Conseil d'État valide la création du traitement automatisé de données personnelles DataJust, système algorithmique analysant la jurisprudence et établissant un référentiel indicatif d'indemnisation des victimes de préjudices corporels.

FOCUS

Cookies : le Conseil d'État valide la sanction de 2020 prononcée par la CNIL contre Google LLC et Google Ireland Limited

Par une décision du 28 janvier 2022[74], le Conseil d'État a confirmé la compétence de la CNIL à prendre des sanctions sur les cookies en dehors du mécanisme de guichet unique. Cette décision fait suite à un recours des sociétés Google LLC et Google ireland LIMITED contre l'amende de 100 millions d'euros prononcée par la CNIL en décembre 2020.

La décision de la CNIL du 7 décembre 2020

Le 7 décembre 2020, la CNIL prononçait une amende d'un montant total de 100 millions d'euros à l'encontre des sociétés Google LLC et Google Ireland Limited, notamment pour avoir déposé des cookies publicitaires sur les ordinateurs d'utilisateurs du moteur de recherche google.fr sans consentement préalable ni information satisfaisante.
Dans sa décision, la CNIL a retenu trois violations à l'article 82 de la loi Informatique et Libertés (transposant la directive « e-Privacy »).
Tout d'abord, la CNIL a relevé que lorsqu'un utilisateur se rendait sur la page google.fr, plusieurs cookies poursuivant une finalité publicitaire étaient automatiquement déposés sur son ordinateur sans action de sa part. Ce type de cookies n'étant pas essentiel au service, la CNIL a considéré que les sociétés n'avaient pas respecté l'obligation de recueillir le consentement des internautes avant le dépôt des cookies.

Ensuite, la CNIL a estimé que le bandeau qui s'affichait en pied de page du moteur de recherche google.fr ne permettait pas aux utilisateurs résidant en France d'être préalablement et clairement renseignés sur le dépôt de cookies, en particulier sur les objectifs de ces cookies et les moyens pour les refuser.

Enfin, la CNIL a considéré que le mécanisme proposé par les sociétés pour refuser les cookies était partiellement défaillant. En effet, lorsqu'un utilisateur désactivait la personnalisation des annonces sur la recherche Google, un cookie publicitaire demeurait stocké sur son ordinateur et continuait de lire des informations à destination du serveur auquel il est rattaché.

L'arrêt du Conseil d'État du 28 janvier 2022

Par sa décision du 28 janvier 2022, le Conseil d'État a confirmé la compétence de la CNIL à prendre des sanctions sur les cookies en dehors du mécanisme de guichet unique prévu par le RGPD[75] et ainsi validé la sanction de la CNIL prononcée à l'encontre des sociétés Google LLC et Google Ireland Limited.

Le Conseil d'État confirme d'abord que le système du guichet unique prévu par le RGPD n'est pas applicable en matière de dépôts de cookies, lesquels sont encadrés par la loi Informatique et Libertés[76].

Il a également relevé que les cookies en cause étant mis en œuvre dans le cadre des activités de Google France, établissement en France des sociétés Google, la CNIL était compétente en vertu de cette loi. Elle n'avait donc pas à transmettre le dossier à l'autorité irlandaise de protection des données (la DPC), qui est l'autorité chef de file des sociétés Google en vertu du RGPD.

Le Conseil d'État a estimé que **l'exclusion du système « guichet unique » en matière de cookies était suffisamment claire pour qu'il n'ait pas besoin de saisir la Cour de justice de l'Union européenne à titre préjudiciel,** comme le lui demandaient les sociétés.

Sur le fond, **le Conseil d'État confirme les trois violations à l'article 82 de la loi Informatique et Libertés sanctionnées par la CNIL :** le dépôt de cookies sans consentement préalable de l'utilisateur, le défaut d'information de l'utilisateur et la défaillance partielle du mécanisme proposé pour refuser les cookies.

Enfin, **le Conseil d'État estime que le montant des amendes prononcées par la CNIL n'est pas disproportionné** au regard de la gravité des manquements, de la portée des traitements et des capacités financières des deux sociétés.

74 « Cookies : le Conseil d'État valide la sanction de 2020 prononcée par la CNIL contre Google LLC et Google Ireland Limited », cnil.fr
75 « Le guichet unique », cnil.fr
76 « Cookies et traceurs : que dit la loi ? », cnil.fr

FOCUS

Conservation des données de connexion : les éclairages apportés par la jurisprudence française et européenne

Le contexte

Le droit français (notamment l'article R10-13 du code des postes et des communications électroniques) impose aux opérateurs de télécommunication de conserver les données de connexion de leurs utilisateurs à des fins de lutte contre la criminalité et le terrorisme. Ces données, parfois appelées « métadonnées » pour les distinguer de celles qui portent sur le contenu des échanges, comprennent trois catégories :

- les données d'identité, qui permettent d'identifier l'utilisateur d'un moyen de communication électronique (par exemple les nom et prénom liés à un numéro de téléphone ou l'adresse IP par laquelle un utilisateur se connecte à internet) ;
- les données relatives au trafic, parfois appelées « fadettes » (factures détaillées), qui tracent les dates, heures et destinataires des communications électroniques, ou la liste des sites internet consultés ;
- les données de localisation, qui résultent du « bornage » d'un appareil par l'antenne relais à laquelle il s'est connecté.

Plusieurs associations actives dans le domaine de la protection des données personnelles ainsi qu'un opérateur de télécoms ont saisi le Conseil d'État de recours contre les décisions du Premier ministre refusant d'abroger les décrets qui prévoient la conservation de ces données et qui organisent leur traitement pour les besoins du renseignement et des enquêtes pénales. Dans le cadre de ces recours, le Conseil d'État a saisi la Cour de justice de l'Union européenne de plusieurs questions préjudicielles aux fins de l'examen de la conformité des règles françaises de conservation des données de connexion au droit européen.

L'arrêt de la CJUE du 6 octobre 2020 (Grande chambre, affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, *French Data Network e.a.*, ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a.)

Par cet arrêt, la Cour de justice a confirmé que le droit de l'Union s'opposait à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation. En revanche, la Cour définit les conditions dans lesquelles un État membre peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant une telle conservation, notamment lorsque l'État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible.

L'arrêt du Conseil d'État du 21 avril 2021 (Assemblée, *French Data Network e.a.*, n° 393099.)

Par cet arrêt, le Conseil d'État juge que certaines dispositions françaises en cause (article R. 10-13 du code des postes et des communications électroniques et certaines dispositions des décrets du 25 février 2011, du 11 décembre 2015 et du 29 janvier 2016) sont contraires au droit européen et doivent être modifiées, dans un délai de 6 mois.

En effet, les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation ne sont pas limitées en droit français à la sauvegarde de la sécurité nationale. Or, une telle conservation n'est justifiée qu'en cas de menace grave pour la sécurité nationale, réelle et actuelle ou prévisible. De plus, elle doit être temporellement limitée au strict nécessaire.

Par conséquent, les dispositions en cause doivent être modifiées afin que l'obligation de conservation faite aux fournisseurs d'accès à internet et aux hébergeurs ait un caractère temporaire et soit liée à l'existence d'une menace grave pour la sécurité nationale. Son renouvellement doit être soumis au constat de la persistance de l'existence d'une telle menace.

Un mécanisme de réexamen périodique de l'existence d'une telle menace doit donc être introduit afin de renouveler les dispositions rendant obligatoire cette conservation généralisée et indifférenciée des données relatives au trafic et à la localisation.

Le Conseil d'État juge également que les dispositions relatives au recours à un recueil en temps réel des données relatives au trafic et des données de localisation doivent être modifiées. En effet, doit être introduit un mécanisme de contrôle préalable, par une autorité administrative indépendante ou une juridiction, de la mise en œuvre des techniques permettant un accès aux données de connexion.

FOCUS

Fuite de données de santé : le 4 mars 2021, le tribunal judiciaire de Paris a demandé le blocage d'un site web

En février 2021, la CNIL a été informée par les médias de la présence sur un forum d'un lien de téléchargement vers un fichier contenant les données médico-administratives de près de 500 000 personnes. Ces données étaient initialement traitées par des laboratoires d'analyse médicale dans leur solution logicielle. Figuraient notamment les noms, prénoms, dates de naissance, adresses, numéros de téléphone, adresses électroniques, mais aussi des informations relatives aux maladies des patients, à l'état de grossesse et aux traitements suivis.

La CNIL a immédiatement diligenté plusieurs contrôles en lien avec cette fuite de données et poursuit actuellement ses investigations. La CNIL a également pris les mesures nécessaires auprès des organismes concernés afin que les personnes dont les données ont été diffusées soient informées de cette violation par les laboratoires dans les meilleurs délais.

En parallèle, la CNIL a saisi le tribunal judiciaire de Paris dans le cadre d'une procédure d'urgence, pour assurer le blocage effectif de l'accès au fichier. Le 4 mars 2021, le tribunal a adopté une décision demandant aux principaux fournisseurs d'accès à internet (FAI) de bloquer l'accès au site internet hébergeant ce fichier mis à disposition par un pirate informatique.

La parole à Romain ROBERT

Directeur de programme chez noyb

En quoi le respect du recueil du consentement des internautes en matière de cookies et de traceurs est-il un enjeu important ?

Ce qui est important, c'est surtout le fait que ce consentement soit éclairé, c'est-à-dire que l'individu soit clairement informé de ce à quoi il consent. Or, c'est précisément là que le bât blesse, dès lors que nous avons pu constater une série de pratiques qui empêchent les utilisateurs de comprendre à quoi ils consentent, qui surprennent leur consentement (en qualifiant un cookie d'essentiel alors qu'il ne l'est pas, par exemple), ou encore qui poussent les utilisateurs à accepter les cookies (ce qu'on appelle les « dark patterns »). Un autre enjeu important, et qui n'était pas abordé par nos plaintes chez noyb, c'est que certains sites ne respectent même pas le choix d'accepter ou de refuser les cookies, pourtant exprimé par les utilisateurs.

Quel bilan noyb tire-t-elle des actions qu'elle a menées en matière de cookies ?

Nous sommes clairement satisfaits de l'effet qu'ont eu les plaintes – ou plutôt les projets de plainte – envoyés aux sites concernés. Une grande proportion des sites contactés ont remédié aux violations visées dans nos plaintes. Les autres sites qui ne se sont pas conformés ont fait l'objet d'une plainte formelle auprès des autorités compétentes. L'automatisation des plaintes était une première pour noyb et ce fut aussi une expérience instructive, que nous espérons pouvoir reproduire dans d'autres domaines. Nous sommes également satisfaits de voir que, de manière générale, les bannières de cookies ont évolué vers un mieux dans leur ensemble, sur beaucoup de sites qui n'avaient pas été visés par une plainte de noyb. Il y a clairement eu un effet de contagion.

Quelles sont les actions envisagées par noyb en 2022 sur ce sujet ?

Comme annoncé au moment de notre campagne, nous avions l'intention de déposer 10 000 plaintes pour août 2022. Vu le taux de conformité atteint après la première vague de plaintes, nous sommes en train de réfléchir à l'opportunité de passer à une autre plateforme que One Trust et d'adapter notre logiciel à cette nouvelle plateforme. Nous réfléchissons également à une manière d'automatiser nos plaintes concernant l'utilisation de SDKs par les téléphones portables, avec une méthode similaire à celle utilisée pour la génération de nos plaintes sur les cookies.

Perspectives

Les grands évènements à venir

air2022 : mineurs, parents et enseignants face à la révolution numérique du monde de l'éducation

Deux ans après le premier confinement, la CNIL souhaite conduire des réflexions éthiques collectives pour interroger les profondes mutations en cours ou à venir du secteur de l'éducation, particulièrement bousculé par la crise sanitaire. L'évènement air2022 sera ainsi l'occasion d'échanger sur la manière dont les professionnels de l'enseignement, notamment au sein de l'éducation nationale et de l'enseignement supérieur, ont vécu cette période, se sont adaptés pour poursuivre leur mission essentielle pour la société et identifier les éventuelles leçons à en tirer.

Le programme, actuellement en cours d'élaboration, sera articulé autour de plusieurs problématiques.

Un premier sujet devrait concerner l'impact des nouveaux outils offerts par le numérique, qu'il s'agisse de la visioconférence, des *learning analytics*, et plus généralement du recours à l'intelligence artificielle, tant dans les pratiques pédagogiques qu'administratives.

Un deuxième sujet devrait traiter des enjeux de souveraineté numérique au regard du poids des GAFAM et de la nécessité d'une alternative européenne en matière d'EdTech.

Enfin, la question de l'éducation au numérique devra également irriguer l'ensemble des travaux, en tant que composante essentielle du droit des mineurs et au regard des révélations de la lanceuse d'alerte France Haugen en octobre dernier sur l'impact des algorithmes des réseaux sociaux sur la santé mentale des jeunes.

La CNIL a fait du thème de l'éducation un sujet prioritaire depuis 2013 en multipliant les actions, notamment à travers son collectif Educnum qui produit de nombreuses ressources pédagogiques pour les enfants et leurs accompagnants éducatifs, parents ou professionnels. L'année 2022 sera aussi l'année du « bac à sable » réglementaire consacré aux EdTechs, la CNIL accompagnera une dizaine de porteurs de projets innovants dans la mise en place de leur *privacy by design*.

INFOS PLUS

Avenirs, innovations, révolutions : la mission éthique de la CNIL

En réponse à la mission qui lui a été confiée par la loi pour une République numérique, la CNIL organise des débats publics autour des nouveaux enjeux du numérique, au croisement d'expertises terrain et scientifiques. Elle a décidé d'intituler cette démarche air, comme avenirs, innovations, révolutions[77].

77 « Avenirs, innovations, révolutions : la mission éthique de la CNIL », cnil.fr

Un nouveau « bac à sable » pour l'innovation numérique dans l'éducation

Une régulation souple, collaborative et proche du terrain

En 2021, la CNIL a décidé de compléter ses outils traditionnels d'appui à l'innovation par la mise en place d'un « bac à sable », dans une logique de régulation souple et ouverte sur des problématiques émergentes. **Ce dispositif a permis un accompagnement renforcé de projets innovants sélectionnés et d'apporter des réponses pragmatiques et de la sécurité juridique sur des problématiques nouvelles.**

Ce dispositif de la CNIL est ouvert à tous les projets innovants, quel que soit le statut (public ou privé) du porteur de projet, sa taille, sa maturité (jeune pousse ou non). Pour être réellement utile, il ne vise pas des projets déjà opérationnels ou commercialisés.

Les outils numériques dans le secteur de l'éducation, le thème pour 2022

Pour cette deuxième édition, le choix de la CNIL s'est porté sur le thème des outils numériques utilisés dans le secteur éducatif. Ce sujet présente de forts enjeux d'actualité (notamment pour la continuité de l'enseignement scolaire et universitaire pendant la pandémie), économiques (les EdTechs sont aujourd'hui un secteur florissant dans l'innovation française et européenne) et sociétaux au regard des droits des personnes (droits des mineurs, inclusion scolaire, etc.).

La mise en place de ce « bac à sable » permettra une meilleure appropriation, par le secteur éducatif du RGPD, dont le respect conditionne le développement d'offres de services et d'outils respectueux de la vie privée. Il permettra également un déploiement des solutions scolaires et universitaires de confiance pour les utilisateurs (enseignants, élèves, parents, étudiants, établissements etc.).

Enfin, ce thème vient consolider le partenariat de la CNIL avec le ministère de l'Éducation nationale, de la Jeunesse et des Sports et les liens noués avec les associations représentatives des acteurs privés du secteur (EdTech France, AFINEF).

Une procédure transparente

En 2022, le dispositif est ouvert à cinq projets innovants et un appel à projet a été ouvert pour sélectionner les lauréats. Quatre critères sont principalement pris en compte :

- l'intérêt du projet pour le public ;
- un engagement fort du porteur de projet pour la conformité RGPD ;
- un projet encore en phase de conception ; et
- l'intérêt pour la protection des données des questions posées par le projet.

Après examen des candidatures, un comité d'évaluation comprenant des membres de la CNIL et des personnalités qualifiées extérieures se réunit pour auditionner les porteurs de projet correspondant le mieux aux priorités de la CNIL.
Pour les cinq projets retenus, l'accompagnement renforcé aura vocation à durer jusqu'à la fin de l'année 2022.

Privacy Research Day : promouvoir les travaux académiques sur la protection de la vie privée

La recherche scientifique, via les publications académiques, est d'un grand soutien pour les régulateurs du numérique. Depuis de nombreuses années, la CNIL met en avant les travaux académiques qui l'éclairent dans sa régulation. C'est particulièrement le cas du prix qu'elle organise depuis de nombreuses années avec l'Inria, mais aussi des articles d'analyse et des interviews qui sont publiés sur le site du LINC. Le 28 juin se tiendra une conférence internationale pour promouvoir les travaux académiques en protection des données.

Une première conférence académique pour la CNIL

Les techniques « masquées » de suivi sur internet comme le *fingerprinting*, les fuites d'informations, les nouveaux types d'attaques mais aussi les technologies émergentes permettant de protéger la vie privée dès la conception (*privacy by design*), sont autant de sujets techniques que la CNIL doit maîtriser.

Si elle suit avec intérêt les travaux académiques et s'en inspire, la CNIL a en revanche rarement l'occasion de faire part à leurs auteurs de son point de vue ou de ses attentes. Afin de stimuler ces échanges, de diffuser les travaux en lien avec la protection de la vie privée mais aussi d'être alerté quand certains échappent à sa veille, de nouveaux modes de communication vont être proposés en 2022.

Le Laboratoire d'innovation numérique de la CNIL (LINC) organisera ainsi le 28 juin 2022 sa première conférence académique : le *Privacy Research Day*. Cet évènement, d'une ampleur inédite en France, est une opportunité pour créer des temps d'échanges entre la communauté scientifique du monde entier et les agents de la CNIL et permettra de mettre en avant des travaux académiques sur la protection des données. Il sera également l'occasion pour la CNIL, et en particulier pour son laboratoire d'innovation, **de nouer des partenariats avec des chercheurs dont les travaux peuvent éclairer la CNIL dans ses missions.**

Au cours de cette journée, des panels se tiendront autour des grands thèmes qui intéressent ou intéresseront la CNIL dans les prochaines années : l'analyse automatisée des vidéos, les apps mobiles, les reventes de données, l'exercice des droits en pratique, l'économie de la donnée, les incitations à se mettre en conformité, les nouvelles formes de discriminations algorithmiques ou encore la surveillance par les pairs.

Ces tables rondes mettront en avant tant les sciences humaines que l'informatique et favoriseront les contributions pluridisciplinaires. Elles devront également répondre à une exigence d'accessibilité, pour que chacun puisse comprendre les présentations quel que soit son propre domaine d'expertise, sa pratique professionnelle.

Les données et l'environnement, un nouveau sujet de préoccupation

Les données, personnelles ou non, sont souvent présentées (à juste titre) comme le nouveau carburant de nos économies. Outre les risques pour la vie privée ou les enjeux économiques, leur utilisation et leur circulation posent aussi des questions environnementales.

Quels sont aujourd'hui les effets de la régulation de la protection des données personnelles sur l'environnement ?

Les conséquences environnementales du numérique font déjà l'objet de nombreux travaux, notamment d'une analyse commune de l'Autorité de régulation des communications électroniques (Arcep) et de l'Agence de l'environnement et de la maîtrise de l'énergie (Ademe) qui a été publiée au mois de janvier 2022[78]. S'il est trop tôt pour prétendre estimer l'empreinte de la protection des données en la matière, on peut anticiper que certaines recommandations techniques vont être énergivores (chiffrement, confidentialité différentielle, etc.), voire consommatrices de ressources matérielles (destruction des disques mis au rebut) quand d'autres – comme la minimisation des données – auraient un impact positif.

Le Laboratoire d'innovation numérique de la CNIL (LINC) a par ailleurs exploré l'articulation entre la protection des données personnelles et le statut de « données environnementales » susceptible d'être attribué à certaines données et qui pourraient être partagées dans le cadre de projet d'intérêt général. Engager de tels processus pose les mêmes questions que le partage de données urbaines ou de santé. Le champ des données environnementales est vaste, les moyens et les dispositifs techniques de collecte mis en place pour leur traitement sont tout aussi divers. La question de leur ouverture ou de la création de communs ne va pas sans risques associés à la protection des données et des libertés, d'autant plus lorsque les citoyens deviennent capteurs, de manière proactive ou plus encore sans en avoir conscience directement. En ce domaine comme ailleurs, la prise en compte de la protection des données ne doit pas être perçue comme un frein, mais agir comme un levier pour engager la participation et l'adhésion des citoyens.

78 « Empreinte environnementale du numérique en France : l'ADEME et l'Arcep remettent leur premier rapport au gouvernement », 19 janvier 2022, arcep.fr

Une exploration à venir

Au cours de 2022, le LINC explorera les liens entre protection des données et environnement, notamment par les « climatopies »[79], récits prospectifs qui mêlent climat et données autour de la question suivante : ***« Alors qu'elle pose pour principe la minimisation des données, et une certaine frugalité, la protection des données pourrait-elle participer de la protection de l'environnement ? »***

De cette question ont émergé trois grands axes prospectifs :

- Et si… demain notre vie était rythmée par les quotas d'émissions, de pollution, de données ?
- Et si… demain l'impact environnemental devenait une donnée publique, pour les particuliers comme pour les entreprises ?
- Et si… demain le monde numérique devait s'adapter à l'écroulement des ressources ?

L'ensemble de ces travaux, du travail documentaire jusqu'à ces futurs imaginés en passant par les échanges des équipes de la CNIL avec les experts du domaine, permettra de publier de nouveaux travaux sur le sujet en 2022.

Alors qu'elle pose pour principe la minimisation des données, et une certaine frugalité, la protection des données pourrait-elle participer de la protection de l'environnement.

79 Ces grandes questions ont guidé la rédaction de six récits, disponibles sur le site climatopie.fr.

Les grands enjeux d'avenir : ces métavers nous bouleversent

Si le projet de métavers promu en 2021 par certains comme le futur de nos interactions numériques ne fait que remettre au goût du jour des dispositifs et des projets anciens, il n'en pose pas moins de nouveaux défis pour la régulation du numérique sous l'angle de la protection des données ainsi que la concurrence. Le metaverse a déjà fait l'objet d'un débat au sein du Comité de la Prospective[80] de la CNIL, et sera sans doute au cœur de nouveaux échanges en 2022.

Vers un « Internet augmenté »

Mark Zuckerberg, PDG du réseau social Facebook, a annoncé fin octobre 2021 sa volonté d'orienter les activités de son entreprise vers le développement des métavers, grâce à « *un ensemble d'espaces virtuels où chacun pourra créer, explorer, échanger avec d'autres personnes qui ne se trouvent pas dans le même espace physique* », au moyen de technologies 3D. Ces annonces, si elles ont fait grand bruit, s'inscrivent dans un mouvement plus général, comme le montre la transformation progressive du jeu vidéo *Fortnite* en espace de vie virtuelle, accueillant concerts de stars et salons de discussions. À la faveur du développement du télétravail occasionné par la pandémie de COVID-19, Microsoft est aussi entré dans la compétition, avec Mesh, une plateforme collaborative pour des « expériences virtuelles » intégrée à Microsoft Teams. D'autres acteurs tels Decentraland ou The Sandbox proposent des modèles décentralisés.

Ces différentes solutions proposent un « internet augmenté » dans lequel les personnes ne se déplacent plus en 2D, mais en immersion. On ne regarde plus l'écran, mais on y entre au moyen de lunettes de réalité virtuelle.

Un concept et des exemples anciens

Le terme de « métavers » est directement tiré de la fiction et du roman de Neal Stephenson : *Le Samouraï Virtuel* (*Snow Crash* en anglais), publié en 1992, dont l'intrigue se déroule dans un univers futuriste, un *« metaverse »* à l'apparence d'un environnement urbain, auquel les utilisateurs peuvent accéder par des terminaux personnels – des lunettes de réalité virtuelle – ou depuis des terminaux publics installés dans des cabines.

Les premières formalisations d'univers virtuels et de formes de métavers se font dans le jeu vidéo, avec l'avènement des « jeux en ligne massivement multijoueur » (MMO), dont les univers sont persistants : le jeu continue à « vivre » même lorsque l'on n'y est pas connecté. Parmi les grands succès on retrouve dès 2004 *World Of Warcraft* (jusqu'à 10 millions d'abonnés en 2014).

INFOS PLUS

Fédivers : l'alter métavers

Bien avant le Métavers de Facebook, le Fédivers (mot valise pour « fédération » et « univers ») a été utilisé pour désigner la fédération de serveurs formant un réseau social, dont les premiers exemples datent de 2008.

Ces services sont construits sur la base de logiciels libres, utilisent des protocoles communs pour échanger entre eux, et permettent notamment l'auto-hébergement, à l'image de Mastodon, Diaspora, XMPP, Peertube, etc.

À partir de 2018, le protocole ActivityPub, normalisé par le W3C, permet d'améliorer les échanges entre ces plateformes et leur interopérabilité.
Ici pas question d'immersion ou de captation de l'attention, à rebours des grandes plateformes du numérique, ces outils naissent de la volonté de fournir des alternatives ouvertes et résilientes aux réseaux sociaux captifs, à la main d'une entité unique.

80 « Les membres du comité de la prospective », cnil.fr

Second Life, quoiqu'en déclin à partir de 2007, reste l'exemple le plus proche de celui proposé par méta : cet univers sorti en 2003 permet aux « résidents » d'incarner des personnages virtuels (avatars) dans un monde en 3D qu'ils peuvent fabriquer eux-mêmes. Une monnaie (convertible en dollars) permet d'y faire des échanges. Plus récemment, des jeux comme *Minecraft* (jeu collaboratif d'aventure et de construction) ou *Fortnite* (plateforme réunissant plusieurs jeux), comportent les caractéristiques de métavers, à la faveur de connexions de plus en plus rapides.

Jusqu'à présent, la limite des métavers était technologique et liée à la capacité à produire des expériences de réalité virtuelle de qualité. Le développement de casques de réalité augmentée et la transformation des interfaces associées y répondent, mais elles ont des conséquences sur les modalités de collectes de données.

Une collecte potentiellement « totale » qui interroge la régulation

La collecte de données permise par le développement des métavers est à priori une version « augmentée » des pratiques de collecte déjà permises par le numérique d'aujourd'hui. Les interactions, mais également l'apparence ou les déplacements pourront être enregistrés. En proposant une immersion « totale » et une intégration complète entre le terminal d'accès et l'univers de services et de contenus, les métavers réduisent la capacité individuelle à échapper à la collecte de données, garantie également par le cadre légal (le RGPD mais aussi le règlement *ePrivacy*).

Parmi les enjeux spécifiques à ces univers, les nouveaux capteurs rendent possible le *eye tracking*, la détection des émotions ou la biométrie comportementale, pour que les avatars reproduisent la manière de se mouvoir des utilisateurs. Ces données générées dans le métavers pourront être nécessaires au métavers lui-même, immense traitement de données, dans lequel divers acteurs produisent des services complémentaires, posant ainsi, au regard du RGPD, les questions de l'identification du responsable de traitement ou de la minimisation des données.

Les exigences de transparence et d'information ou celles liées à l'exercice des droits représentent de grands enjeux, notamment concernant la configuration et la forme des interfaces qui ont un rôle déterminant sur notre capacité à être correctement informés. À cela s'ajoute la multiplicité des acteurs rencontrés dans ces espaces virtuels, qui rendra compliquée l'identification et la répartition des responsabilités concernant les traitements mis en œuvre.

Les métavers pourraient aussi devenir les lieux du développement de la publicité augmentée. Aux données de navigation pourraient s'ajouter des données plus comportementales, comme cela a été anticipé dans le Cahier IP3 de la CNIL et déjà été testé dans le secteur du jeu vidéo pour améliorer l'expérience[81], dans le travail pour déceler le stress des téléopérateurs[82], les émotions des ouvriers en Chine[83]. La voie d'un développement plus large du marketing émotionnel[84] pourrait ainsi être ouverte.

Au-delà, on pourrait assister à de nouveaux modes de vidéosurveillance virtuelle : dans la mesure où des espaces virtuels sont ouverts au public – à la manière du concert sur *Fortnite* – on pourrait imaginer la création de nouvelles formes de vidéosurveillance dans ces espaces, avec l'enregistrement des vidéos, potentiellement associés à la reconnaissance des personnes. Des espaces où, déjà, on assiste à des comportements inappropriés par des « avatars » masculins à l'encontre de femmes, qu'il s'agira de contrôler[85].

Nouvelles « plateformes essentielles » ?

La création d'un métavers par un grand acteur comme Facebook – désormais méta - s'inscrit enfin dans la volonté d'intégration de services proposés par les acteurs dominants du marché : Facebook lui-même (réseau social, messagerie, service de paiement, etc.) Google (compte Google, Youtube, Android), Apple (iOS) et Amazon (vente en ligne, vidéo). Le réseau social, qui ne disposait pas de son système d'exploitation, à l'image de Google et Apple, trouve avec les métavers un moyen de transformer son casque de réalité virtuelle (Oculus Rift) en nouvelle porte d'accès à des gammes de services, permettant l'émergence d'un nouveau « gate keeper » (traduisible par « portier » ou « intermédiaire »).

De ce point de vue, et si les usages s'imposent – les casques de réalité virtuelle restent à ce jour très inconfortables – le métavers de Facebook présente une possible évolution de la notion de « plateforme », en y adjoignant de nouvelles sources de données (capteurs, activités, échanges, etc.). **Il nécessite de ce fait une attention particulière des régulateurs de la protection des données**, mais aussi en matière de concurrence.

81 Lancé dès 2013, le projet Fun II mené en collaboration avec Ubisoft et l'Université Laval au Québec cherchait à « mieux comprendre les émotions des joueurs afin de créer des jeux mieux adaptés ». Les travaux menés auprès de volontaires visaient à « extraire une signature physiologique du plaisir », à partir de données du rythme cardiaque, du regard des joueurs ou de l'expression faciale, ou même sur l'analyse des mouvements.
82 « Affective computing : des casques qui analysent le cerveau », linc.cnil.fr
83 « Captation des émotions : comment vous le direz pourra être retenu contre vous… », linc.cnil.fr
84 « Parce que je le vaux bien ? Enjeux éthiques et juridiques du marketing émotionnel », linc.cnil.fr
85 « *It's Awkward Being a Woman in the Metaverse* » (en anglais), bloomberglinea.com

Le plan stratégique 2022-2024

La CNIL articule son nouveau plan stratégique 2022-2024[86] autour de trois axes prioritaires pour une société numérique de confiance : favoriser le respect des droits, promouvoir le RGPD comme un atout et cibler la régulation sur des sujets à fort enjeux.

Être à vos côtés pour construire une société numérique de confiance

Le plan stratégique de la CNIL 2019-2021 était placé sous le signe de l'entrée en vigueur du RGPD en 2018. La CNIL se donnait pour principal objectif de permettre à chacun de s'approprier les différentes facettes de cette nouvelle réglementation sans équivalent dans le monde.

Elle souhaitait ainsi lui donner tout son potentiel, tout en restant un régulateur efficace, pragmatique et moderne, et en donnant la priorité aux enjeux numériques de la vie quotidienne.

Bientôt quatre ans après l'entrée en application du RGPD, la plupart des entreprises et services publics se sont mobilisés pour répondre à ces enjeux et le nouveau cadre réglementaire est également mieux connu des personnes concernées. De son côté, grâce à un effort continu, la CNIL a adapté son cadre juridique, déployé son expertise technologique et crédibilisé sa politique de sanction. Répondre à toutes les sollicitations et besoins en très forte croissance sur le terrain reste un défi quotidien pour l'institution, ce dont ont pris conscience les pouvoirs publics qui ont ainsi décidé d'augmenter les effectifs de l'autorité de plus de 25 % sur les trois dernières années.

En effet, la numérisation croissante de la vie économique et sociale ainsi que la survenance de la pandémie ont accru les risques pour la vie privée. Par ailleurs, l'omniprésence des grands services du numérique suscite de nouveaux enjeux de régulation. Dans ce contexte, la donnée personnelle est, plus que jamais, le fil rouge de notre quotidien numérique. Face à ces constats, il est indispensable que le RGPD, au travers de la coopération européenne entre autorités, joue pleinement son rôle de levier offensif de conformité et permette un respect effectif des droits des personnes et une égalité concurrentielle entre les acteurs économiques.

C'est dans cette dynamique que s'inscrivent les nouvelles orientations stratégiques de la CNIL pour la période de 2022 à 2024. Ces orientations sont déclinées en trois axes prioritaires :

- **Axe 1** - Favoriser la maîtrise et le respect des droits des personnes sur le terrain.
- **Axe 2** - Promouvoir le RGPD comme atout de confiance pour les organismes.
- **Axe 3** - Prioriser des actions de régulation ciblées sur des sujets à fort enjeu pour la vie privée.

Consciente des attentes liées à son action, la CNIL s'engage à réaliser ses missions au service des droits et libertés des personnes au moyen d'une régulation agile, équilibrée et efficace.

Par ses actions et ses ambitions pour les années à venir, la CNIL aspire à être - plus que jamais - à vos côtés pour construire une société numérique de confiance.

86 « La CNIL publie son plan stratégique 2022-2024 », cnil.fr

Axe 1 : favoriser la maîtrise et le respect des droits des personnes sur le terrain

La protection des droits des personnes sur leurs données personnelles, renforcée par le RGPD, est la mission principale de la CNIL depuis la loi du 6 janvier 1978. Dans la continuité de son précédent plan stratégique, la CNIL se mobilise pour favoriser l'exercice de leurs droits par les personnes.

Cet objectif implique de diffuser auprès du public, notamment avec le support de partenaires opérationnels, les informations et les outils lui permettant de comprendre ses droits et de les exercer. Assurer l'effectivité de ces droits nécessite également une intensification de l'action répressive de la CNIL. Enfin, l'ensemble de ces actions doit être porté en coopération avec le collectif européen pour faire modifier les pratiques de grands acteurs du numérique et fixer de nouveaux standards.

La CNIL se donne quatre objectifs en la matière :

1 - Renforcer l'information et la sensibilisation des personnes pour favoriser l'exercice des droits

La maîtrise des données personnelles par le public suppose une meilleure connaissance de ses droits et implique d'en rendre l'exercice plus aisé. La CNIL intensifiera ses actions de communication et publiera des outils pour faciliter cet exercice, en s'appuyant sur son réseau de partenaires.

2 - Accroître l'efficacité de l'action répressive

Pour assurer l'effectivité des droits des personnes et la conformité des organismes au RGPD, la CNIL doit mettre en œuvre une politique répressive dissuasive et proportionnée dans des délais plus resserrés. Pour cela, la CNIL travaillera à l'adaptation de ses procédures de contrôle, de mise en demeure et de sanction. Elle maintiendra l'instruction des plaintes comme une priorité au cœur de sa stratégie répressive et veillera à réduire les délais d'instruction.

3 - Renforcer le rôle européen de la CNIL et l'efficacité du collectif européen

C'est au niveau européen que se joue la prise en compte de la protection des droits des personnes par les grands acteurs du numérique. La CNIL y a, traditionnellement, un rôle moteur. Elle poursuivra ses efforts de manière déterminée pour accroître l'efficacité du mécanisme de « guichet unique », consolider ses relations avec ses partenaires et pousser des priorités communes d'action au sein du Comité européen de la protection des données.

4 - Prioriser les actions pour protéger les usages du quotidien

Face à des services et des outils numériques parfois complexes et souvent opaques, les personnes ont besoin d'un allié de confiance pour comprendre leur fonctionnement et les enjeux en termes de libertés et de vie privée. La CNIL prendra en compte les besoins concrets du public et lui donnera des outils pour lui permettre de se repérer dans son quotidien numérique.

Axe 2 : promouvoir le RGPD comme atout de confiance pour les responsables de traitement

Au cours des trois dernières années, la protection des données s'est peu à peu imposée dans la culture quotidienne des responsables de traitement (entreprises, administrations, associations, etc.). Afin de prolonger cette dynamique, la CNIL va encore renforcer son offre d'accompagnement en facilitant la compréhension et la prévisibilité du cadre légal, en développant des outils de conformité et en les aidant à se prémunir contre les risques cyber. Elle fera également évoluer sa stratégie d'accompagnement grâce à de nouveaux outils de type « bac à sable ». Au-delà d'une culture de conformité et de ses avantages, elle agira pour que les acteurs publics et privés se saisissent du RGPD comme d'un atout pour leur image ou leur compétitivité.

Cet axe se décline en cinq objectifs :

1 - Renforcer la sécurité juridique des responsables de traitement par des orientations pratiques et claires

Pour assurer leur conformité, les responsables de traitement doivent pouvoir s'appuyer sur la CNIL pour obtenir une clarification de la législation et ainsi être en mesure de décliner les principes de protection des données de manière adaptée à leurs enjeux. La CNIL continuera à produire de la doctrine, en concertation avec toutes les parties prenantes, et la restituera sous une forme accessible, synthétique et opérationnelle.

2 - Développer les outils de certification et de code de conduite

Prévus par le RGPD, ces outils permettent aux responsables de traitement

de prendre en main leur conformité de manière adaptée à leurs spécificités. La CNIL renforcera son dialogue avec les auxiliaires de conformité (porteurs de code, organismes certificateurs) et œuvrera, tant au plan national qu'européen, au développement et à la simplification de ces outils.

3 - Faire de la conformité RGPD la meilleure prévention contre les risques cyber

La cybercriminalité se développe au détriment des entreprises et des administrations mais également des personnes dont les données sont corrompues ou exposées. Par ses missions en matière de sécurité des données et son expertise technologique, la CNIL renforcera son rôle dans la réponse des pouvoirs publics au risque cyber.

4 - Renforcer et faire évoluer la stratégie d'accompagnement

Les responsables de traitement ont besoin d'outils d'accompagnement transparents, accessibles, adaptés à leurs enjeux. La CNIL poursuivra la transformation de sa stratégie d'accompagnement, en appui à l'innovation (« bac à sable », stratégie « start-up », accompagnement renforcé).

5 - Assumer un rôle de régulateur ayant un impact économique

Une protection efficace des données personnelles va de pair avec la compréhension des modèles d'affaires et de l'impact économique des choix de régulation. La CNIL poursuivra le développement en interne d'une expertise économique appuyée sur des compétences d'analyse et sur l'évaluation de ses actions.

Axe 3 : nos priorités face à l'intensification des usages des données personnelles

Aujourd'hui, chacun peut mesurer la place occupée par le numérique dans notre quotidien et dans le débat public. Les technologies utilisées reposent de plus en plus sur une collecte et un traitement intensif des données.

Elles suscitent parallèlement des usages de plus en plus variés et qui évoluent très rapidement. Pour répondre à ces défis en tant que régulateur de référence dans l'univers numérique, la CNIL mettra en place un plan d'action global sur trois thématiques prioritaires.

Comme elle a pu le faire pour les cookies, elle commencera sa stratégie de mise en conformité par une phase de fixation de la doctrine. Une deuxième phase permettra l'établissement avec le secteur concerné d'outils pratiques d'aide à la conformité.

Enfin, la CNIL conduira des campagnes de contrôles et adoptera si besoin des mesures correctrices. L'objectif est d'aboutir à une mise en conformité des pratiques d'un secteur sur deux ou trois ans.

Trois thématiques prioritaires ont été retenues :

1 - Les caméras augmentées et leurs usages

Le développement accéléré sur le terrain des caméras dites « augmentées », souvent couplées à des algorithmes prédictifs, pose la question du caractère nécessaire et proportionné de ces dispositifs et fait courir le risque d'une surveillance à grande échelle des personnes. La CNIL mettra en œuvre un plan d'action qui concernera autant les usages régaliens (police/justice) que commerciaux et qui comportera une phase d'accompagnement des acteurs.

2 - Les transferts de données dans l'informatique en nuage (cloud)

Le transfert de données constitue un véritable enjeu de sécurité et de conformité pour les utilisateurs français de solutions d'informatique en nuage des grands acteurs du numérique, mais aussi d'un enjeu de souveraineté numérique européenne. Le plan d'action de la CNIL sur ce sujet, en coopération avec ses homologues européens, permettra, sur le fondement de l'arrêt dit « Schrems II », de sécuriser les transferts de données personnelles des Français vers des pays en dehors de l'Union européenne.

3 - Les collectes de données personnelles dans les applications des smartphones

Face à l'opacité des technologies et à l'hétérogénéité des pratiques, l'objectif de la CNIL est de rendre visibles les flux de données et renforcer la conformité des applications mobiles et de leurs écosystèmes, pour mieux protéger la vie privée des utilisateurs d'ordiphones (smartphones). Le plan d'action qu'elle adoptera comprendra des thèmes d'intervention ciblés, une sensibilisation des usagers et une déclinaison européenne de l'approche.

Vie de la CNIL : dévoilement de la tapisserie commandée au Mobilier national

Carton de tapisserie
«Sans titre», *Julien Prévieux, 2017*

En 2017, la CNIL commandait au Mobilier national une tapisserie pour commémorer son 40e anniversaire, célébré en 2018.

4 ans plus tard, l'oeuvre réalisée d'après un carton original de Julien Prévieux et réalisée par la manufacture nationale de Beauvais a été installée dans les locaux de la CNIL.

La cérémonie de dévoilement a eu lieu le 20 octobre 2021 en présence de l'artiste, d'Emmanuel Pénicaut, directeur de la production du Mobilier national, d'Isabelle Falque-Pierrotin, présidente de l'autorité nationale des jeux et anciennement présidente de la CNIL à l'origine de la commande, et de Marie-Laure Denis, présidente de la CNIL.

Cet évènement a également permis de réunir celles et ceux qui ont contribué à la réalisation de ce projet de longue date : le chef d'atelier de la manufacture nationale de Beauvais, la cheffe de pièce de la tapisserie ainsi que les commissaires et agents de la CNIL ayant participé au jury et aux ateliers d'oculométrie proposés par Julien Prévieux lors de la préparation de son carton.

À propos de l'oeuvre :
À travers son carton, composé à la suite d'une analyse approfondie du travail des agents de la CNIL, l'artiste Julien Prévieux a souhaité évoquer la complexité des flux des données et les différentes couches entremêlées du « déluge numérique » auquel la CNIL et notre société contemporaine sont confrontées.

C'est sur la base de ce «carton» que les liciers de la manufacture de Beauvais ont réalisé la tapisserie aujourd'hui exposée dans les locaux de la CNIL.

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