Protéger les données de chacun pour sécuriser l'avenir numérique de tous

COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

–

RAPPORT ANNUEL 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Sommaire

Introduction

LA CNIL, RÉGULATEUR DES DONNÉES PERSONNELLES 4

SES VALEURS EN 4 MOTS CLÉS 4

SES MISSIONS 5

CONTACTER LA CNIL 5

AVANT-PROPOS DE MARIE-LAURE DENIS, PRÉSIDENTE DE LA CNIL 6

CHIFFRES CLÉS 9

LES TEMPS FORTS 2024 10

L'ÉCLAIRAGE DU SECRÉTAIRE GÉNÉRAL ET DU SECRÉTAIRE GÉNÉRAL ADJOINT 12

LE COLLÈGE DE LA CNIL 14

LES MEMBRES DE LA CNIL 16

ORGANIGRAMME DES DIRECTIONS ET SERVICES 18

1. Un accompagnement en phase avec les évolutions sectorielles et technologiques 21

OUTILS D'ACCOMPAGNEMENT DE LA CNIL 22

APPLICATIONS MOBILES 24

SURVEILLANCE 26

JEUX OLYMPIQUES ET PARALYMPIQUES 26

ÉLECTIONS EUROPÉENNES ET LÉGISLATIVES 27

BRÈVES ET CHIFFRES CLÉS 28

Mentions légales

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 :
La Netscouade / www.lanetscouade.com

Impression : Direction de l'information légale et administrative

Conception éditoriale : Citizen press

Crédits photos :
John Nguyen : pages 7, 15
William Parra (Jon Cherki) : page 23
Gezelin Gree : page 57
Juliette Leclercq : page 61

Date de publication : Avril 2025

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.

2. Une intensification de l'action répressive 29

PLAINTES ET DEMANDES D'EXERCICE INDIRECT DES DROITS (EDI) 30

CONTRÔLES DE LA CNIL 32

SANCTIONS ET AUTRES MESURES RÉPRESSIVES 34

3. L'indispensable encadrement de l'IA et des algorithmes 37

RÉGLEMENT IA 38

PREMIÈRES RECOMMANDATIONS DE LA CNIL 39

CONCILIER IA GÉNÉRATIVE ET RGPD 40

COMMENT UNE INTELLIGENCE PIÈGE LES UTILISATEURS TROP CONFIANTS 41

LES RISQUES DE L'IA DANS LE CADRE DES HYPERTRUCAGES 42

JOURNÉE DE RECHERCHE SUR LA VIE PRIVÉE 42

4. L'éducation au numérique et la protection des mineurs 43

PARTENARIATS DE LA CNIL POUR S'ADRESSER AUX MINEURS ET À LEURS FAMILLES 44

LA CNIL CONTRIBUE AUX TRAVAUX SUR LE NUMÉRIQUE ET LES JEUNES 45

SENSIBILISER ET ACCOMPAGNER TOUS LES PUBLICS 48

5. La sécurité des données face à des risques de plus en plus élevés 49

DES VIOLATIONS DE DONNÉES D'UNE AMPLEUR INÉDITE 50

LA NOTIFICATION À LA CNIL 51

NOUVELLE ÉDITION DU GUIDE SÉCURITÉ 52

SÉCURITÉ SUR LE CLOUD 53

L'ACCÈS AU DOSSIER PATIENT INFORMATISÉ 54

6. Des coopérations renforcées en France, en Europe et à l'international 55

PARTENARIATS EN FRANCE 56

COOPÉRATION EUROPÉENNE 58

ACTIONS AU NIVEAU INTERNATIONAL 59

7. Les ressources humaines et financières 60

UNE MAITRISE BUDGÉTAIRE MAINTENUE 61

LES RESSOURCES HUMAINES 63

La CNIL, régulateur des données personnelles

3 dates clés

1978 : naissance de la CNIL

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle a été créée par la loi Informatique et Libertés du 6 janvier 1978, bien avant la généralisation d'Internet et de l'intelligence artificielle générative ! Son rôle : veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papier, aussi bien publics que privés. Au quotidien, la CNIL s'assure que l'informatique est au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

2004 : des pouvoirs supplémentaires

Transposant une directive européenne, la France fait le choix, symbolique, de maintenir la loi pionnière Informatique et Libertés tout en la remaniant profondément. La loi du 6 août 2004, qui porte ces évolutions, octroie notamment de nouveaux pouvoirs d'intervention à la CNIL, tant en ce qui concerne les investigations sur place que les sanctions. Elle peut désormais prononcer une sanction pécuniaire (sauf à l'encontre de l'État), une injonction de cesser le traitement ou encore retirer son autorisation.

2018 : entrée en vigueur du RGPD

Nouvelle adaptation de la loi Informatique et Libertés pour une mise en conformité avec les dispositions du règlement général sur la protection des données (RGPD), applicable dans l'Union européenne depuis le 25 mai 2018. Ce règlement renforce le contrôle des citoyens sur l'utilisation qui peut être faite de leurs données. Les missions de la CNIL évoluent afin de les adapter à la nouvelle logique de responsabilisation et d'accompagnement des acteurs traitant des données. Ses pouvoirs de contrôle et de sanction se voient aussi précisés et étendus.

Ses valeurs en 4 mots clés

Indépendance :
autonomie décisionnelle et pouvoir d'action

Conviction :
engagement, dialogue, sens de l'intérêt général

Expertise :
compétence, qualité, exigence

Collégialité :
collectif, compromis, pluridisciplinarité

Ses missions

Informer et protéger les droits

La CNIL répond aux demandes des particuliers et des professionnels. Elle 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 et elle met à disposition des outils pédagogiques et pratiques. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits ou si elle estime qu'il y a une atteinte à ses données personnelles.

298 agents
en 2024

28,2 M€
de budget en 2024

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 adaptée à leurs tailles et à leurs besoins (référentiels, recommandations, guides pratiques, modèles, fiches pratiques, etc.). Elle peut également être saisie par différents acteurs publics sur des projets de texte (lois, décrets, etc.) avant leur adoption. Elle conseille tout particulièrement le gouvernement, qui doit obligatoirement demander son avis pour certains projets.

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 protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de protection de la vie privée dès la conception. La CNIL participe également à l'animation d'un débat de société sur les enjeux éthiques des données.

Contrôler et sanctionner

Les contrôles (sur place, sur pièces, sur audition et en ligne) permettent à la CNIL de vérifier la mise en œuvre concrète de la loi par les acteurs publics et privés. Le choix de procéder à un contrôle s'effectue en fonction des plaintes reçues par la CNIL, de l'actualité et d'un programme annuel élaboré sur la base de thématiques pour lesquelles un enjeu de protection des données a été identifié. La CNIL peut imposer à un acteur de régulariser son traitement et prononcer des mesures correctrices (mises en demeure, amendes, injonctions, etc.).

Contacter la CNIL

En ligne, via les formulaires de contact sur cnil.fr, rubrique Nous contacter

Par téléphone, tous les jours ouvrés de 9h30 à 17h00 : 01 53 73 22 22

Par courrier :
CNIL,
3 place de Fontenoy,
TSA 80715, 75334
PARIS CEDEX 07

Avant-propos de
Marie-Laure Denis
présidente de la CNIL

Quelles sont les réalisations phares de la CNIL pour l'année 2024 ? Que retenez-vous en particulier ?

Tout d'abord, je ressors de l'année écoulée avec le sentiment que les sujets sur lesquels la CNIL est sollicitée, voire parfois apostrophée sur les réseaux sociaux, augmentent sans cesse, avec un renouvellement permanent des questions posées et une technicité accrue. Au début de mon second mandat et avec le recul du premier, je mesure que la CNIL régule un domaine, le numérique, qui implique qu'elle soit toujours en mouvement, dans une dynamique d'amélioration et de questionnement continus. C'est passionnant et motivant, d'autant plus que j'ai la chance de travailler avec un Collège et des agents compétents et motivés.

Ensuite, il est difficile d'isoler quelques actions en particulier, surtout au regard de la multiplicité et de la variété des missions de la CNIL, qui vont de l'éducation au numérique, en passant par le conseil au gouvernement et l'accompagnement des organismes dans l'utilisation des données, à l'instruction des plaintes et le recours à des mesures répressives pour stopper des pratiques non conformes.

Pour autant, en préparant ce rapport annuel, quatre actions me paraissent particulièrement notables en ce qu'elles témoignent soit d'un investissement particulier de l'institution, soit d'une évolution stratégique dans la mobilisation de ses pouvoirs.

La première concerne le plan d'action relatif aux applications mobiles. À l'issue d'une large consultation publique, la CNIL a publié le 24 septembre 2024 la version finale de ses recommandations pour aider les professionnels à concevoir des applications mobiles respectueuses de la vie privée. Elle mènera dès 2025 une campagne de contrôles. Il s'agit de l'aboutissement de travaux initiés en 2022 et qui s'appuient sur une méthode de régulation efficace, initiée sur les cookies, et consistant à échanger avec les parties prenantes, à clarifier le cadre légal et ensuite à effectuer des vérifications sur le terrain.

La seconde est relative à la procédure de sanction simplifiée introduite dans la loi Informatique et Libertés en 2022 et permettant d'adopter de manière accélérée des amendes avec un plafond de 20 000 euros pour des affaires ne présentant pas de difficulté particulière. En l'espace de trois ans, cette modification de la loi a permis de passer de 21 sanctions en 2022 à 87 en 2024 et ainsi d'assurer une meilleure réactivité et effectivité de l'action répressive de la CNIL, en particulier concernant les plaintes.

La troisième est liée aux actions de terrain menées dans le cadre de l'éducation au numérique et à la sensibilisation du public aux enjeux de protection des données. Ce sont ainsi 173 actions de sensibilisation qui ont été menées en 2024 auprès de l'ensemble des publics sur la France entière, dont près de la moitié (84) auprès de jeunes et d'acteurs entourant la jeunesse (parents, enseignants, éducateurs, animateurs, etc.).

Enfin, l'année 2024 a marqué la fin du plan stratégique 2022-2024 et l'élaboration d'un nouveau plan pour la période 2025-2028.

Quel bilan peut-on dresser du précédent plan stratégique 2022-2024 ?

Pour mémoire, le plan stratégique 2022-2024 a été élaboré au sortir de la pandémie avec le constat que la numérisation croissante de la vie économique et sociale s'était accélérée, entraînant avec elle des risques accrus pour la vie privée.

Pour faire face à ces enjeux, la CNIL avait identifié trois axes prioritaires pour orienter son action. Le premier visait à favoriser la maîtrise et le respect des droits des personnes sur le terrain. Le second avait pour ambition de promouvoir le RGPD comme atout de confiance pour les organismes. Enfin, le dernier axe consistait à prioriser des actions de régulation ciblées sur des sujets à forts enjeux pour la vie privée. Ces trois axes avaient été déclinés en 12 objectifs, eux-mêmes traduits en 48 actions clés sous la forme d'une feuille de route opérationnelle afin d'assurer une mise œuvre concrète de ce plan stratégique.

La préparation du nouveau plan stratégique a été l'occasion de passer en revue ces différentes actions et de faire un bilan de ces dernières années.

Ainsi, sur la période 2022-2024, s'agissant de favoriser la maîtrise de leurs droits par les personnes, la CNIL a traité presque 45 000 plaintes, répondu par téléphone et écrit à environ 170 000 demandes. De même, afin de promouvoir le RGPD auprès des organismes, la CNIL a produit une quarantaine de guides, référentiels et recommandations et traité presque 4 500 demandes de conseils. Enfin, la CNIL a mené des actions de régulation ciblées, notamment sur les traceurs et les cookies, conduisant à des effets structurels de mise en conformité à l'échelle française, voire européenne, le cas échéant en ayant recours à ses pouvoirs de contrôle et de sanction. À cet égard, sur la période écoulée, la CNIL a adopté 495 mises en demeure et 150 sanctions, pour un montant cumulé de plus de 245 millions d'euros d'amende.

Comment le nouveau plan stratégique 2025-2028 s'est-il construit ? Dans quel état d'esprit ?

–

Je souhaite tout d'abord souligner qu'il s'agit d'un travail collectif qui a mobilisé tant le Collège de la CNIL et ses 18 commissaires, que l'ensemble des agents de la CNIL. Ce nouveau plan stratégique est ainsi le fruit d'échanges au sein de l'institution et d'expériences recueillies, y compris sur le terrain, dans la mise en œuvre de nos missions.

S'agissant de l'état d'esprit, l'objectif est de se mobiliser sur des sujets à forts enjeux qui permettent d'agir dans une triple temporalité, c'est-à-dire à court, moyen et long terme. L'idée est de mener des actions concrètes dès l'adoption du plan, tout en menant des tâches de fond visant des transformations plus systémiques. Il faut pouvoir avoir des effets immédiats pour les citoyens et les entreprises, mais aussi une influence sur des écosystèmes, des marchés ou des politiques publiques, ce qui nécessite plus de temps.

« C'est en améliorant le niveau de maturité de chacun que nous pourrons augmenter la sécurité globale. »

Marie-Laure DENIS
présidente de la CNIL

Quels sont les grands axes d'action identifiés pour la période 2025-2028 ? Qu'est-ce qui a justifié leur choix ?

–

À vrai dire, les grands axes d'action se sont assez facilement imposés car ils répondaient à la fois à des enjeux de société et à la nécessité d'une mobilisation dans le temps.

Le premier concerne l'intelligence artificielle et l'avènement de l'IA générative. Ce thème était évident, il s'agit non seulement de la nouvelle révolution numérique comparable à l'essor de l'Internet grand public au début des années 2000, mais aussi d'une technologie qui repose sur l'exploitation massive de données, souvent personnelles.

Ce choix s'inscrit dans le prolongement de travaux de fond de la CNIL (fiches pratiques, webinaires, colloques…) destinés à clarifier le cadre légal, dialoguer avec l'écosystème et développer des capacités d'audit des systèmes. Notre but est de favoriser une intelligence artificielle respectueuse des droits des personnes et d'articuler le RGPD avec le règlement européen sur l'IA.

Le second porte sur la protection des plus jeunes face aux risques liés à la surexposition aux écrans. Cette hyperconnectivité, à un âge de plus en plus précoce, s'accompagne de risques majeurs notamment en matière de protection de la vie privée, de sécurité en ligne et de ciblage publicitaire.

À cet égard, la protection de la vie privée des enfants constitue une priorité absolue justifiant la mobilisation de moyens importants. La mise en œuvre de cet axe doit non seulement permettre de promouvoir un environnement numérique plus sûr et favorable au développement des enfants, mais également de former les citoyens numériques de demain.

Le troisième se rapporte à la cybersécurité. Là encore, il aurait été difficile de ne pas le retenir dans un contexte de multiplication des violations à grande échelle en 2024 qui renforce l'inquiétude des personnes sur l'usage de leurs données.

Au travers du plan stratégique 2025-2028, l'ambition de la CNIL est d'aider les organismes et les individus à prendre la mesure des risques et à recourir à des solutions et des outils adaptés. C'est en améliorant le niveau de maturité de chacun que nous pourrons augmenter la sécurité globale.

Enfin, en complément de son action sur ces trois axes, la CNIL se mobilisera sur deux thématiques prioritaires au centre des usages numériques du quotidien, d'une part, les applications mobiles pour lesquelles j'ai évoqué le plan d'action, d'autre part, les systèmes d'identité numérique.

Concrètement, comment la CNIL va assurer la mise en œuvre de ce plan et notamment, garantir le développement de systèmes d'IA respectueux des droits et libertés ou encore remédier à la multiplication des violations massives de données ?

–

D'un point de vue méthodologique, nous avons de nouveau fait le choix de traduire les quatre axes du plan stratégique en objectifs (14) qui sont eux-mêmes déclinés en une quarantaine d'actions clés. Comme pour le précédent plan, cette méthode doit nous permettre de garantir une mise en œuvre concrète des différents axes, notamment ceux relatifs à l'IA et à la cybersécurité, et de pouvoir la mesurer objectivement.

Sur le fond, pour promouvoir une IA respectueuse des droits tout en préservant les capacités d'innovation, la CNIL va agir dans quatre directions : en consolidant sa compréhension et son expertise en matière d'IA, en continuant à clarifier le cadre juridique dans le cadre des travaux européens et à accompagner les entreprises, en sensibilisant le grand public aux enjeux de l'IA et à l'exercice de leurs droits et en concevant et mettant en œuvre une méthodologie et des outils permettant de contrôler la conformité des systèmes d'IA.

Concernant la cybersécurité, la collaboration et la coordination avec les différents acteurs de l'écosystème comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Cybermalveillance.gouv.fr ou la section « cyber » du parquet de Paris J3 sont décisives. Il faut ensuite accompagner les individus et les organismes face aux violations de données en leur diffusant des outils pratiques (guides, recommandations, etc.) et contribuer au développement de solutions techniques favorisant la protection de la vie privée dès la conception. Enfin, la CNIL devra accroitre les opérations de contrôle à l'issue de violations de données pour vérifier la mise en œuvre de mesures correctives adaptées et, si besoin, réévaluer ses recommandations en matière de sécurité.

« Fluidifier la coopération européenne pour renforcer la protection des données personnelles dans le nouvel environnement numérique européen. »

Marie-Laure DENIS
présidente de la CNIL

Quelle forme va prendre l'engagement de la CNIL à l'échelle européenne et internationale dans un contexte de multiplication des législations sur le numérique ?

–

La stratégie européenne et internationale de la CNIL s'inscrit dans le prolongement d'une volonté historique de prendre en compte les enjeux internationaux et européens de la protection des données personnelles pour s'assurer de la protection des personnes en France, en Europe et au-delà.

En plus de sa mobilisation au quotidien dans les travaux du Comité européen de la protection des données (CEPD) ou d'enceintes internationales comme l'Assemblée mondiale pour la protection de la vie privée (*Global Privacy Assembly*, GPA), la CNIL a élaboré une stratégie pour donner un cap à son action européenne et internationale à l'instar du plan stratégique global que j'évoquais précédemment.

En synthèse, deux grandes orientations peuvent être mises en exergue.

La première vise à fluidifier la coopération européenne pour renforcer la protection des données personnelles dans le nouvel environnement numérique européen. À ce titre, la CNIL va notamment maintenir une implication importante dans les travaux du CEPD et participer à la coopération européenne inter-réglementaire avec ses homologues comme elle le fait par exemple en prenant part aux travaux pour l'élaboration d'un code de conduite sur l'IA piloté par la Commission européenne ou en collaborant avec l'Arcom dans le cadre de la mise en œuvre du règlement sur les services numériques.

La seconde doit permettre de garantir des standards internationaux de protection des données personnelles élevés. Ainsi, dans le cadre de sa participation à de nombreuses instances internationales intergouvernementales, comme le Conseil de l'Europe ou l'Organisation de coopération et de développement économiques (OCDE), la CNIL va œuvrer à diffuser le modèle de protection et de régulation du RGPD.

Dans les deux cas, un des principaux objectifs est de consolider l'influence européenne et internationale de la CNIL en portant un modèle de protection des données personnelles centré sur l'équilibre entre innovation et protection des personnes.

Chiffres clés

Contrôler & sanctionner

321
contrôles

64 rappels
aux obligations légales
de la présidente

180
mises en demeure

87
sanctions

55 212 400 €
d'amendes

Accompagner & conseiller

16 auditions
parlementaires

21 questionnaires
adressés au parlementaire
ou à un parlementaire
en mission

101 délibérations
dont 68 avis
sur projets de texte

1 448
demandes de conseil traitées

Anticiper & innover

1 700
participants à l'événement *air2024*

1 400
participants au *Privacy Research Day*

Informer & protéger

38 386
appels répondus

15 639
plaintes traitées

16 130
demandes d'information écrites traitées

15 350
plaintes reçues en données nettes*

24 947
demandes d'exercice
des droits indirect (EDI) reçues

14 654
demandes d'EDI traitées

11,6
millions de visites sur les sites
web cnil.fr et linc.cnil.fr

5 629
notifications de violation
de données personnelles

* Les statistiques agrégées sont exprimées en données nettes : des données brutes sont exclues, les affaires dites de « série » correspondant à un grand nombre de plaintes dirigées contre un même responsable de traitement et relatives à des faits analogues.

Les temps forts 2024

Janvier

29 janvier
Début à Marseille d'une semaine inédite d'éducation au numérique dans les écoles primaires. En partenariat avec la Ville de Marseille, les agents de la CNIL sont intervenus dans 8 écoles auprès de 52 classes.

Février

7 février
Une violation de données touche deux opérateurs de tiers payants. La CNIL ouvre une enquête et rappelle à des millions d'assurés les précautions à prendre.

9 février
Mise en demeure de plusieurs établissements de santé de prendre les mesures permettant d'assurer la sécurité du dossier patient informatisé.

19 février
Signature d'un partenariat avec la Conférence des grandes écoles pour poursuivre les actions de sensibilisation et d'information sur la protection des données personnelles.

Mars

13 mars
Publication d'un guide RGPD réalisé avec les professionnels des affaires et des relations publiques.

26 mars
Nouvelle édition du guide de la sécurité des données personnelles.

Avril

9 avril Journée RGPD à Lille.

17 avril Payer ou consentir ? Le Comité européen de la protection des données (CEPD), qui réunit la CNIL et ses homologues européens, adopte un avis mettant en avant la nécessité pour les grandes plateformes concernées de donner un véritable choix aux utilisateurs.

25 avril Observations sur le texte instituant un laissez-passer à l'occasion des Jeux olympiques et paralympiques 2024. La CNIL adresse des recommandations sur l'utilisation de la photographie et sur les durées de conservation des données.

Mai

16 mai
Lancement d'une consultation publique sur les référentiels santé pour mieux accompagner les professionnels du secteur dans leurs démarches de conformité.

Juin

4 juin Troisième édition de la « Journée de recherche sur la vie privée » (*Privacy Research Day*) organisée à Paris.

12 juin Journée RGPD à Nancy.

27 juin Signature d'une convention avec l'Arcom et la DGCCRF pour la mise en œuvre du règlement sur les services numériques. Ce texte européen apporte une meilleure protection contre les contenus illicites et dangereux en encadrant les activités des grandes plateformes numériques.

Juillet-Août

12 juillet Parution au Journal officiel de l'Union européenne du règlement européen sur l'IA (RIA) visant à **encadrer le développement, la mise sur le marché et l'utilisation de systèmes d'IA.**

18 juillet Publication d'une première série de questions-réponses pour aider les différents acteurs à concilier IA générative et RGPD.

22 juillet En coopération avec la CNIL, l'autorité néerlandaise de protection des données prononce une amende de 290 millions d'euros contre UBER B.V. et UBER TECHNOLOGIES INC. pour avoir transféré des données personnelles hors UE sans garanties suffisantes.

26 juillet Ouverture des Jeux olympiques 2024. Avant, pendant et après l'événement, la CNIL contrôle les dispositifs utilisés pour la sécurité des sites (QR codes, caméras de vidéoprotection « augmentée ») ou encore la gestion des données des spectateurs, participants et volontaires.

Septembre

23 septembre Choix des 4 entreprises qui bénéficieront d'un accompagnement renforcé durant six mois : Docaposte, Doctrine, la Française des Jeux et ShareID.

24 septembre Publication de recommandations pour aider les professionnels à concevoir des applications mobiles respectueuses de la vie privée.

Octobre

7-11 octobre À Rome, les autorités de protection des données du G7 adoptent une position commune sur leur rôle dans la promotion d'une IA digne de confiance et soulignent l'importance de la protection des mineurs dans ce contexte.

25 octobre Free annonce avoir été victime d'un des plus importants vols de données en France en 2024. Parmi les données dérobées figurent des coordonnées bancaires pouvant mener à des exploitations frauduleuses ou des usurpations d'identité.

Novembre

14 novembre Amende de 50 millions d'euros à l'encontre de la société Orange pour avoir affiché des publicités dans son service de messagerie électronique sans le consentement des utilisateurs.

15 novembre Lancement du concours « Trophées des classes » avec le ministère de l'Éducation nationale pour promouvoir une culture citoyenne des usages du numérique.

18 novembre Signature avec la DGCCRF d'un nouveau protocole de coopération renforçant la collaboration et l'échange d'informations.

19 novembre Journée de réflexions air (Avenir, Innovations, Révolutions) organisée à Paris avec la Commission nationale de contrôle des techniques de renseignement (CNCTR).

Décembre

4 décembre Journée RGPD à Montpellier.

5 décembre Mise en demeure de 6 communes pour qu'elles mettent fin à des manquements constatés dans l'utilisation de caméras augmentées permettant l'analyse en temps réel du comportement des personnes filmées sur la voie publique.

17 décembre Signature d'un partenariat avec France Télévisions pour mieux informer et sensibiliser le grand public aux enjeux soulevés par le numérique.

18 décembre Le CEPD adopte un avis sur le traitement de données personnelles pour le développement et le déploiement de modèles d'IA. Il s'agit de la première position européenne et harmonisée en la matière.

L'éclairage
du secrétaire général et du secrétaire général adjoint

Une nouvelle organisation effective

En 2019, une première adaptation des services de la CNIL avait été effectuée pour répondre au déploiement du RGPD. Depuis, plusieurs tendances ont été confirmées et notre organisation ne nous permettait pas de nous projeter efficacement sur certaines nouvelles missions ou de suffisamment faire évoluer notre action sur des missions historiques. Un projet de réorganisation a ainsi été initié à la demande de la présidente de la CNIL. Il a fait l'objet d'une concertation interne tout au long de l'année 2024 et a été mis en œuvre début 2025.

En pratique, cela s'est concrétisé par des unités plus petites et une homogénéisation des directions, notamment pour mieux répartir la charge, accélérer les validations et, pour les encadrants, assurer un meilleur équilibre entre tâches opérationnelles et management. La gestion de la connaissance en interne a aussi émergé comme un chantier prioritaire pour 2025.

Sur le fond, cette réorganisation permettra de consolider nos missions. Ainsi, par exemple, la création d'une direction de l'exercice des droits et des plaintes doit permettre de répondre à la croissance du nombre de saisines reçues (+ 26 % plaintes – + 236 % EDI). De même, un service de sensibilisation du public a été mis en place pour apporter sur le terrain des réponses concrètes aux besoins des particuliers, TPE/PME et collectivités locales.

« Le RGPD permet d'agir concrètement sur le quotidien numérique des Français. »

Mathias Moulin
secrétaire général adjoint

Mettre en œuvre le « paquet numérique européen »

Cette réorganisation doit aussi permettre de faire face à la diffusion accélérée de l'intelligence artificielle (IA), en particulier générative, et aux nouveaux textes visant à réguler la donnée, en particulier, le règlement sur la gouvernance des données (DGA), le règlement sur les données (DA) et le règlement sur les services numériques (DSA).

La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN) confie déjà de nouvelles compétences à la CNIL. Ainsi, pour le règlement sur les services numériques, la CNIL a la charge de faire appliquer les dispositions sur le ciblage publicitaire, les systèmes de recommandation automatique et la protection des données des mineurs. Il en est de même du règlement sur la gouvernance des données qui crée un nouveau cadre juridique relatif à « l'altruisme des données » dont la mise en œuvre relève de la CNIL.

D'autres textes viendront prochainement attribuer des compétences à des autorités nationales, notamment en matière d'IA. Quels que soient les choix qui seront opérés, le règlement IA impactera fortement la CNIL, au regard du poids des algorithmes dans les traitements de données personnelles.

D'ores et déjà, ces nouvelles législations entraînent une mobilisation de la CNIL pour se coordonner avec les autres autorités compétentes au niveau national (Arcom, ARCEP, etc.) et assurer une bonne compréhension des droits et obligations qui en résultent.

« Cette réorganisation doit aussi permettre de faire face à la diffusion accélérée de l'intelligence artificielle (IA), en particulier générative, et aux nouveaux textes visant à réguler la donnée. »

Louis Dutheillet de Lamothe
secrétaire général

Adapter les outils pour améliorer les services

Deux chantiers majeurs de 2024 se distinguent par leur impact et le temps mobilisé pour améliorer les services de la CNIL.

Le premier porte sur l'accessibilité et la mise en conformité avec la loi sur le handicap et le référentiel général d'amélioration de l'accessibilité (RGAA). Toutes les directions de la CNIL ont participé à l'élaboration d'un schéma pluriannuel d'accessibilité numérique 2025-2027 et d'un plan d'action annuel publiés début 2025. Parallèlement, la CNIL a engagé des travaux pour proposer des contenus en facile à lire et à comprendre (FALC), afin de favoriser l'accessibilité de l'information pour les personnes en situation de handicap cognitif et, plus largement, pour toute personne ayant des difficultés de compréhension.

Le second chantier concerne l'usage de l'IA à la CNIL, là où elle pourrait apporter des gains de productivité, tout en garantissant la fiabilité des décisions et la sécurité des informations traitées. Dans ce cadre, le projet LIAN, avec la contribution de l'Institut national de recherche en sciences et technologies du numérique (Inria), permet une première analyse automatique des règles d'entreprise contraignantes (ou *Binding Corporate Rules* – BCR – en anglais) soumises à la CNIL pour identifier la cohérence entre les critères du référentiel d'analyse et le projet de BCR communiqué. Un autre projet consiste à analyser les sanctions prononcées en Europe en application du RGPD en utilisant des modèles de langage pour extraire automatiquement les articles qui sont visés dans celles-ci.

Contribuer à une application plus efficace du RGPD

Le RGPD permet d'agir concrètement sur le quotidien numérique des Français. Outre les axes de travail prioritaires dégagés dans le nouveau plan stratégique, nous souhaitons améliorer ses modalités d'application dans deux directions.

D'une part, il est nécessaire de renforcer l'harmonisation des procédures administratives nationales qui ont pu freiner la coopération. La Commission européenne a élaboré un projet de règlement en ce sens qui devrait être adopté au premier semestre 2025 et sur lequel la CNIL a contribué au sein du Comité européen de la protection des données (CEPD). Sur la base de ce projet, la CNIL travaille déjà à l'adaptation de ses procédures, principalement concernant l'instruction des plaintes où le rôle du plaignant et les étapes de coopération devraient être renforcées.

D'autre part, certains professionnels, en particulier les TPE/PME, indiquent rencontrer des difficultés dans la mise en œuvre du RGPD par sa complexité. À cet égard, le CEPD et la CNIL doivent renforcer leurs efforts pour les accompagner et faciliter leur mise en conformité, en particulier par la publication de documents simples et courts. Dans cette optique, la CNIL développe de manière continue un service de réponse rapide à des questions de base via sa rubrique « Besoin d'aide », et répond chaque année à des milliers de demandes d'information et à environ 1 500 demandes de conseil de professionnels.

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, le Premier ministre ou les présidents des deux assemblées.

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.

« Chaque semaine, le Collège de la CNIL siège en formation plénière, notamment pour adopter les avis sur les projets de textes qui nous sont soumis par le gouvernement. »

Marie-Laure DENIS
présidente de la CNIL

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. Dans certains cas, le président de la formation restreinte ou un membre de la CNIL qu'il désigne peut prononcer seul une sanction : c'est ce que l'on désigne sous le terme de procédure de sanction simplifiée.

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, si nécessaire, 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.

Qui compose le collège ?

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 membres de la CNIL

Les membres (commissaires)

Philippe-Pierre CABOURDIN
Conseiller maître à la Cour des comptes, président de la formation restreinte de la CNIL
Secteurs : Banque, Assurance, Fiscalité

Claude CASTELLUCCIA
Directeur de recherche à l'Inria Grenoble
Secteur : Intelligence artificielle

Bertrand DU MARAIS
Conseiller d'État
Secteurs : Régulation du numérique et économie de la donnée, International

Jérôme DURAIN
Sénateur de la Saône-et-Loire
Secteur : Intérieur

Laurence FRANCESCHINI
Conseillère d'État
Secteur : Éducation et enseignement supérieur, Vie politique et citoyenne (dont culture, sport), Commerce et publicité

Didier KLING
Commissaire aux comptes, membre du Conseil économique, social et environnemental
Secteur : Environnement

Bruno LASSERRE
Président de la Commission d'accès aux documents administratifs (Cada)

Philippe LATOMBE
Député de la Vendée
Secteur : Social

Isabelle LATOURNARIE-WILLEMS
Conseillère maître à la Cour des comptes
Secteur : Défense

Le bureau

Marie-Laure DENIS
Conseiller d'État, Présidente de la CNIL depuis février 2019

Sophie LAMBREMON
Conseiller honoraire à la Cour de cassation, vice-présidente déléguée de la CNIL
Secteur : Intérieur

Anne DEBET
Professeur des universités, vice-présidente de la CNIL
Secteurs : Affaires européennes, Outils de la conformité

Vincent LESCLOUS
Avocat général honoraire à la Cour de cassation, vice-président de la formation restreinte
Secteurs : Justice, Santé

Catherine MORIN-DESAILLY
Sénatrice de la Seine-Maritime
Secteur : Éducation et enseignement supérieur, Collectivités territoriales

Aminata NIAKATÉ
Avocate, membre du Conseil économique, social et environnemental
Secteurs : Travail et ressources humaines, Recherche et statistiques

Julie OZENNE
Députée de l'Essonne
Secteur : Collectivités territoriales

Fabien TARISSAN
Chercheur au CNRS
Secteur : Cybersécurité et technologies innovantes

Marie ZINS
Professeure des universités
Secteur : Santé

Les membres élus de la formation restreinte

Philippe-Pierre CABOURDIN (président)
Vincent LESCLOUS (vice-président)
Laurence FRANCESCHINI
Isabelle LATOURNARIE-WILLEMS
Bertrand DU MARAIS
Didier KLING

Commissaire du gouvernement

Damien MILIC
Adjointe : **Céline BOYER**

Organigramme des directions et services

au 1er janvier 2025

Marie-Laure DENIS
Présidente

Louis DUTHEILLET DE LAMOTHE
Secrétaire général

Mathias MOULIN
Secrétaire général adjoint

Cabinet du secrétariat général

Secrétariat de la présidente et des secrétaires généraux

Service des affaires européennes et internationales

Service de la communication

Mission qualité, performance, risques

Direction de l'accompagnement juridique

- Service des affaires régaliennes et des libertés publiques
- Service de la santé
- Service de l'économie numérique et du secteur financier
- Service des affaires sociales, des collectivités territoriales, du sport et de l'environnement
- Service des délégués et de l'accompagnement
- Service des outils de la conformité

Direction de l'exercice des droits et des plaintes

- Service de l'exercice des droits et des plaintes
- Service des plaintes • Affaires publiques, sociales et financières
- Service des plaintes • Affaires numériques et commerciales

Direction des contrôles et des sanctions

- Service des contrôles • RH, santé et affaires publiques
- Service des contrôles • Affaires économiques
- Service des sanctions et du contentieux 1
- Service des sanctions et du contentieux 2

Direction des technologies, de l'innovation et de l'intelligence artificielle

- Service de l'expertise technologique
- Service du laboratoire d'innovation numérique de la CNIL
- Service de l'intelligence artificielle
- Mission d'analyse économique

Direction des relations avec les publics

- Service de sensibilisation du public
- Service d'information du public
- Service de l'information et de la documentation

Direction administrative et financière

- Service des ressources humaines
- Service des finances, de la commande publique et des moyens généraux

Direction des systèmes d'information

- Service des projets, applications et développements
- Service des infrastructures, de la sécurité et du support

Un accompagnement en phase avec les évolutions sectorielles et technologiques

OUTILS D'ACCOMPAGNEMENT DE LA CNIL 22

APPLICATIONS MOBILES 24

SURVEILLANCE 26

JEUX OLYMPIQUES ET PARALYMPIQUES 26

ÉLECTIONS EUROPÉENNES ET LÉGISLATIVES 27

BRÈVES ET CHIFFRES CLÉS 28

Entretien avec

Thomas Dautieu

directeur de l'accompagnement juridique de la CNIL

« La CNIL a redoublé d'efforts pour assurer la sécurité juridique des acteurs qu'elle régule »

Quels ont été les grands enjeux de l'accompagnement de la CNIL en 2024 ?

L'année écoulée a confirmé le besoin des entreprises et administrations d'être accompagnées et conseillées. Les nouveaux textes européens et l'irruption de l'IA générative ont incité la CNIL à redoubler d'efforts pour assurer la sécurité juridique des acteurs qu'elle régule. Ces actions se sont traduites par la diffusion de contenus sur notre site web, par exemple les fiches sur l'IA très attendues, et la priorité donnée au « bac à sable » (voir ci-contre).

Quelles ont été les évolutions concernant la certification ou les codes de conduite ?

Nous constatons un intérêt croissant pour ces outils qui ont des périmètres différents : la certification concerne un produit ou un service ; les codes s'adressent aux traitements mis en œuvre par un secteur d'activité.

En 2024, nous avons travaillé sur trois projets de code et deux projets de certification dont le référentiel de certification « sous-traitant » mis en consultation fin 2024 qui suscite un grand intérêt. Les porteurs de ces initiatives bénéficient d'un accompagnement important de notre part. Je veux saluer l'engagement des porteurs des codes européens CISPE (*cloud*) ou EUCROF (sous-traitants en recherche médicale) : leurs outils ont un effet de levier certain pour aider les entreprises européennes des secteurs concernés à améliorer leur niveau de conformité.

Je souhaite aussi mentionner le succès de la certification des prestataires de formation : en 2024, six d'entre eux ont obtenu leurs certificats attestant de la qualité des formations qu'ils dispensent. Nous observons le même mouvement d'intérêt chez nos homologues européens avec une dizaine de dossiers en cours d'examen, dont un projet de certification IA.

Lancement d'un appel à projets « bac à sable » pour la *silver* économie

Le « bac à sable » données personnelles de la CNIL est un dispositif d'accompagnement à destination des innovateurs d'un secteur sur des problématiques émergentes. Ce dispositif s'inscrit dans l'une des grandes missions de la CNIL : le soutien à l'innovation.

Sur la base d'un appel à projets thématique, la CNIL sélectionne des organismes qui pourront bénéficier d'un accompagnement sur-mesure pour sécuriser les enjeux RGPD. Ce dispositif permet de **faire progresser tout un écosystème** : les bilans des travaux menés avec les porteurs de projets sont publiés pour que tous puissent en bénéficier.

Après l'IA et les services publics en 2023, le thème choisi en 2024 est celui de l'économie des seniors, la *silver* économie. Cela englobe l'ensemble des activités économiques et industrielles qui bénéficient aux plus de 60 ans. Ce secteur en pleine croissance traite un très grand nombre de données personnelles, y compris des données sensibles, sur la santé par exemple.

L'appel à projets lancé en novembre 2024 s'adressait prioritairement aux produits et services innovants à destination des seniors dont l'objectif est d'améliorer leur bien-être, d'assurer la sécurité des personnes ou de renforcer la prise en charge et la prévention dans le domaine de la santé.

« Bac à sable » données personnelles : la CNIL lance un appel à projets pour la *silver* économie (économie des seniors)

Pourquoi la CNIL apporte un accompagnement renforcé à quatre entreprises

La CNIL a poursuivi en 2024 une initiative lancée en 2023 consistant à proposer sur plusieurs mois un accompagnement à des entreprises innovantes en dehors de toute thématique, contrairement au dispositif de « bac à sable ». Quatre entreprises ont ainsi été sélectionnées en septembre 2024 par la CNIL pour bénéficier d'un accompagnement renforcé durant six mois : Docaposte (lire ci-contre), la Française des Jeux, Doctrine (une plateforme d'intelligence artificielle pour les professionnels du droit) et ShareID, qui propose des solutions de vérification d'identité, d'authentification et de vérification d'âge.

Ces lauréats ont répondu à un appel à candidatures à destination des **entreprises innovantes**, engagées dans une évolution rapide de leurs activités et dont **le modèle d'affaires repose sur le traitement de données**. La CNIL a reçu des dossiers couvrant des champs d'activités très variés (identité numérique, vidéo « augmentée », numérique en santé, sécurité numérique, *legal tech*…), témoignant d'un fort intérêt pour améliorer la protection des données.

Cet accompagnement renforcé prend trois formes :

- un appui juridique et technique dans des délais rapides : réponses à des questions juridiques ou techniques, formation et assistance à la réalisation d'analyse d'impact relative à la protection des données (AIPD), recommandations en matière de cybersécurité, etc. ;
- une revue de conformité des traitements mis en œuvre. Ce passage en revue des grands enjeux de conformité se traduit par des recommandations adaptées ;
- des actions de sensibilisation aux enjeux de la protection des données à destination des salariés et/ou des dirigeants.

Les enseignements tirés de cet accompagnement viendront alimenter et enrichir les publications de la CNIL afin que d'autres acteurs puissent en bénéficier.

Accompagnement renforcé : la CNIL guidera quatre entreprises pendant six mois

« Un enjeu clé pour une IA de confiance »

Docaposte fait partie des entreprises sélectionnées en 2024 par la CNIL pour un accompagnement renforcé. Son PDG Olivier Vallet en livre les enjeux.

« Lorsque nous avons décidé de lancer notre solution d'IA générative, DalvIA Santé, nous avons sollicité un accompagnement de la CNIL. En effet, l'usage de l'IA appliqué aux données de santé soulevait un certain nombre de questions quant aux mesures les plus adaptées à mettre en œuvre. Ce dialogue avec le régulateur a permis d'établir des repères clairs sur les responsabilités, de sécuriser les étapes clés de l'expérimentation et d'anticiper la mise en production.

L'application du *privacy by design* [vie privée dès la conception, ndlr] permet ainsi aux patients et professionnels de santé de bénéficier de technologies innovantes pour réaliser une synthèse de dossiers médicaux, tout en garantissant les meilleures pratiques en matière de RGPD. Ce cadre est un enjeu clé pour le déploiement d'une IA de confiance. »

« Une collaboration précieuse et stratégique »

Contentsquare a été accompagné par la CNIL en 2023 (qualification RGPD*, recueil du consentement aux cookies, durées de conservation). Retour d'expérience avec son PDG Jonathan Cherki.

« L'accompagnement de la CNIL nous a permis de renforcer notre engagement sur la protection des données personnelles et notre conformité au RGPD. Pendant neuf mois, nos échanges approfondis – sur les aspects technologiques, juridiques et économiques – ont permis d'aligner nos équipes et de progresser. Plus qu'un régulateur, la CNIL s'est révélée être un véritable partenaire de la croissance de Contentsquare. Une collaboration précieuse et stratégique ! »

*La qualification (responsable de traitement seul ou conjoint, ou encore sous-traitant) permet d'identifier, pour chaque traitement, les obligations de chaque acteur.

Applications mobiles : des recommandations pour mieux protéger la vie privée

À l'issue d'une large consultation publique, la CNIL a publié le 24 septembre 2024 la version finale de ses recommandations pour aider les professionnels à concevoir des applications mobiles respectueuses de la vie privée. Elle mènera dès 2025 une campagne de contrôles.

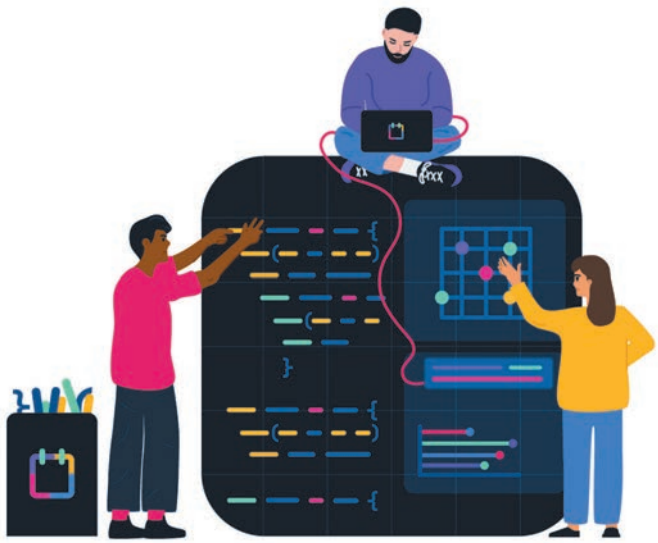
Des usages qui explosent

En 2023, les Français ont téléchargé en moyenne 30 applications (source : data.ai). Ils les utilisent pour communiquer, se divertir, se déplacer, faire des achats, se rencontrer, suivre leur santé… et un constat s'impose : l'environnement mobile présente aujourd'hui plus de risques que le web pour la confidentialité et la sécurité des données. Les applications mobiles ont en effet accès à des informations personnelles plus variées que les sites web, et qui peuvent être plus sensibles, comme la localisation en temps réel, les photographies ou encore des données de santé. De plus, ces applications demandent souvent des permissions pour accéder à des fonctionnalités et à des données du téléphone : microphone, caméra, carnet de contacts, etc. Enfin, beaucoup d'acteurs sont impliqués dans le fonctionnement d'une application, et sont donc susceptibles de collecter, et de partager entre eux, des données personnelles.

Une large concertation

Il revenait à la CNIL de formuler des recommandations pour faire respecter la vie privée des utilisateurs. Sur le modèle de ses travaux sur les cookies, la CNIL a conduit une large concertation avec différents acteurs représentatifs de l'écosystème des applications mobiles.

La concertation a démarré en janvier 2023 avec le lancement d'un appel à contributions, qui a donné lieu à une première synthèse publiée sur le site web de la CNIL. Un projet de recommandations a ensuite été soumis à consultation publique en juillet 2023 afin de recueillir les avis de l'ensemble des parties prenantes, qu'elles soient issues du secteur associatif, du grand public ou des milieux professionnels. La CNIL a par ailleurs saisi l'Autorité de la concurrence (voir encadré).



Tout l'écosystème est concerné

Les recommandations de la CNIL s'adressent à l'ensemble des acteurs du secteur :

- les éditeurs d'applications mobiles, qui mettent des applications à disposition des utilisateurs ;
- les développeurs d'applications mobiles, qui écrivent le code informatique ;
- les fournisseurs de kits de développement logiciel (*SDK* ou *software development kit*), qui développent des fonctionnalités « prêtes à l'emploi » pouvant être directement intégrées par les développeurs (mesure d'audience, ciblage publicitaire, etc.) ;
- les fournisseurs de systèmes d'exploitation, qui mettent à disposition des systèmes d'exploitation (par exemple iOS ou Android) sur lesquels les applications mobiles seront exécutées ;
- enfin, les fournisseurs de magasins d'applications qui mettent à disposition des plateformes permettant le téléchargement de nouvelles applications.

Coopération avec l'Autorité de la concurrence

La CNIL a, pour la première fois, formellement saisi l'Autorité de la concurrence (ADLC) au sujet des recommandations pour les applications mobiles. Cette saisine est une première concrétisation de la volonté des deux instances d'approfondir leur coopération (lire aussi page 57). Dans son avis rendu le 4 décembre 2023 et publié en septembre 2024, l'ADLC souligne notamment qu'il est essentiel que les mesures de protection de la vie privée soient « définies et mises en œuvre en évitant d'engendrer des effets anticoncurrentiels qui ne seraient pas contrebalancés par un gain suffisant pour les consommateurs ».

Obligations réglementaires et bonnes pratiques

Trois grands axes se dégagent pour concevoir des applications respectueuses de la vie privée.

1• Clarifier et encadrer le rôle de chaque acteur

Dans ses recommandations, la CNIL précise le **partage des responsabilités** entre les acteurs de l'écosystème mobile et clarifie leurs **obligations respectives** afin d'apporter de la sécurité juridique. Elle fournit des conseils pratiques pour encadrer leurs relations.

2• Améliorer l'information des personnes sur l'utilisation de leurs données

Un des enjeux est d'**améliorer l'information des personnes** sur l'utilisation de leurs données. La CNIL apporte conseils et bonnes pratiques permettant notamment de garantir que les utilisateurs comprennent si les permissions demandées sont réellement nécessaires au fonctionnement de l'application.

3• S'assurer que le consentement est éclairé

La CNIL rappelle que les applications doivent obtenir un consentement éclairé de l'utilisateur pour traiter des données qui ne sont pas nécessaires à leur fonctionnement, à des fins de ciblage publicitaire par exemple. L'utilisateur doit pouvoir refuser de consentir, ou retirer son consentement s'il change d'avis, aussi simplement qu'il lui est proposé de le donner.
Après avoir accompagné les acteurs professionnels, notamment grâce à des webinaires, la CNIL déploiera, à partir du début du printemps 2025, une campagne spécifique de contrôle des applications mobiles pour s'assurer du respect des règles applicables.

Applications mobiles : la CNIL publie ses recommandations pour mieux protéger la vie privée

Entretien avec

Bertrand du Marais

membre du Collège de la CNIL en charge de la régulation du numérique, de l'économie de la donnée et de l'international

« La CNIL est la première autorité européenne à s'intéresser ainsi aux applications mobiles »

Quels sont les enjeux de cette recommandation sur les applications mobiles ?

–

Compte tenu de l'usage quasi-permanent que nous faisons presque tous de notre ordiphone, cette recommandation est extrêmement structurante pour la société de l'information, à l'instar de celle sur les traceurs (cookies). L'enjeu est donc considérable pour la protection de la vie privée, les terminaux mobiles (téléphones et tablettes) constituant le premier vecteur d'accès à l'univers numérique. L'objectif de nos recommandations est d'assurer que les utilisateurs ont le choix de pouvoir refuser d'être suivis, voire traqués. Cette recommandation est alors très structurante pour tout l'écosystème et pour toute l'industrie.
En outre, cette première saisine formelle de l'Autorité de la concurrence montre la réalité pratique de l'inter-régulation. Enfin, il faut noter que la CNIL est la première des autorités européennes à s'intéresser de façon aussi complète aux applications mobiles : nous lançons le mouvement.

Pourquoi avoir mené une large consultation avec les acteurs représentatifs de l'écosystème des applications mobiles ?

–

Un sujet aussi sensible et complexe exige de recueillir les avis et suggestions de tous les acteurs, industrie comme société civile. Mon prédécesseur, François Pellegrini, a lancé cette consultation approfondie. Pour rédiger la version définitive, nous avons ensuite veillé à tester chaque recommandation à l'aune des commentaires reçus. Le texte s'est ainsi grandement amélioré, dans sa forme comme au fond. Par exemple, nous avons fait évoluer nos recommandations sur le « score de vie privée » : pour mieux protéger les usagers et les opérateurs, il devrait reposer sur une méthodologie préalablement définie, de manière transparente, par un acteur tiers au fournisseur de magasin d'applications.

Entretien avec

Shoshana Zuboff,

sociologue et professeure émérite
à la Harvard Business School,
intervenante lors de l'événement air2024.

En collaboration avec la Commission nationale de contrôle des techniques de renseignement (CNCTR), la CNIL a organisé le 19 novembre 2024 son événement éthique sur le thème « La surveillance dans tous ses états. Quelle éthique pour protéger nos libertés ? ».

« Le capitalisme de surveillance transforme nos vies en marchandises »

Vous développez le concept de « capitalisme de surveillance ». Quelles en sont les idées clés ?

–

Le capitalisme de surveillance décrit la façon dont les grandes entreprises technologiques comme Google ou Facebook collectent et analysent des données personnelles à grande échelle pour prédire et influencer le comportement humain. Il est né au début du XXIe siècle, lors de l'éclatement de la bulle Internet et de la crise financière qui a suivi, quand ces entreprises ont dû trouver comment monétiser les données. Cela peut être les habitudes de vie, mais aussi le ton de la voix, la direction du regard, le choix des mots, les temps de pause… Ces données sont volées, capturées sans la connaissance des utilisateurs et immédiatement redéfinies comme des actifs d'entreprise, agrégées, analysées et utilisées pour réaliser des prédictions comportementales et générer des ventes. Ce modèle économique transforme les informations personnelles en une marchandise précieuse. Le capitalisme de surveillance est devenu un ordre institutionnel mondial qui n'est plus confiné aux géants de la technologie ou au secteur de la publicité. Les implications sont vastes : perte de vie privée, manipulation des comportements, corruption de l'information…

Lors de l'événement air, vous avez déclaré : « Internet est devenu une prison de la surveillance, sans barreaux, ni sortie ». Partant de ce constat, comment protéger nos libertés ?

–

Pour contrer cette dynamique, il est crucial de réguler ces technologies, mais la régulation seule ne suffit pas. Elle doit être accompagnée d'une prise de conscience collective et d'une volonté politique de protéger les libertés individuelles. Le capitalisme de surveillance n'est qu'une logique économique parmi d'autres pour donner vie aux technologies numériques et structurer l'ordre social. Il est tout à fait possible pour l'ordre démocratique d'abolir le capitalisme de surveillance et de libérer le numérique pour réinventer notre civilisation de l'information pour un avenir démocratique.

Revoir l'événement – air2024 : La surveillance dans tous ses états

Les Jeux olympiques et paralympiques sous le regard de la CNIL

–

Des observations sur le laissez-passer

Les Jeux olympiques et paralympiques ont soulevé des enjeux forts en matière de protection des données personnelles et de vie privée. Dès fin 2022, la CNIL a rendu un premier avis sur le projet de loi prévoyant la mise en œuvre de caméras « augmentées » à titre expérimental lors des Jeux. Elle s'est ensuite prononcée le 25 avril 2024 sur le texte qui instituait un laissez-passer dans les « zones de sécurité » où la circulation était restreinte en raison de l'organisation des Jeux et a inscrit, dans ses thématiques prioritaires, le contrôle des données collectées lors de l'événement (voir page 32). Le laissez-passer contenant un code QR était délivré à la suite d'une **inscription sur une plateforme numérique, ce qui entrainait la collecte de données personnelles**. Dans son avis, la CNIL a confirmé la légitimité du traitement de données pour sécuriser les événements exceptionnels, mais a émis des observations sur l'utilisation de la photographie et sur les durées de conservation des données. Ces réserves ont été intégrées dans l'arrêté publié. Les **copies de cartes nationales d'identité, permis de conduire, passeports et titres de séjour ne pouvaient ainsi être conservées que le temps nécessaire à la délivrance du titre d'accès**.

Questions-réponses sur le site de la CNIL

Afin d'apporter au grand public une grande transparence sur l'utilisation des données personnelles lors des JOP 2024, la CNIL a publié sur son site une liste de questions-réponses sur les impacts sur la vie privée et les libertés des personnes concernées. Exemple de questions traitées : « Si je suis spectateur, ferai-je l'objet d'une enquête administrative ? », « Scanners corporels : dois-je donner mon accord ? », « Puis-je m'opposer au système de laissez-passer ou à mon enregistrement par les caméras « augmentées » ? »…

Tous les contenus sur les Jeux olympiques et paralympiques 2024

Un guide pour le déploiement des caméras de vidéoprotection

À l'occasion du salon des maires 2024, la CNIL et l'Association des maires de France (AMF) ont publié, dans le cadre de leur partenariat, un guide commun pour aiguiller les collectivités territoriales dans la mise en place de dispositifs vidéo conformes à la réglementation relative à la protection des données.

En complément, la CNIL a publié ou mis à jour certaines fiches pratiques sur son site web sur le déploiement de dispositifs vidéo dans l'espace public, notamment sur les caméras « augmentées », la vidéo-verbalisation ou encore l'interdiction de la captation sonore.

Le guide « Mettre en place des dispositifs vidéo conformes »

« La CNIL doit répondre aux sollicitations d'acteurs hétérogènes utilisant la vidéo »

Mathilde est juriste au service des affaires régaliennes et des libertés publiques

« De nombreux dispositifs vidéo se déploient dans un cadre juridique qui demeure complexe. Le secteur est en perpétuelle mouvance, en particulier depuis les Jeux olympiques de 2024 et son cadre expérimental. La CNIL doit s'assurer que le déploiement de ces dispositifs se fasse dans le respect de la réglementation applicable et joue pleinement son rôle de régulateur dans le cadre du déploiement de ces nouvelles technologies. Il s'agit également pour la CNIL de répondre aux sollicitations d'acteurs hétérogènes ayant recours à la vidéo et redoublant d'innovation. Elle veille à construire une doctrine solide pour chacun des dispositifs émergents, en compréhension des besoins et des contraintes du secteur. »

Élections européennes et législatives : envois massifs de SMS et courriels, développement de l'IA

Depuis 2012, pour chaque élection locale ou nationale, la CNIL met en place un « observatoire des élections » dont les principales missions sont d'organiser une veille sur les pratiques de communication politique, de dialoguer avec les partis et candidats, et d'informer les électeurs sur leurs droits et de recueillir leurs signalements.

À l'issue de la séquence électorale 2024, l'observatoire des élections de la CNIL a dressé le bilan des méthodes de prospection auxquelles les partis politiques ont eu recours lors des campagnes des européennes et des législatives. Les messages par courriel et SMS restent les principaux canaux de diffusion de la prospection politique des partis.

La CNIL a concentré sa mission sur plusieurs enjeux : la prospection téléphonique, la réutilisation des fichiers à des fins de propagande électorale, l'information des personnes concernées et la sécurité des données collectées par les prestataires.

Il ressort des plaintes et signalements reçus par la CNIL que, le plus souvent, les personnes indiquent ne jamais avoir communiqué leurs coordonnées aux partis qui les sollicitent, ni disposer d'information sur l'utilisation de leurs données personnelles. Pour autant, les personnes concernées se sont très peu manifestées pour exercer leurs droits auprès des partis.

Enfin, la séquence électorale 2024 a été l'occasion pour le service de l'intelligence artificielle de la CNIL de se pencher sur l'utilisation de l'IA et son impact sur les processus électoraux. Les résultats de cette étude approfondie sont publiés dans un article sur le site du Laboratoire d'innovation numérique de la CNIL (LINC).

Il en ressort que **l'intelligence artificielle joue un rôle central dans le fonctionnement des réseaux sociaux, moteurs de recherches en ligne et autres plateformes**, alors même que ces sites constituent des espaces d'information pour les citoyens, de communication pour les partis politiques ou d'influence pour d'autres acteurs intéressés par les résultats d'élections.

167 signalements ont été recueillis par la CNIL à l'issue d'une campagne des élections européennes particulièrement atone. La quasi-totalité (146 signalements) a porté sur des opérations de prospection par SMS. La CNIL a également été destinataire de 12 plaintes, a prononcé 4 rappels à la loi et a instruit 1 contrôle sur pièces dont les suites sont en cours d'instruction.

462 signalements ont été recueillis dans le cadre des élections législatives. Ce bilan marque une hausse significative du nombre de sollicitations avec 176 signalements de plus qu'en 2022 (+ 61,5 %). La CNIL a également été destinataire de 42 plaintes et a instruit 4 contrôles dont les suites sont en cours d'instruction.

Brèves et chiffres clés

LES JOURNÉES RGPD SE POURSUIVENT

La CNIL continue ses déplacements pour échanger sur la mise en œuvre du RGPD. En 2024, ces rencontres se sont tenues à **Lille**, en collaboration avec la faculté de droit de l'Université catholique et l'Association française des juristes d'entreprise, à **Nancy** avec l'Association française des correspondants à la protection des données à caractère personnel (AFCDP) et la Métropole du Grand Nancy, et à **Montpellier**, avec la région Occitanie, Montpellier Méditerranée Métropole, l'Université de Montpellier et l'AFCDP.

DIFFUSION D'UN OUTIL D'AUTO-ÉVALUATION POUR LES RÈGLES D'ENTREPRISE CONTRAIGNANTES

Les règles d'entreprise contraignantes (*binding corporate rules*, *BCR*, en anglais) sont des outils de conformité prévus par le RGPD visant à mettre en œuvre une politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne. La CNIL a publié en avril 2024 un outil d'auto-évaluation permettant de vérifier le niveau de maturité d'un projet par rapport aux exigences du Comité européen de la protection des données.

BCR : la CNIL publie un outil d'auto-évaluation

AFFAIRES PUBLIQUES ET LOBBYING : UN GUIDE RGPD PUBLIÉ AVEC LES PROFESSIONNELS DU SECTEUR

Plusieurs associations représentatives des professionnels des affaires et des relations publiques (l'Association française des conseils en lobbying et affaires publiques, l'Association des professionnels des affaires publiques, l'Association des avocats-conseils en affaires publiques et le Syndicat du conseil en relations publics) ont sollicité l'accompagnement de la CNIL. Après plus de deux années d'échanges, un guide a été publié en mars 2024.

Affaires publiques et lobbying : les professionnels du secteur publient un guide RGPD en concertation avec la CNIL

CONSULTATION PUBLIQUE SUR LES RÉFÉRENTIELS SANTÉ

La CNIL a lancé en mai 2024 une concertation publique sur la refonte des référentiels santé afin de mieux accompagner les professionnels du secteur. La synthèse des contributions a été présentée en novembre 2024. La démarche se poursuit en 2025, avec, à la clé, la publication de référentiels ajustés.

Consultation publique sur les référentiels santé : la CNIL publie la synthèse des contributions

RECHERCHE CLINIQUE : LA CNIL APPROUVE LE CODE DE CONDUITE EUROPÉEN DE LA FÉDÉRATION EUCROF

Prévu par le RGPD, un tel code permet notamment de construire un socle commun de bonnes pratiques et de contribuer à démontrer sa conformité au règlement européen. Il a été porté par la **fédération EUCROF** (*European Clinical Research Organisations Federation*), à l'attention des prestataires de services en recherche clinique (*Clinical Research Organisations*, CRO, en anglais). La CNIL l'a approuvé en octobre 2024.

DE NOUVEAUX WEBINAIRES POUR LES PROFESSIONNELS

La CNIL a organisé 12 webinaires en 2024 pour aider les entreprises à mieux protéger leurs données et à s'assurer de leur conformité avec la réglementation. Parmi les rendez-vous de 2024 : « Applications mobiles : que retenir des nouvelles recommandations de la CNIL ? », « Transferts de données hors de l'UE, quelles sont les règles de base ? », « Appariement de données avec le SNDS, les circuits de traitement du NIR », etc.

Les webinaires de la CNIL

DE PLUS EN PLUS DE DÉLÉGUÉS À LA PROTECTION DES DONNÉES

103 602 organismes privés et publics ont, au total, désigné un délégué à la protection des données (DPO).

36 777 DPO étaient en poste en 2024, plusieurs organismes pouvant désigner le même délégué.

SANTÉ : DE NOMBREUX PROJETS TRAITÉS PAR LA CNIL

574 dossiers ont été traités en santé (demandes d'autorisation) dont **424** en recherche en santé.

Une intensification de l'action répressive

PLAINTES ET DEMANDES D'EXERCICE INDIRECT DES DROITS (EDI) 30

CONTRÔLES 32

SANCTIONS ET AUTRES MESURES RÉPRESSIVES 34

Entretien avec

Philippe-Pierre Cabourdin

président de la formation restreinte de la CNIL, membre du Collège et conseiller maître à la Cour des comptes.

« La procédure simplifiée connait une forte montée en puissance »

Quels sont les principaux manquements constatés en 2024 ?

–

Cette année, la formation restreinte, dans le cadre de la procédure ordinaire (voir page 16), a sanctionné des manquements récurrents en matière de prospection commerciale, rappelant aux organismes l'obligation de garantir la conformité de la collecte des données à caractère personnel à des fins de prospection. Des décisions majeures ont également concerné la protection des données de santé, la CNIL ayant souligné le risque de réidentification des données pseudonymisées. Le défaut de mise à jour des bases de données administratives, notamment dans le traitement des antécédents judiciaires, a conduit à plusieurs rappels à l'ordre. Enfin, la sécurité des données personnelles a fait l'objet de sanctions pour des insuffisances techniques, telles que l'usage de mots de passe non sécurisés ou de protocoles obsolètes.

Quel bilan tirez-vous de la mise en œuvre de la procédure simplifiée ?

–

La procédure simplifiée a connu une forte montée en puissance en 2024, avec 69 sanctions prononcées, contre 24 en 2023. Elle a permis de traiter rapidement des manquements fréquents, en particulier le défaut de coopération avec la CNIL, qui concerne 27 organismes, et le non-respect de l'exercice des droits (23 décisions). Les sanctions ont aussi visé le non-respect du principe de minimisation des données et les insuffisances en matière de sécurité. Ce dispositif permet d'apporter une réponse rapide et efficace aux manquements les plus courants, renforçant ainsi l'efficacité de l'action de la CNIL.

Nouveau record de plaintes

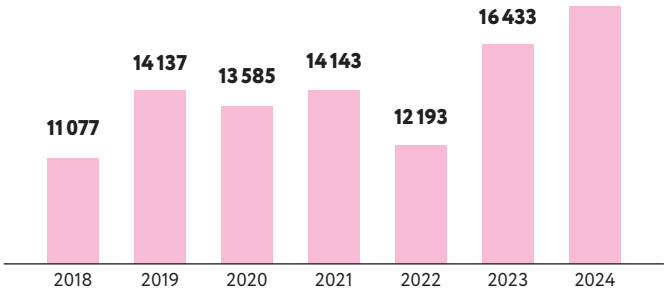
–

2024 a constitué une nouvelle année record de plaintes reçues par la CNIL en données brutes, en hausse de plus de **8 % par rapport à 2023**. Afin d'apporter une réponse appropriée et dans les meilleurs délais à chaque demande, la CNIL continue d'adapter ses modalités d'action. Elle mène d'abord un premier examen de la plainte pour déterminer si elle est bien compétente pour agir et si les éléments fournis sont suffisamment précis.

Pour les plaintes recevables, la CNIL peut considérer, selon la nature et la gravité des faits, que la solution à apporter est de **rappeler la réglementation applicable à l'organisme en cause**. Plusieurs milliers de courriers ont été adressés dans ce cadre. La CNIL peut aussi décider de mener des investigations plus approfondies et, si nécessaire, obliger formellement l'organisme à mettre un terme au manquement, voire le sanctionner. Les plaintes reçues ont ainsi conduit à l'ouverture de procédures de contrôle, à l'adoption de mises en demeure et à des rappels aux obligations légales ou à des sanctions. En 2024, plus de la moitié des dossiers ayant abouti à une sanction avaient pour origine une plainte.

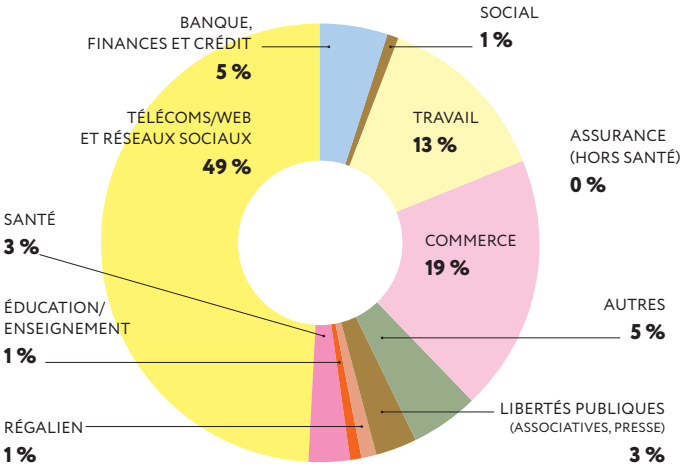
Pour la troisième année consécutive, **la CNIL est parvenue à traiter autant de plaintes qu'elle en a reçues**. La seule exception est la série de 2 423 plaintes relatives à la violation de données de FREE (lire page 50), car arrivée en fin d'année et ayant justifié une procédure de contrôle impliquant des investigations approfondies toujours en cours.

PLAINTES REÇUES **17 772**



L'objet des plaintes

Pour la plupart, l'objet des plaintes reste très lié aux difficultés quotidiennes des personnes, dans leur vie numérique, sur leur lieu de travail ou dans leurs achats.



15 350 plaintes reçues (données nettes excluant les affaires dites de « série » correspondant à un grand nombre de plaintes dirigées contre un même responsable de traitement et relatives à des faits analogues)

15 639 plaintes traitées dont :
5 771 plaintes rejetées car irrecevables (par rapport à la problématique soulevée ou défaut de preuve de la potentielle violation, etc.)
9 868 plaintes closes après instruction, intervention auprès de l'organisme mis en cause, résolution du problème et/ou adoption de mesures correctrices ou sanctions.

« Il faut des éléments probants, comme des captures d'écran, pour instruire les dossiers »

Hélène est chargée de greffe des plaintes à la direction de l'exercice des droits et des plaintes.

« Je suis une des deux chargées du greffe des plaintes à la CNIL. En 2024, nous avons examiné près de 18 000 plaintes pour vérifier que chaque dossier est complet, en l'état d'être instruit et si la CNIL peut agir. À défaut, nous adressons des demandes de complément ou des courriers de rejet. Par exemple, si une plainte porte sur une demande de suppression d'informations en ligne, nous vérifions si une demande d'exercice de droits a d'abord été adressée à l'auteur de la publication ou la plateforme. Si c'est le cas, nous vérifions que nous avons bien tous les justificatifs de cette démarche. Ensuite, il faut des éléments probants pour instruire le dossier. Si l'usager semble en difficulté pour nous les fournir, il peut être nécessaire d'appeler pour expliquer précisément ce dont nous avons besoin et comment faire les copies et captures nécessaires. Une fois que nous disposons de ces éléments, nous transmettons le dossier pour instruction, en précisant le caractère urgent ou sensible aux agents qui interviendront auprès de l'organisme mis en cause. »

Fuite de données, pourquoi saisir la CNIL ?

Quand la CNIL reçoit une plainte liée à une violation de données (voir page 50), elle vérifie toujours si cette violation lui a bien été notifiée par l'organisme, conformément à ses obligations prévues par le RGPD. Ensuite, selon la nature et la gravité de la violation, la CNIL peut décider d'instruire les plaintes reçues en interrogeant l'organisme ou en menant des opérations de contrôle. Dans de telles situations, le rôle de la CNIL est d'apprécier si les mesures prises par l'organisme ayant subi la violation de données pour assurer la sécurité des données étaient ou non appropriées. Le non-respect des obligations du RGPD peut aboutir à des sanctions.

La plainte auprès de la CNIL est distincte de la plainte pénale qui peut être déposée auprès d'un commissariat de police ou auprès de la gendarmerie par les personnes qui seraient victimes d'une exploitation frauduleuse de leurs données, d'une usurpation d'identité ou encore d'un « hameçonnage » à la suite de la fuite de données. La CNIL n'est pas compétente pour traiter ces infractions, ni pour octroyer d'éventuels dommages et intérêts.

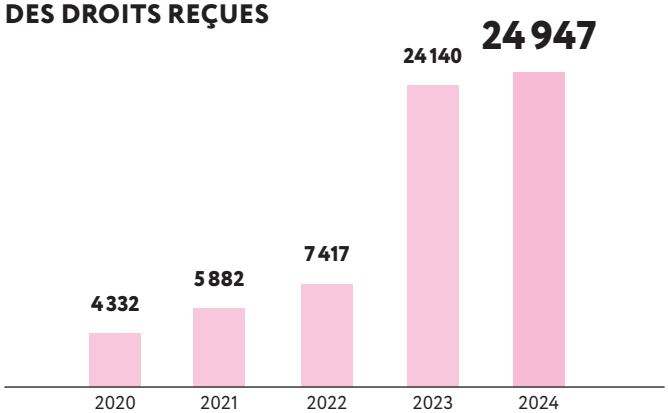
Des évolutions majeures concernant l'exercice des droits indirect (EDI)

L'exercice des droits indirect (EDI) consiste à demander à la CNIL qu'elle vérifie le contenu d'un fichier dont la loi n'autorise pas la consultation directe. Cela peut concerner des fichiers de police ou de renseignement en particulier (voir ci-dessous). Au total, en 2024, **la CNIL a traité 14 654 demandes d'EDI sur les 24 947 reçues** (dont 17 % de demandes non recevables). Ces dernières années, la grande majorité des demandes concernait le fichier national des comptes bancaires et assimilés (FICOBA). Ce fichier, qui recense tous les comptes détenus par une personne, a été mis en place par l'administration fiscale pour faciliter la conduite des contrôles fiscaux.

L'accès des particuliers à ces données devait obligatoirement se faire par l'intermédiaire de la CNIL. Depuis 2020, les demandes sont en très forte augmentation. Les usagers indiquent notamment redouter une usurpation d'identité qui se traduirait par l'ouverture frauduleuse d'un compte à leur nom. Pour répondre à ces sollicitations, la CNIL avait mis en place un téléservice. 2024 est toutefois la dernière année de fonctionnement de ce service.

En effet, depuis le 6 janvier 2025, **les modalités d'accès au FICOBA ont été revues** pour les particuliers agissant en leur nom ou au nom d'un enfant mineur dont ils sont le représentant légal : **ils doivent désormais s'adresser directement** à leur service des impôts **sans passer par la CNIL.**

DEMANDES D'EXERCICE INDIRECT DES DROITS REÇUES



Les demandes FICOBA représentent
91 % du total des demandes d'EDI

La CNIL est également saisie pour d'autres fichiers :
- **TAJ** (traitement des antécédents judiciaires)
- **SIS** (système d'information Schengen)
- **FPR** (fichier des personnes recherchées)
- **EASP** (enquêtes administratives liées à la sécurité publique)
- **PASP** (prévention des atteintes à la sécurité publique)
- **CRISTINA** (fichier de la direction générale de la sécurité intérieure)
- **TREX** (fichier de la direction générale de la sécurité extérieure)

Le contrôle de la CNIL

4 thématiques prioritaires pour les contrôles en 2024

En plus des contrôles faisant suite à des plaintes, à des signalements ou en lien avec l'actualité, la CNIL intervient dans le cadre de thématiques prioritaires qu'elle définit annuellement, sur des sujets à forts enjeux pour le public. Ces thématiques représentent en moyenne 30 % des contrôles effectués.

1• La collecte de données dans le cadre des Jeux olympiques et paralympiques

22 contrôles ont été effectués avant, pendant et après les JOP, entre avril et octobre 2024. Ils ont concerné :

- la sécurité des sites, à la fois les zones de restrictions (QR codes, 4 contrôles) et les caméras de vidéoprotection « augmentée » – 6 contrôles ;
- le traitement des **données des spectateurs et des participants aux différents événements** (10 contrôles en tout), dans le cadre de la billetterie officielle par exemple ;
- les **traitements RH** en lien avec la gestion des volontaires (300 000 candidatures reçues, pour 45 000 volontaires sélectionnés) – 2 contrôles.

La CNIL s'est notamment assurée de la proportionnalité des données collectées, de leur sécurité et de leur sort une fois les Jeux terminés. Elle a constaté que l'ensemble des acteurs contrôlés était globalement en conformité. Les contrôles concernant l'utilisation des caméras « augmentées », qui faisait l'objet d'une expérimentation, ont notamment permis de vérifier que les dispositifs mis en œuvre étaient conformes aux cas d'usage prévus par la loi.

2• Les données des mineurs collectées en ligne

Les contrôles de la CNIL se sont concentrés sur la vérification des **mécanismes de contrôle de l'âge**, des **mesures de sécurité**, ainsi que du respect du principe de **minimisation des données** (les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire en fonction de la finalité poursuivie). Ils se sont déroulés dans 10 sociétés ayant souvent plusieurs millions d'utilisateurs actifs en France, principalement des éditeurs d'applications mobiles dans les domaines des réseaux sociaux, des messageries et des jeux vidéo.

Les principaux manquements apparus concernent :

- une conservation trop longue des données au regard des finalités ;
- une information lacunaire, difficilement accessible ou insuffisamment claire, surtout pour un jeune public ;
- la collecte d'informations ou le suivi des utilisateurs via des traceurs sans leur consentement.

L'instruction de certains de ces contrôles se poursuit. D'autres ont déjà donné lieu à l'adoption de mises en demeure.

3• Les programmes de fidélité et les tickets de caisse dématérialisés

La CNIL a souhaité vérifier les modalités de traitement de la dématérialisation des tickets de caisse et du programme de fidélité mis en place par les commerçants. En particulier, elle voulait s'assurer qu'il n'y avait pas de détournement de finalité à la suite de la collecte des données personnelles des clients. Des contrôles ont été réalisés auprès de 11 organismes (mode, commerce, grande distribution, station-service…).

À ce stade, les principaux manquements constatés portent sur :

- l'information dispensée aux consommateurs ;
- une collecte excessive de données (manquement au principe de minimisation) ;
- une faible mise en œuvre des mesures de sécurité autour des données d'achat et des comptes fidélité ;
- des détournements de finalité du traitement (ciblage publicitaire sans consentement préalable) ;
- un défaut de base légale pour certains traitements réalisés dans le cadre de la dématérialisation des tickets de caisse ou du programme de fidélité.

À noter également qu'un contrôle a permis d'identifier une bonne pratique de la part d'un acteur, qui prévoit la conservation en local, sur le terminal de l'utilisateur, de ses tickets de caisse.

Ces dossiers de contrôle sont toujours en cours d'instruction.

4• Le droit d'accès des personnes

Pour la troisième année consécutive, la CNIL et plusieurs de ses homologues européens ont participé à une action coordonnée (*coordinated enforcement framework*) du Comité européen de la protection des données (CEPD). Le thème retenu pour 2024 portait sur le respect du droit d'accès des personnes. Les vérifications ont montré que les organismes contrôlés ont majoritairement mis en œuvre des mesures organisationnelles pour traiter les demandes de droit d'accès (par exemple en désignant un délégué à la protection des données). Toutefois, ces mesures sont parfois insuffisantes et insatisfaisantes. Lorsque des personnes exercent leur droit d'accès à l'intégralité de leurs données, certains organismes ne fournissent qu'une réponse partielle ou incomplète. Les résultats nationaux vont être regroupés et analysés, afin d'assurer un suivi ciblé aux niveaux national et européen.

3 procédures emblématiques de l'année 2024

Les contrôles menés dans le cadre de violations de données d'ampleur

À la suite de l'augmentation du nombre de violations de données de très grande ampleur, la CNIL a lancé des contrôles auprès de grands acteurs, privés comme publics, victimes de ces agissements. Ils ont permis de constater que **des mesures élémentaires, recommandées par la CNIL et l'ANSSI, auraient pu permettre de prévenir les violations subies (voir page 50).** Les suites répressives à apporter à ces contrôles sont en cours d'examen.

L'usage des logiciels d'analyse vidéo par les pouvoirs publics

La CNIL a réalisé des contrôles auprès du ministère de l'Intérieur et de plusieurs communes afin de vérifier les conditions dans lesquelles des logiciels d'analyse automatique des images, tels que le logiciel BriefCam, sont utilisés.
Elle a mis en demeure le ministère de l'Intérieur le 15 novembre 2024 car :

- des engagements de conformité au référentiel unique relatif aux logiciels de rapprochement judiciaire (statut juridique encadrant l'usage des logiciels d'analyse de type Briefcam) et des analyses d'impact relatives à la protection des données (AIPD) n'avaient pas été transmis à la CNIL ;
- la CNIL a constaté un usage isolé de reconnaissance faciale.

En outre, la CNIL a mis en demeure six communes afin de mettre fin à des manquements constatés dans l'utilisation de caméras augmentées. Elles avaient installé des logiciels permettant l'analyse en temps réel du comportement des personnes filmées sur la voie publique (cet usage par les communes n'est pas autorisé en l'état du droit).

Les bannières cookies trompeuses

La CNIL a réalisé plus de 40 contrôles en ligne, concernant des sites web et des applications mobiles, après des plaintes concernant des bandeaux de recueil du consentement trompeurs, incitant les internautes à accepter les cookies. **Pour rappel, sauf exceptions, les cookies ne peuvent être déposés qu'après le consentement des internautes. De plus, refuser les cookies doit être aussi simple que de les accepter.**

À l'issue de ces contrôles, la CNIL a mis en demeure plusieurs éditeurs de sites web de modifier leur bannière.

Au total

321
contrôles
166 sur place
99 en ligne
44 sur pièces
12 sur audition

Les contrôles en coopération avec d'autres autorités

290 millions d'euros d'amende à l'encontre d'UBER

À la suite d'une plainte collective de la Ligue des droits de l'Homme, représentant plus de 170 chauffeurs de la plateforme UBER, la CNIL a coopéré avec l'autorité de protection des données des Pays-Bas, où se trouve l'établissement principal d'UBER. En application des procédures instaurées par le RGPD, c'était en effet l'autorité compétente pour mener des investigations et prononcer des sanctions. La collaboration a été étroite tout au long de la procédure. Résultat : une amende de 290 millions d'euros prononcée en juillet 2024, portant sur le transfert vers les États-Unis de données des chauffeurs inscrits sur la plateforme UBER. Cette décision s'ajoute à une précédente procédure contre UBER ayant abouti en décembre 2023 à une amende de dix millions d'euros pour plusieurs manquements à l'information des chauffeurs.

Le nombre de sanctions a plus que doublé

L'année 2024 est marquée par une forte augmentation de l'ensemble des mesures correctrices prononcées par la CNIL : le nombre de sanctions a doublé par rapport à 2023. Les mises en demeure et les rappels aux obligations légales sont, de leur côté, en constante hausse.

331
mesures correctrices au total

87 **sanctions**
dont 18 selon la procédure ordinaire et **69** selon la procédure simplifiée

55 212 400 €
d'amendes cumulées

180
mises en demeure

64 **rappels aux obligations légales par la présidente**

12 **sanctions européennes** examinées par la CNIL

7 **sanctions de la CNIL** examinées par ses homologues européens

Les sanctions prononcées par la CNIL ont des natures variées : amendes, injonctions sous astreinte (avec ou sans amende) ou encore rappels à l'ordre.

Bilan de la procédure ordinaire

En 2024, **18 sanctions ont été prononcées selon la procédure ordinaire** par la formation restreinte, l'organe de la CNIL en charge de prononcer les sanctions. Ces sanctions comportent **13 amendes** (dont 2 assorties d'une injonction sous astreinte) et 2 décisions 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 dans sa décision de sanction) pour un montant total de 54 496 900 €, ainsi que 3 rappels à l'ordre.

Des manquements récurrents dans la prospection commerciale

La formation restreinte a rappelé à plusieurs occasions que les organismes qui utilisent à des fins de prospection commerciale électronique des données personnelles transmises par des partenaires primo-collectants (qui organisent des jeux-concours par exemple) ou des courtiers en données doivent s'assurer que **les conditions dans lesquelles les données ont été collectées sont conformes au RGPD** (si nécessaire, avec le consentement de la personne et après la fourniture d'une information claire et concise).

En outre, un fournisseur de messagerie électronique qui insère des publicités entre les courriels reçus par ses utilisateurs dans leur boite de réception doit préalablement recueillir leur consentement (voir un exemple de sanction en page 36).

Des données de santé qui doivent être particulièrement protégées

La CNIL a également rendu plusieurs décisions marquantes en matière de données de santé. La formation restreinte s'est en particulier prononcée sur la qualification des données traitées dans des entrepôts de données de santé. Elle a rappelé que, même lorsqu'elles sont collectées à grande échelle par un organisme qui ignorerait l'identité des personnes concernées, **ces données restent pseudonymes et non anonymes dès lors qu'elles sont reliées entre elles par un identifiant et présentent ainsi un risque de réidentification**. Ces données restent donc des données personnelles auxquelles la législation s'applique et **dont le traitement doit être autorisé par la CNIL**.

Des fichiers de l'État non mis à jour

La formation restreinte a prononcé 3 rappels à l'ordre à l'encontre de ministères notamment pour ne pas s'être assurés, dans le cadre de plusieurs traitements distincts, de l'exactitude des données figurant dans leurs bases de données. En particulier, s'agissant du traitement des antécédents judiciaires, la formation restreinte a relevé que de nombreuses fiches établies par les services de police n'étaient pas mises à jour pour prendre en compte les décisions de relaxe ou d'acquittement.

L'essor de la procédure simplifiée

En 2024, **l'essor de la procédure de sanction simplifiée s'est confirmé :** le président de la formation restreinte seul (ou un membre de la formation restreinte) a prononcé **69 sanctions**, soit près de trois fois plus qu'en 2023. Elles prennent la forme de 62 amendes (dont 12 assorties d'une injonction sous astreinte) et de 6 décisions de liquidation d'astreinte, pour un montant total de **715 500 euros**, ainsi que d'un rappel à l'ordre.

Parmi les manquements les plus fréquemment sanctionnés figurent :

- **Le défaut de coopération avec la CNIL**, qui a concerné 27 organismes (sociétés, professionnels libéraux) sanctionnés pour n'avoir pas répondu à ses sollicitations ;
- **Le non-respect de l'exercice de leurs droits par les personnes concernées**, avec 23 décisions concernant un manquement relatif au non-respect d'une demande d'effacement, d'opposition ou d'accès ;
- **Le manquement à la minimisation des données**, qu'il s'agisse de commentaires excessifs, d'enregistrement systématique et en intégralité de conversations téléphoniques ou de la surveillance vidéo permanente de salariés à leur poste de travail, avec 10 sanctions ;
- **Le manquement relatif à la sécurité des données** personnelles, retenu à l'encontre de 11 organismes qui n'avaient pas mis en œuvre toutes les mesures nécessaires pour assurer la sécurité des données. Ils ont été sanctionnés pour l'utilisation de mots de passe insuffisamment robustes, le stockage de mots de passe en clair, l'absence de politique d'habilitation, ou encore l'utilisation d'une version obsolète du protocole TLS qui permet d'assurer la confidentialité et l'intégrité des informations qui circulent entre le serveur et le navigateur de l'utilisateur.

Augmentation du nombre de mises en demeure

En 2024, la CNIL a prononcé 180 mises en demeure (décision de la présidente de la CNIL ordonnant à un organisme de se mettre en conformité dans un délai fixé).

Parmi les thématiques majeures abordées dans ces mises en demeure figurent :

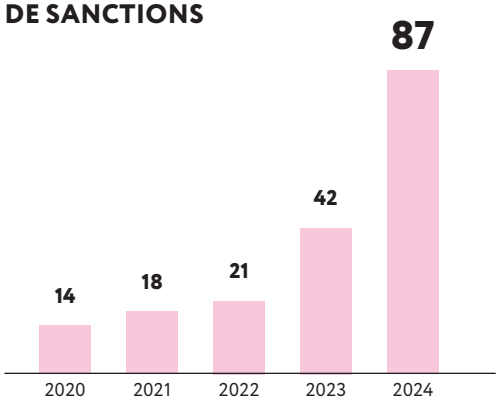
L'accès au dossier patient informatisé (DPI)

Ce dossier centralise l'ensemble des données de santé des patients pris en charge au sein d'un établissement de santé. Il permet aux professionnels de santé d'accéder facilement à leurs informations médicales. La CNIL a mis en demeure plusieurs établissements de santé de prendre les mesures permettant d'assurer la sécurité du dossier patient informatisé, rappelant que les données des patients ne doivent être accessibles qu'aux personnes justifiant du besoin d'en connaître (voir page 54).

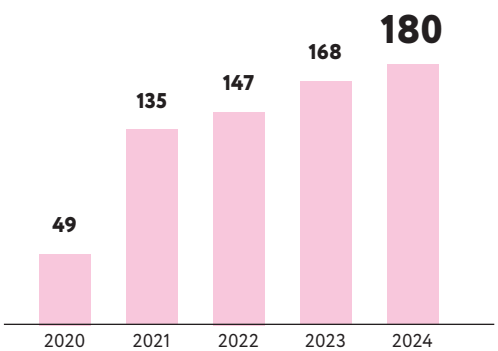
L'absence de réponse à un exercice des droits

La CNIL reçoit de nombreuses plaintes concernant l'absence de réponse d'un organisme à une demande d'exercice d'un droit (droit d'accès aux données, droit d'opposition ou encore droit à l'effacement des données). La CNIL a mis plusieurs dizaines d'organismes en demeure d'apporter une réponse à ces demandes et, en cas d'inaction, a engagé une procédure de sanction simplifiée à l'encontre de plusieurs d'entre eux. D'autres thématiques ont également été traitées dans le cadre de la procédure de sanction simplifiée : **vidéosurveillance des salariés** à leur poste de travail ou encore **insuffisance des mesures de sécurité** pour protéger les données.

ÉVOLUTION DU NOMBRE DE SANCTIONS



ÉVOLUTION DES MISES EN DEMEURE



L'activité contentieuse

Deux sanctions marquantes en 2024

Amende de

50

millions d'euros
contre la société Orange

Le 14 novembre 2024, la CNIL a sanctionné la société Orange d'une amende de 50 millions d'euros, notamment pour avoir affiché des publicités entre les courriels des utilisateurs de son service de messagerie électronique, sans leur consentement. Les contrôles réalisés par la CNIL ont permis de constater que les utilisateurs des comptes de messagerie électronique Orange voyaient s'afficher au sein de leur boîte de réception, entre les courriels reçus et sans qu'ils n'y aient consenti, des messages publicitaires prenant la forme de courriers électroniques.

La CNIL, s'appuyant sur un arrêt de la Cour de justice de l'Union européenne du 25 novembre 2021, a considéré que ces messages faisant la promotion de services ou de biens, mais affichés dans **un espace normalement réservé aux courriels privés** en prenant l'apparence de véritables courriels, constituaient de la prospection directe par courrier électronique. En conséquence, il était nécessaire **de recueillir le consentement des personnes concernées** en application de l'article L. 34-5 du code des postes et des communications électroniques.

40 000 **euros**

d'amende à l'encontre
d'une entreprise du secteur immobilier

Le 19 décembre 2024, la CNIL a sanctionné une société d'une amende de 40 000 euros en raison d'une surveillance disproportionnée de l'activité de ses salariés, à travers un logiciel. En outre, les salariés étaient filmés en permanence.

La société avait paramétré un logiciel de manière à détecter automatiquement, tout au long de la journée, si le salarié n'effectuait aucune frappe sur le clavier ou mouvement de souris sur une durée paramétrée de 3 à 15 minutes. Ces temps « d'inactivité » comptabilisés, à défaut d'être justifiés par les salariés ou rattrapés, pouvaient faire l'objet d'une retenue sur salaire par la société. Le logiciel effectuait également des captures d'écran régulières des ordinateurs des salariés. La CNIL a considéré que dans la mesure où les périodes pendant lesquelles le salarié n'utilise pas son ordinateur peuvent tout de même correspondre à du temps de travail effectif (par exemple, réunions ou appels téléphoniques), le dispositif était disproportionné. De même, la CNIL a relevé que les captures d'écrans pouvaient conduire à la captation d'éléments d'ordre privé, portant ainsi atteinte aux droits fondamentaux des salariés.

Des décisions de la CNIL majoritairement confirmées par le Conseil d'État

Lorsque la CNIL prononce une mesure correctrice, l'organisme concerné à la possibilité de la contester devant le Conseil d'État. En 2024, 93 nouveaux recours ont été communiqués à la CNIL. Sur les 30 décisions rendues par le juge administratif en 2024, toutes, à l'exception d'un non-lieu (l'objet du litige ayant disparu), ont confirmé la légalité des décisions de la CNIL.

Une décision marquante sur la responsabilité d'une filiale

Le 19 novembre 2024, le Conseil d'État a rejeté la requête de la société SAF LOGISTICS qui demandait l'annulation de la délibération de la formation restreinte de la CNIL prononçant une amende de 200 000 euros à son encontre.

La société SAF LOGISTICS est une société de fret aérien dont la société mère est localisée en Chine. Dans le cadre d'un recrutement interne pour un poste au sein de la société mère, SAF LOGISTICS collectait des données relatives à la vie privée de ses employés (affiliation politique, appartenance ethnique, groupe sanguin, situation maritale…). Dans cette affaire, le Conseil d'État a confirmé la qualité de responsable de traitement de la société dont le siège social est en France, même si le traitement a été initialement mis en place par la société mère. Le Conseil d'État a aussi confirmé l'existence de manquements au RGPD, comme la collecte d'informations sensibles sans recueil du consentement des salariés. Enfin, il a confirmé le manquement à l'obligation de coopérer avec la CNIL, SAF LOGISTICS s'étant notamment abstenue de lui communiquer la traduction complète du formulaire litigieux.

L'indispensable encadrement de l'IA et des algorithmes

RÉGLEMENT IA 38

PREMIÈRES RECOMMANDATIONS DE LA CNIL 39

CONCILIER IA GÉNÉRATIVE ET RGPD 40

COMMENT UNE INTELLIGENCE PIÈGE LES UTILISATEURS TROP CONFIANTS 41

LES RISQUES DE L'IA DANS LE CADRE DES HYPERTRUCAGES 42

JOURNÉE DE RECHERCHE SUR LA VIE PRIVÉE 42

Entretien avec

Claude Castelluccia

directeur de recherche à l'Inria Grenoble et membre du Collège de la CNIL en charge du secteur de l'intelligence artificielle

« La CNIL s'est organisée pour apporter une approche globale sur l'IA face à des enjeux complexes »

Qu'a changé la création d'un service dédié à l'intelligence artificielle ?

Transversale, l'IA touche de nombreux secteurs tels que la santé, le régalien ou les ressources humaines. La mise en place d'un service dédié au sein de la CNIL, regroupant des expertises tant juridiques que techniques, offre aujourd'hui une approche globale face à des enjeux complexes. Ce service joue un rôle-clé dans l'élaboration d'outils adaptés à ce domaine comme des recommandations, des outils d'audit ou un accompagnement des acteurs du secteur. Ce dernier est essentiel : bien que l'IA ouvre des perspectives extraordinaires, il est crucial d'encadrer son développement afin de maîtriser ses risques potentiels.

En outre, ce service mène des réflexions stratégiques pour anticiper les évolutions technologiques et réglementaires, offrant une capacité accrue d'adaptation aux transformations rapides induites par l'IA.

Quel bilan faites-vous de 2024 concernant la réglementation de l'IA ?

Si l'adoption du règlement européen sur l'IA est un tournant majeur auquel la CNIL se prépare activement, le RGPD restera un pilier dans l'évolution de l'IA compte tenu du nombre de systèmes reposant sur l'utilisation de données personnelles.

Parallèlement, en Europe, la coopération entre régulateurs s'est intensifiée pour harmoniser les approches en matière d'IA. Afin de prévenir une complexification des réglementations, il est également important de contribuer à l'émergence d'une gouvernance mondiale de l'IA. Dans ce contexte, la CNIL a développé ses collaborations à l'international, notamment avec ses homologues sud-coréen et californien.

Entrée en vigueur du règlement européen sur l'IA

Le règlement européen sur l'IA (RIA) entre en application en 2025 et vise à **encadrer le développement, la mise sur le marché et l'utilisation de systèmes d'IA qui peuvent poser des risques pour la santé, la sécurité ou les droits fondamentaux.**

Le RIA établit notamment 4 niveaux de risque, du risque minimal ne nécessitant pas d'obligation spécifique, au risque inacceptable, comme la notation sociale ou l'exploitation de la vulnérabilité des personnes, totalement interdit depuis février 2025. Ce règlement ne remplace pas les exigences du RGPD : il les complète en posant les conditions requises pour développer et déployer des systèmes d'IA de confiance.

L'application du RIA sera contrôlée à deux niveaux :

- au niveau européen par le Comité européen de l'IA, rassemblant des représentants de chaque État membre, ainsi que par le Bureau de l'IA, une institution nouvellement créée rattachée à la Commission européenne ;
- au niveau national par une autorité de surveillance du marché. Chaque État membre doit en désigner une avant le 2 août 2025.

Le Comité européen de la protection des données (CEPD), qui a pour mission de veiller à l'application du RGPD dans l'UE et dont la CNIL est membre, souhaite que les autorités de protection des données européennes endossent ce rôle d'autorité de surveillance du marché. Une telle désignation permettrait d'assurer une bonne coordination entre les différentes autorités nationales, ainsi qu'une articulation harmonieuse du RIA avec le RGPD. La CNIL a en tout cas déjà lancé un plan d'action pour accompagner les entreprises développant un système d'IA dans la bonne application du RGPD (lire ci-contre).

Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL

Premières recommandations sur le développement des systèmes d'intelligence artificielle

La CNIL a publié 12 fiches pratiques pour encadrer le développement de systèmes d'IA, soumises à consultations publiques.

Une demande remontée du terrain

De nombreux acteurs ont fait part à la CNIL de questionnements concernant l'application du RGPD pour les systèmes d'intelligence artificielle, en particulier depuis l'émergence de l'IA générative (lire également page 40). La CNIL a ainsi lancé depuis 2023 un important travail de clarification du cadre juridique. Il est en effet possible de concilier développement de l'IA et protection de la vie privée, dans le respect des valeurs européennes. C'est même une condition indispensable pour que les citoyens fassent confiance à ces technologies.

À l'issue de ses travaux, la CNIL a publié en 2024 12 fiches pratiques permettant un usage de l'IA respectueux des données personnelles.

Concertation avec les acteurs de l'IA

Ces recommandations ont été élaborées après une série de rencontres avec des acteurs publics et privés afin de recueillir leurs interrogations sur le sujet. Pour être au plus près des réalités des **usages de l'IA**, la CNIL a organisé deux consultations publiques de plusieurs mois. Les différentes parties prenantes (entreprises, chercheurs, universitaires, associations, conseils juridiques et techniques, syndicats, fédérations, etc.) ont ainsi pu s'exprimer et **contribuer à l'élaboration de bonnes pratiques.** Ainsi, sur les 12 fiches soumises à consultations publiques, 9 ont été publiées dans leur versions définitives et les suivantes seront adoptées courant 2025.

Répondre aux enjeux juridiques et techniques

Les 12 fiches publiées en 2024 apportent des réponses concrètes, illustrées d'exemples, aux enjeux juridiques et techniques liés à l'application du RGPD à l'IA. Elles posent les bases d'une méthodologie pour développer un système d'IA respectueux de la vie privée :

- déterminer le régime juridique applicable ;
- définir une finalité ;
- déterminer la qualification juridique des acteurs ;
- définir une base légale ;
- effectuer des tests et vérifications en cas de réutilisation des données ;
- réaliser une analyse d'impact si nécessaire ;
- tenir compte de la protection des données dès les choix de conception du système ;
- tenir compte de la protection des données dans la collecte et la gestion des données ;
- mobiliser la base légale de l'intérêt légitime pour développer un système d'IA ;
- informer les personnes concernées ;
- respecter et faciliter l'exercice des droits des personnes concernées ;
- annoter les données ;
- garantir la sécurité du développement d'un système d'IA.

Les fiches pratiques IA

Des réponses pour concilier IA générative et RGPD

Sollicitée par de nombreux acteurs, la CNIL a publié une première série de questions-réponses sur les bonnes pratiques à adopter pour un déploiement des systèmes d'IA générative respectueux du RGPD.

Qu'est-ce que l'IA générative ?

L'intelligence artificielle dite « générative » désigne les systèmes capables de créer des contenus : texte, code informatique, image, musique, audio, vidéo, etc. Leur utilisation vise généralement à accroitre la créativité et la productivité en permettant de générer quasi instantanément de nouveaux contenus, mais aussi en analysant ou en retravaillant des contenus préexistants (par exemple, en proposant des résumés, corrections ou traductions automatiques). Leurs performances sont aujourd'hui proches de certaines productions réalisées par des personnes en raison de la grande quantité de données ayant servi pour leur entrainement.

Des précautions s'imposent

Comment déployer de façon responsable et respectueuse de la protection des données un système d'IA générative ? Cette question intéresse au plus haut point la plupart des acteurs privés et publics. L'adoption de l'IA générative (voir définition ci-contre) est identifiée comme cruciale car elle constitue un facteur d'amélioration de la créativité et de la productivité. Toutefois, ces systèmes peuvent nécessiter d'utiliser des données personnelles. **Il convient donc de prendre un certain nombre de précautions pour respecter les droits des personnes sur leurs données.**

Partir de besoins concrets

En juillet 2024, la CNIL a publié une première série de questions-réponses pour guider les différents acteurs dans une approche responsable et sécurisée. Pour le choix d'un système d'IA générative, la CNIL recommande ainsi de partir de besoins concrets pour choisir le système le plus adapté et de tenir compte des risques encourus, non seulement du fait des usages poursuivis mais aussi des limitations du système envisagé. Ainsi, mettre à disposition des salariés un agent conversationnel pour aider à la rédaction présente moins de risque qu'un système d'aide à la décision à l'égard de clients, candidats à l'embauche ou citoyens.

Des thématiques inspirées par les parties prenantes

Les échanges entre la CNIL et les différentes parties prenantes ont permis de traiter d'autres thématiques :

- « Quel mode de déploiement privilégier (sur site, *API*, *cloud*) ? » ;
- « Comment mettre en œuvre et encadrer l'utilisation d'un système d'IA générative ? » ;
- « Comment former et sensibiliser les utilisateurs finaux de ces systèmes ? » ;
- « Quelle gouvernance de ces systèmes mettre en œuvre ? » ;
- « Comment s'assurer de la conformité de l'utilisation d'un système d'IA générative au règlement européen sur l'IA ? »…

Conformément à son plan d'action sur l'IA, la CNIL prévoit de publier **de nouvelles recommandations au sujet des systèmes d'IA générative.**

Les questions-réponses de la CNIL sur l'utilisation d'un système d'IA générative

Comment une Intelligence piège les utilisateurs trop confiants

Informations sur notre santé, sur nos préférences alimentaires, sur nos amis et notre famille : sans nous en rendre compte, nous confions de nombreuses données personnelles aux assistants vocaux. La CNIL a mené une opération ludique de sensibilisation.

Stratagème à La Roche-sur-Yon

Mercredi 24 janvier 2024, accompagnée de la Fédération des centres sociaux de Vendée et de leur café mobile, la CNIL s'est rendue sur une place publique à La Roche-sur-Yon (85) pour **proposer aux passants d'échanger avec Germain, « un nouvel assistant vocal utilisant de l'intelligence artificielle »**. Ils étaient invités à chercher de l'aide pour trouver un numéro de téléphone, pour arrêter de fumer ou encore pour localiser un circuit de cyclotourisme. Pour avoir la réponse à leur demande, les participants ont fourni au fil de la discussion **de nombreuses données personnelles**.

Jusqu'au moment où ils découvraient la vérité : ils n'interagissaient pas avec **un assistant vocal, mais avec un agent de la CNIL caché à proximité**. C'était le but de l'expérience : faire prendre conscience de toutes les données que l'on dévoile, parfois sans s'en rendre compte. Comme l'a souligné une participante : *« C'est vrai que je n'ai pas fait attention à toutes les informations que j'ai pu donner… C'était tellement pratique d'avoir une réponse immédiate à ma question ! ». « Effectivement quand l'IA s'est présentée et m'a demandé mon prénom, je lui ai répondu naturellement ! C'est une habitude de politesse comme si je parlais à une personne »*, a témoigné un autre utilisateur.

Pourquoi nous nous dévoilons

En échangeant ensuite avec l'un des concepteurs de l'outil et avec un sociologue du Laboratoire d'innovation numérique de la CNIL (LINC), les participants ont relevé certains facteurs qui ont favorisé ce partage de leurs données :

- les IA, comme celles utilisées pour le service à la clientèle ou pour des assistants vocaux, **posent souvent des questions directes, parfois personnelles,** qui semblent anodines ou pertinentes pour résoudre un problème : on y répond sans prendre conscience de la quantité d'informations partagées ;
- les échanges reproduisent les conditions d'une conversation humaine et **favorisent un échange spontané d'informations** au fil de la discussion ;
- **l'interaction avec une IA peut être perçue comme étant sous contrôle,** donnant une impression de sécurité qui facilite parfois le partage d'informations initialement considérées comme privées.

8 conseils pour échanger avec un assistant vocal

1. Ne partagez que le strict **minimum d'informations nécessaire pour obtenir une réponse**. Si l'assistant vous demande des informations personnelles, réfléchissez à leur utilité réelle.
2. **Ne confiez pas des données sensibles ou intimes** telles que vos informations de santé, vos coordonnées bancaires ou vos mots de passe.
3. Soyez conscient de ce que vous avez partagé au fil des conversations et **supprimez régulièrement vos données.**
4. **Formulez des questions claires et simples** pour éviter toute incompréhension par l'assistant.
5. Privilégiez les dispositifs qui vous permettent de **désactiver l'analyse de vos données**.
6. Si vous le souhaitez, **exercez votre droit d'accès** aux données collectées en contactant l'éditeur du service (consultez la politique de confidentialité qui doit comporter une rubrique relative à l'exercice de vos droits).
7. **Les réponses des assistants ne sont pas toujours fiables :** n'hésitez pas à vérifier les informations obtenues grâce à d'autres sources.
8. En cas de doute sur la nature de votre interlocuteur (robot ou humain), **consultez les conditions d'utilisation** ou contactez le concepteur du service.

Voir l'expérience : votre assistant vocal connait-il votre vie privée ?

Une étude sur les risques de l'IA dans le cadre des hypertrucages

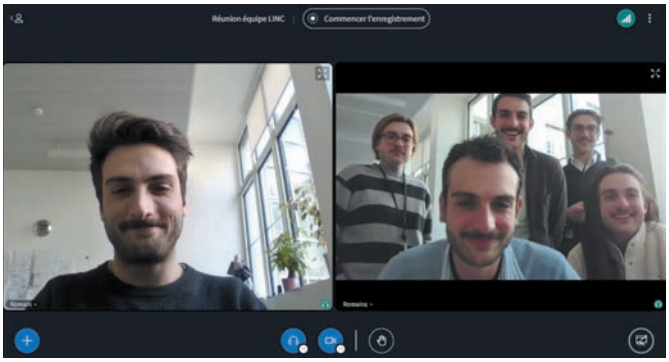
Les hypertrucages, ou « *deep fakes* », ne sont pas un phénomène nouveau. Ils existent depuis quelques années, mais ils étaient souvent mal réalisés et facilement détectables à l'œil nu. Cependant, depuis quelques mois, la quantité et la qualité des vidéos hypertruquées visibles sur Internet ne cessent de faire des bonds en avant. Ces manipulations vidéo prennent la forme d'échange de visages (*face swapping*), d'animation de portraits ou encore de modification de discours. Les risques associés à ce nouvel environnement technologique sont nombreux : usurpation d'identité, escroquerie, désinformation, diffamation, humiliation…

Pour alerter sur ces dangers, le Laboratoire d'innovation numérique de la CNIL (LINC) s'est associé avec le PEReN (le pôle d'expertise de la régulation numérique). Ensemble, ils ont voulu explorer avec quelle facilité ces hypertrucages pouvaient être désormais réalisés. Menée fin 2024 selon un protocole très strict, l'étude réalisée par le PEReN visait notamment à répondre aux questions suivantes :

- quelle qualité d'hypertrucage peut-on attendre d'un non-expert ?
- peut-on tromper un public averti avec ces outils ?

Il en ressort, dans les grandes lignes, que les outils disponibles en ligne sont facilement accessibles et utilisables, très performants et permettent de produire des trucages presque indétectables humainement. Plusieurs prolongements sont envisagés pour enrichir cette étude.

Partenariat avec le PEReN : les risques de l'intelligence artificielle dans le cadre des hypertrucages



« Des trucages difficilement détectables à l'œil nu »

Romain est ingénieur Recherche & Développement au Laboratoire d'innovation numérique de la CNIL (LINC)

« Les hypertrucages sont aujourd'hui extrêmement accessibles, et peuvent porter de graves atteintes aux personnes qui en sont victimes. Que l'on se fasse passer pour quelqu'un d'autre ou que l'on insère la photo d'une personne sur une vidéo, les impacts vont de l'escroquerie à la désinformation, en passant par des *deep fakes* pornographiques.

Ces technologies font l'objet d'une attention particulière par le LINC et un partenariat a été monté avec le PEReN pour étudier leur facilité d'accès et leur niveau de réalisme. Le rapport propose un état de l'art de ces techniques, ainsi qu'une étude montrant qu'il peut être aujourd'hui difficile de détecter ces trucages à l'œil nu. Des outils existent pour nous assister, leur recensement et l'analyse de leur efficacité sont en cours. »

Troisième édition de la « Journée de recherche sur la vie privée »

La CNIL a organisé le 4 juin 2024 à Paris la troisième édition du *Privacy Research Day* ou « Journée de recherche sur la vie privée ». Pensée comme un **espace d'échanges et de rencontres**, cette conférence internationale fait dialoguer **experts juridiques, informaticiens, *designers*, économistes, chercheurs en sciences sociales**… Elle est aussi une opportunité de construire des partenariats durables entre le monde de la recherche, la CNIL et d'autres organismes publics.

Six grands thèmes ont structuré l'événement en 2024 : « **Stratégies pour une régulation efficace de l'IA** », « **Sécurité et vie privée, de la théorie à la pratique** », « **Information et perception des utilisateurs** », « **Publics vulnérables** », « **Publicité et collecte de données des mineurs** » et « **Données personnelles dans l'économie numérique** ».

Journée de recherche sur la vie privée 2024 : retrouvez l'événement en vidéo

L'éducation au numérique et la protection des mineurs

PARTENARIATS DE LA CNIL POUR S'ADRESSER AUX MINEURS ET À LEURS FAMILLES 44

LA CNIL CONTRIBUE AUX TRAVAUX SUR LE NUMÉRIQUE ET LES JEUNES 45

SENSIBILISER ET ACCOMPAGNER TOUS LES PUBLICS 48

Entretien avec

Xavier Delporte

directeur des relations avec les publics de la CNIL

« C'est la réalité du terrain qui décide de nos productions pédagogiques »

Quels ont été les grands enjeux de la protection des mineurs en 2024 ?

–

La protection des mineurs est au cœur de l'actualité. Accès à la pornographie, utilisation des téléphones dans les écoles, temps d'écran, contrôle ou surveillance parentale, majorité numérique, cyberharcèlement, éducation aux médias, « révolution » de l'IA… Les sujets n'ont pas manqué. La CNIL a participé à ces débats, par ses prises de position, sa participation à des auditions ou encore sa production juridique. En effet, les données personnelles sont à chaque fois au cœur des problématiques soulevées et des solutions envisagées.

Qu'apportent les partenariats pour toucher cette cible ?

–

La CNIL a un rôle à jouer pour sensibiliser les jeunes et leurs entourages (parents, enseignants, éducateurs) à un usage raisonné du numérique, pour protéger ses données et sa vie privée. Pour cela, elle a besoin, d'une part, de comprendre les usages et les capacités des publics et, d'autre part, de s'appuyer sur des partenaires lui donnant accès aux publics et en mesure de relayer ses messages au plus près des personnes concernées.

Comment évolue la diffusion des bonnes pratiques de la CNIL pour sensibiliser les mineurs et leur famille ?

–

La CNIL est de plus en plus présente dans les régions, à la rencontre directe des acteurs publics et associatifs mais aussi des élèves, des enseignants et des éducateurs. C'est la réalité du terrain qui décide de nos productions pédagogiques. Nous voulons répondre à des préoccupations réelles par des ressources de qualité, adaptées sur le fond et sur la forme.

Les partenariats de la CNIL pour s'adresser aux mineurs et à leurs familles

–

« Protéger les mineurs et leurs données dans l'univers numérique ». C'est l'un des axes clés du plan stratégique de la CNIL 2025-2028 (lire page 6). Plusieurs partenariats ont déjà été noués au service de cet enjeu.

Avec France Télévisions

Le 17 décembre 2024, France Télévisions et la CNIL ont signé un partenariat visant à mieux informer et sensibiliser le grand public aux enjeux soulevés par le numérique. Cette collaboration s'étendra sur les trois prochaines années et se traduira notamment par des interventions pédagogiques de la CNIL pour les plus jeunes sur les antennes et programmes de France Télévisions. La CNIL interviendra aussi dans le cadre de la plateforme Lumni proposant des contenus multimédias gratuits pour les élèves, parents, enseignants et médiateurs, dans les dispositifs d'éducation aux médias et à l'information (EMI) portés par France Télévisions, ainsi que lors de rencontres avec les journalistes et les salariés du groupe public.

Avec le ministère de l'Éducation nationale

Partenaire de l'Éducation nationale, la CNIL apporte son soutien et participe aux événements et initiatives du ministère au sujet de l'éducation au numérique. Elle intervient ainsi dans les classes sur l'ensemble du territoire national pour promouvoir une culture citoyenne des usages du numérique, pour faire connaître les droits et les devoirs liés à l'usage d'Internet, et pour expliquer comment protéger sa vie privée en ligne. En 2024, la CNIL a notamment participé au dispositif Territoire Numérique Éducatif, un programme expérimental du ministère de l'Éducation nationale. Dans ce cadre, la CNIL a échangé avec des enseignants, des parents et des médiateurs en Isère, Corse et Hérault.

La CNIL contribue aux travaux sur le numérique et les jeunes

La CNIL a participé au rapport « Enfants et écran, à la recherche du temps perdu » commandé par le président de la République et publié en avril 2024. Auditionnée par la commission chargée de formuler des recommandations, la CNIL a partagé ses constats, issus des travaux sur le numérique adolescent et des nombreuses visites dans les classes ou ateliers avec les jeunes. Elle a notamment souligné la nécessité d'une information à large échelle, des mineurs et aussi de leurs parents, sur le sujet de la protection de la vie privée. Elle a rappelé que, pour répondre à cet enjeu sociétal, il convenait d'agir collectivement, en faveur d'une sensibilisation de tous les publics. Forte de son expérience et dans un souci de coordination, la CNIL a proposé de centraliser les actions d'éducation au numérique menées au plan national.

Avec le réseau Info Jeunes France

Ce réseau de médiation est constitué de plus de 1100 structures qui informent et accompagnent les jeunes (collégiens, lycéens, étudiants, salariés, demandeurs d'emploi…) sur tous les sujets liés à leur autonomie afin de les rendre acteurs de leur futur numérique. Au niveau national et local, la CNIL intervient auprès des médiateurs pour les sensibiliser à la protection des données personnelles et mettre à disposition ses ressources pédagogiques pour les différents publics. 300 médiateurs ont ainsi été touchés directement en 2024.

Avec France services

France services est un réseau de plus de 2700 lieux d'accueil sur l'ensemble du territoire qui accompagnent le grand public dans ses démarches administratives du quotidien. La CNIL intervient auprès des conseillers pour les aider à protéger les usagers dans leur vie numérique. Les thématiques abordées : gestion des mots de passe, arnaques en ligne, usurpation d'identité… Des supports ont été co-construits et mis à disposition dans les espaces France services pour sensibiliser les usagers à la protection des données en ligne et diffuser les bonnes pratiques.

Participation à la refonte des programmes en Enseignement moral et civique

Entre février et mars 2024, le Conseil supérieur des programmes, une instance indépendante placée auprès du ministre de l'Éducation nationale, a lancé une consultation sur le nouveau programme d'Enseignement moral et civique (EMC), du CP à la terminale. La CNIL y a participé, proposant de renforcer l'éducation à la citoyenneté numérique. Objectif : permettre aux élèves d'être acteurs de leur vie numérique, notamment en étant en capacité d'exercer leurs droits. En fonction de l'âge, cela signifie pouvoir :

- faire la différence entre l'espace public et l'intimité ;
- mesurer les conséquences de son comportement en ligne vis-à-vis des autres ;
- mieux comprendre comment fonctionne l'écosystème numérique ;
- mesurer les enjeux éthiques.

La « réflexion sur les données personnelles, les traces numériques » est désormais inscrite au programme de la classe de 6e.

173

actions de sensibilisation menées au total en 2024 auprès de l'ensemble des publics sur la France entière, dont près de la moitié (84) auprès de jeunes et d'acteurs entourant la jeunesse (parents, enseignants, éducateurs, animateurs, etc.).

Programme inédit de sensibilisation dans les écoles de Marseille

Du 29 janvier au 2 février 2024, la CNIL et la Ville de Marseille ont déployé un dispositif exceptionnel de sensibilisation dans les écoles primaires. Trois agents de la CNIL sont intervenus dans 8 écoles de la ville, auprès de 52 classes, du CE2 au CM2, rencontrant ainsi 1131 enfants. Au programme : comprendre comment fonctionne Internet, comment protéger sa vie privée, pourquoi il faut faire preuve de prudence, et comprendre aussi les mécanismes du cyberharcèlement. Le matin, avant les cours, un livret destiné aux parents était distribué devant les écoles. Et les parents étaient invités à venir échanger avec la CNIL en fin de journée, en partenariat avec La Ligue de l'Enseignement des Bouches-du-Rhône, dans le cadre du programme Territoires Numériques Educatifs. À l'issue de cette semaine, la Ville de Marseille a mis en place un parcours citoyen « *Le parcours des petits explor@teurs du Web et des médias* » sur sa plateforme ENT lui permettant d'être en lien avec toutes les écoles de son territoire, associant l'Académie d'Aix-Marseille, La Ligue de l'Enseignement des Bouches-du-Rhône, la CNIL et l'Arcom.

Réponses aux questions des parents lors de la semaine sur la parentalité numérique à Paris

Du 23 au 30 mars 2024, la CNIL a participé à la semaine sur la parentalité numérique organisée par la Ville de Paris, l'association WeTechCare et la Caisse d'allocations familiales (CAF) de Paris. Sur le thème « Mon enfant et les écrans : une semaine pour bien vivre le numérique en famille », l'événement a démarré au Théâtre de La Villette dans le 19e arrondissement de Paris où la CNIL était présente pour répondre aux questions des parents et les aider à accompagner leurs enfants dans leurs usages numériques. Des démonstrations de jouets connectés étaient proposées pour sensibiliser le public à la sécurisation des données. La CNIL est aussi intervenue, les 26 et 28 mars, dans deux écoles élémentaires parisiennes pour des temps d'échanges avec les parents en fin de journée.

Ateliers thématiques au Festival Hauts-de-Seine Digital Games

Les 24 et 25 mai 2024, la CNIL a participé au Festival Hauts-de-Seine Digital Games, organisé à Paris Expo Porte de Versailles. Proposé par le Département des Hauts-de-Seine, ce festival unique en France mêle jeux vidéo, pédagogie et formation autour du numérique. Présente dans l'espace « Sensibilisation », la CNIL animait toutes les heures **des ateliers thématiques** de 20 à 30 minutes à destination des jeunes, des enseignants, des éducateurs et des parents.

Les « Trophées des classes »

En novembre 2024, la CNIL a lancé une nouvelle édition des « Trophées des classes », en collaboration avec le ministère de l'Éducation nationale, ainsi qu'avec Radio France, le collectif Educnum et les établissements scolaires membres du dispositif eTwinning, déployé par le réseau Canopé.
Ce concours est ouvert **à toutes les classes, du CM1 à la 3e**. Elles sont invitées à créer de manière collective un support numérique (affiche multimédia, podcast, quiz, vidéo, livre numérique, jeu numérique, etc.) autour de la thématique « Connaître ses droits numériques » ou « Civisme numérique ». Remise des prix en juin 2025.

Affiche franco-coréenne « Tes données, tes droits »

Dans le cadre de son partenariat mis en place en 2022 avec la PIPC, l'autorité de protection des données de la Corée du Sud, la CNIL a réalisé en 2024 une affiche dans un style manhwa (l'équivalent du manga japonais) sur le thème « Tes données, tes droits ». Disponible en français, en coréen, en brésilien et en anglais, elle explique comment protéger sa vie privée en ligne. Une initiative originale pour attirer l'attention d'un public jeune.

Affiche « Tes données, tes droits »

Conseils et flyer pour les fans de jeux vidéo

Autre initiative de la CNIL en 2024 : la diffusion de conseils sur le thème « Jeux vidéo : protège ta vie privée ». Présentés sur le site de la CNIL, ces conseils sont repris dans un flyer sous le message : « La CNIL ne peut pas t'aider à gagner, mais elle peut t'aider à protéger tes données personnelles ». D'après l'Association française du jeu vidéo, la France compte plus de 39 millions de joueurs, dont 5,7 millions d'enfants et d'adolescents (entre 10 et 17 ans).

Les conseils pour protéger sa vie privée dans les jeux vidéo

Sensibiliser et accompagner tous les publics

Au-delà de ses interventions dédiées à la sensibilisation des mineurs et de leur famille (voir pages précédentes), la CNIL est allée à rencontre de tous les publics, notamment les personnes les plus en difficulté avec le numérique. 12 régions de France métropolitaine ont été visitées. Voici quelques initiatives.

Des ateliers intergénérationnels sur la protection des données

Pour sensibiliser enfants et seniors, et créer du dialogue entre générations, la CNIL déploie des ateliers ludiques et interactifs. À l'occasion des journées RGPD à Lille, elle a ainsi proposé, avec la compagnie *La Belle Histoire*, une pièce de théâtre immersif sur le thème « Je protège ma vie numérique », un atelier intergénérationnel avec des seniors usagers des centres sociaux et des élèves de CM2. D'autres ateliers intergénérationnels ont été organisés à Paris et à Montpellier.

Des sessions pour les personnes en situation de handicap

Trois sessions d'une journée ont été organisées en 2024 dans un foyer de vie du Nord pour sensibiliser les résidents, dans un format d'atelier et d'échanges, aux usages responsables et sûrs des outils numériques et des réseaux sociaux. La dernière séquence a permis de co-construire des règles d'usage des outils numériques au sein du foyer.

Deux guides sur les cybermenaces pour les familles et les seniors

En collaboration avec l'Union nationale des associations familiales (Unaf) et Cybermalveillance.gouv.fr, la plateforme de prévention et d'assistance aux victimes d'actes de cybermalveillance, la CNIL a publié deux guides en 2024 pour sensibiliser les utilisateurs de tous âges aux dangers d'Internet et proposer des conseils pratiques pour s'en protéger. L'un s'adresse aux familles, l'autre aux seniors.

Les guides « cybersécurité : ayez les bons réflexes »

Un nombre toujours élevé de visiteurs sur le site de la CNIL

Les sites web de la CNIL (cnil.fr et linc.cnil.fr) ont cumulé environ 11,6 millions de visites en 2024, un chiffre stable par rapport à 2023 (11,8). La CNIL a publié 274 actualités, communiqués et nouvelles fiches, soit nettement plus qu'en 2023 (+ 114 %), dû principalement aux nombreuses fiches pratiques sur l'IA.

L'information sur cnil.fr et les réseaux sociaux

Top 3 des pages et fiches pour les professionnels

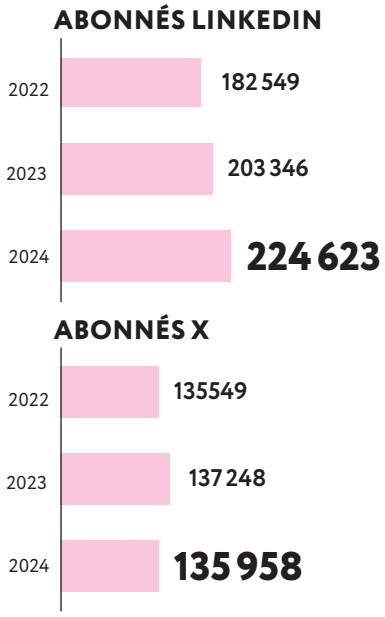
Titre de la publication	Visites uniques
Le règlement général sur la protection des données	341 342
Cookies et traceurs : que dit la loi ?	279 293
RGPD : de quoi parle-t-on ?	157 285

Top 3 des pages et fiches pratiques pour le grand public

Titre de la publication	Visites uniques
Générer un mot de passe solide	497 133
Les conseils de la CNIL pour maîtriser votre navigateur	176 435
Spam, phishing, arnaques : signaler pour agir	171 508

Sur les réseaux sociaux
Pour les internautes de la CNIL, LinkedIn reste le réseau social le plus plébiscité (+ 10,5 % vs. 2023), alors que le nombre d'abonnés au compte X (ex-Twitter) est en légère baisse (- 1%). Toutefois, la CNIL est désormais présente sur le réseau social Mastodon, dont le compte a réuni 1 900 abonnés en quelques mois.

ÉVOLUTION DU NOMBRE D'ABONNÉS SUR LES RÉSEAUX SOCIAUX



« Un défaut d'information général »

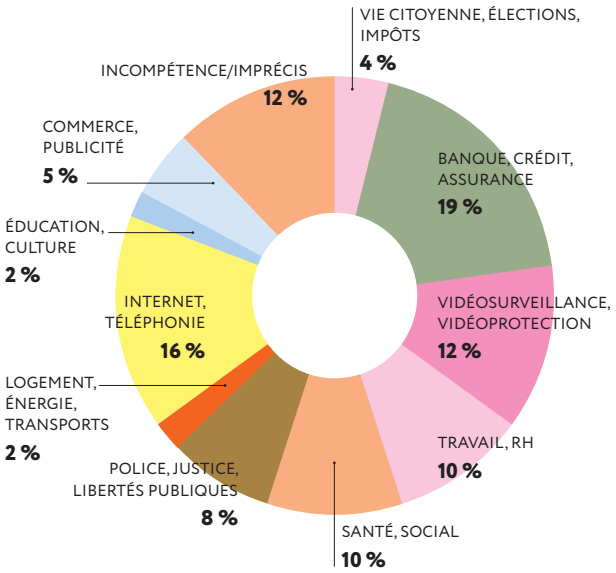
Jennifer est chargée de mission éducation au numérique à la CNIL

« En allant vers les publics, nous constatons un défaut d'information général sur la protection des données personnelles. Le cœur de nos interventions porte sur les définitions essentielles, les droits et les moyens de se protéger. Les sujets évoqués spontanément concernent les arnaques, les mots de passe, et la fiabilité des messages reçus dans l'environnement numérique. Les personnes, même quand elles disposent de connaissances, se sentent peu compétentes, voire peuvent exprimer de la honte quant aux situations vécues. Les interventions de la CNIL sont toujours bien accueillies, permettent de mettre des mots sur des expériences, de prendre conscience de ce que l'on peut faire, de développer des réflexes. »

Sur quoi portent les questions écrites du public reçues par la CNIL ?

En plus du canal téléphonique (38 386 appels répondus, toutes permanences confondues), la CNIL a répondu à **16 130 demandes écrites du public** via son formulaire de contact en ligne ou par courrier postal, pour aider chacun à comprendre ses droits et ses obligations dans de nombreuses thématiques de sa vie quotidienne.

RÉPONSES AU PUBLIC THÈMES DES REQUÊTES TRAITÉES



La sécurité des données face à des risques de plus en plus élevés

DES VIOLATIONS DE DONNÉES D'UNE AMPLEUR INÉDITE 50

LA NOTIFICATION À LA CNIL 51

NOUVELLE ÉDITION DU GUIDE SÉCURITÉ 52

SÉCURITÉ SUR LE *CLOUD* 53

L'ACCÈS AU DOSSIER PATIENT INFORMATISÉ 54

Entretien avec

Michel Combot

directeur des technologies, de l'innovation, et de l'intelligence artificielle de la CNIL

« La CNIL adapte son accompagnement à l'évolution de la menace cyber »

Quel bilan peut-on tirer en 2024 en matière cyber ?

L'année 2024 a été marquée par une série de violations massives touchant plusieurs dizaines de millions de personnes. En cascade, les données exfiltrées lors d'une violation peuvent servir à faciliter de nouvelles violations, soit directement, soit combinées avec des données issues d'autres violations. Le niveau de menace qui en résulte requiert que les particuliers et les professionnels réhaussent leur posture cyber. Pour les y aider, la CNIL adapte de manière continue ses fiches, guides et recommandations face à l'évolution de la menace. Cette année, le guide de sécurité des données personnelles a évolué pour aider les responsables de traitement à mieux sécuriser leurs données. Aussi, la consultation publique du projet de recommandation sur l'authentification multifacteur qui a eu lieu va permettre à la CNIL de publier prochainement une recommandation portant sur une mesure essentielle.

Quelle a été la participation de la CNIL à l'écosystème cyber ?

La CNIL échange avec les autres acteurs de l'écosystème à propos des risques cyber, de leurs évolutions et des mesures à mettre en œuvre pour y remédier. Elle participe aussi à des actions de sensibilisation communes à destination des particuliers et des professionnels. Enfin, lors de violations de grande ampleur, elle collabore étroitement avec les autres autorités compétentes (notamment l'Agence nationale de la sécurité des systèmes d'information – ANSSI et le parquet national cyber) et aide directement ou renvoie les victimes vers les acteurs à même de les aider au mieux (notamment Cybermalveillance.gouv.fr et le 17Cyber).

Des violations de données d'une ampleur inédite

En 2024, les violations de données ont été non seulement plus nombreuses mais aussi d'une plus grande ampleur, entraînant le vol de données de millions de Français.

Qu'est-ce qu'une violation de données ?

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

Exemples :

- suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ;
- perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ;
- introduction malveillante dans une base de données scolaires et modification des résultats obtenus par les élèves.

Les obligations des responsables du traitement concernant les violations de données personnelles, et notamment leur notification à la CNIL et aux personnes concernées, sont définies aux articles 33 et 34 du RGPD.

Tous les secteurs d'activité sont concernés

En 2024, la CNIL a été notifiée de 5 629 violations de données personnelles. C'est 20 % de plus qu'en 2024. Au-delà de cet accroissement notable, la tendance la plus préoccupante est celle d'une recrudescence des violations de très grande ampleur. **Le nombre de violations touchant plus d'un million de personnes a ainsi doublé en un an**, passant d'une vingtaine à une quarantaine d'attaques réussies. Parmi les organismes qui en ont été victimes en 2024 : France Travail, Free, les opérateurs du tiers payant Viamedis et Almerys, Auchan, la plateforme de streaming Molotov, Truffaut, Cultura, Boulanger… Autrement dit, tous les secteurs d'activité sont concernés.

Face à cet enjeu, la CNIL a fait de la cybersécurité un des axes de son plan stratégique 2025-2028 (lire page 6). En pratique, son action se traduit par :

- **l'accompagnement des organismes**, en produisant des recommandations permettant de protéger les données personnelles au regard de l'évolution de la menace et de l'état de l'art ;
- des **contrôles** sur la mise en œuvre de mesures de sécurité par les organismes ;
- **l'information et la sensibilisation** des particuliers à la cybersécurité pour les rendre acteurs de la protection de leurs données.

Parallèlement, la CNIL intensifie sa coordination avec les acteurs de la cybersécurité, en particulier l'ANSSI et Cybermalveillance.gouv.fr.

Des défauts de sécurité récurrents

Les informations fournies à la CNIL par les organismes à la suite d'une violation de données, ou obtenues à l'occasion d'un contrôle, montrent que les modes opératoires des attaquants sont souvent similaires et exploitent régulièrement les mêmes failles. Ces informations amènent notamment les constats suivants :

- les informations de connexion utilisées pour l'attaque avaient été compromises ;
- les intrusions et exfiltrations n'ont pas été détectées par l'organisme avant la mise en vente des jeux de données ;
- une part significative des incidents impliquait un sous-traitant.

5 629
violations de données
notifiées à la CNIL en 2024
+20 % par rapport
à l'année précédente

La notification à la CNIL en cas de violation de données

Un organisme ayant subi une fuite, un vol ou une perte de données susceptible d'engendrer un risque pour les personnes concernées a l'obligation de le notifier à la CNIL. Le responsable des traitements doit fournir toutes les informations sur la nature de la violation, ses conséquences et les mesures prises pour y remédier. La CNIL est alors en mesure d'accompagner l'organisme en le conseillant, lorsque cela est nécessaire, sur la meilleure manière de réagir et d'améliorer sa posture de cybersécurité. La CNIL peut aussi être amenée à collaborer avec d'autres acteurs institutionnels ayant pour mission de veiller à la cybersécurité de l'espace numérique, tels que l'ANSSI, la section cyber du parquet de Paris (J3) ou encore cybermalveillance.gouv.fr.

La notification doit être transmise à la CNIL dans les meilleurs délais suite à la constatation. Si un délai de 72 heures est dépassé, l'organisme est susceptible de devoir rendre compte des motifs du retard. La CNIL conseille donc aux organismes d'effectuer une notification initiale dans les délais, qu'ils pourront compléter par la suite.

Exemples illustrés de violations de données

Fuite de données : un exemple de procédé typique

La CNIL a retracé en 2024 les procédés les plus souvent constatés et en expose ci-dessous un exemple typique.

1• L'attaquant obtient des données de connexion (identifiant + mot de passe) d'un collaborateur ou d'un partenaire

Comment y arrive-t-il ?

- Les comptes de connexion sont génériques ou partagés.
- Un utilisateur a reçu un message (hameçonnage) l'invitant à saisir son identifiant et son mot de passe sur un faux site.
- Un logiciel malveillant a été installé sur le poste d'un utilisateur et a permis de dérober les données de connexion.
- Un utilisateur a accepté de vendre ses données de connexion.
- Des données de connexion, issues d'une précédente fuite, sont proposées sur le marché noir.

2• L'attaquant obtient un accès au système d'information (SI)

Cela se produit quand le SI est accessible librement depuis Internet, sans limitation aux seuls équipements authentifiés. L'accès au SI peut aussi venir de l'exploitation de failles de sécurité dans des pare-feu, passerelles VPN ou de filtrage.

3• L'attaquant analyse le système d'information et accède aux données de façon massive

Voici les principales causes constatées par la CNIL :

- Un grand nombre d'utilisateurs ont accès à d'importants volumes de données du fait d'habilitations trop larges.
- La récupération de toutes les entrées dans une application est possible par du script.
- Il n'existe pas de limitations quant aux requêtes ou à la fonctionnalité applicative d'export susceptibles d'être effectués par un utilisateur.
- Les données sont collectées ou partagées avec un sous-traitant de façon excessive au regard de la finalité du traitement.
- Les données en base active sont conservées pendant une durée excessive.

4• L'attaquant extrait les données de façon massive

Les indicateurs devant permettre de détecter une activité anormale, et réagir rapidement en cas d'alerte, sont inexistants, insuffisants ou inexploités.

5• L'attaquant propose les données à la vente

Le responsable du traitement ou le sous-traitant n'ont pas détecté l'exfiltration massive et/ou ne se sont pas aperçus de la mise en vente des données.

Il existe des solutions pour prévenir ces différents risques. Elles sont recensées dans le Guide de la sécurité des données personnelles (voire pages suivantes).

Nouvelle édition du guide de la sécurité des données personnelles

L'objectif de ce guide est d'accompagner les organismes dans la mise en place de mesures de sécurité pour assurer la protection des données personnelles qu'ils traitent. Cette nouvelle version introduit de nouvelles fiches, notamment sur l'intelligence artificielle, les applications mobiles et l'informatique en nuage (*cloud*).

Un contenu qui se veut accessible

La sécurité est un élément essentiel de la protection des données personnelles. L'obligation de sécurité est même inscrite dans la loi depuis 1978, renforcée par le RGPD depuis 2018. Il peut cependant être difficile, lorsque l'on n'est pas familier avec les méthodes de gestion des risques, de mettre en œuvre une telle démarche et de s'assurer que le nécessaire a bien été fait. C'est tout l'enjeu de ce guide réactualisé en mars 2024 : faciliter et guider la mise en œuvre de mesures de sécurité pour les données personnelles.

L'approche se veut pédagogique : pour aider dans la mise en conformité, chaque fiche est découpée en trois sections :

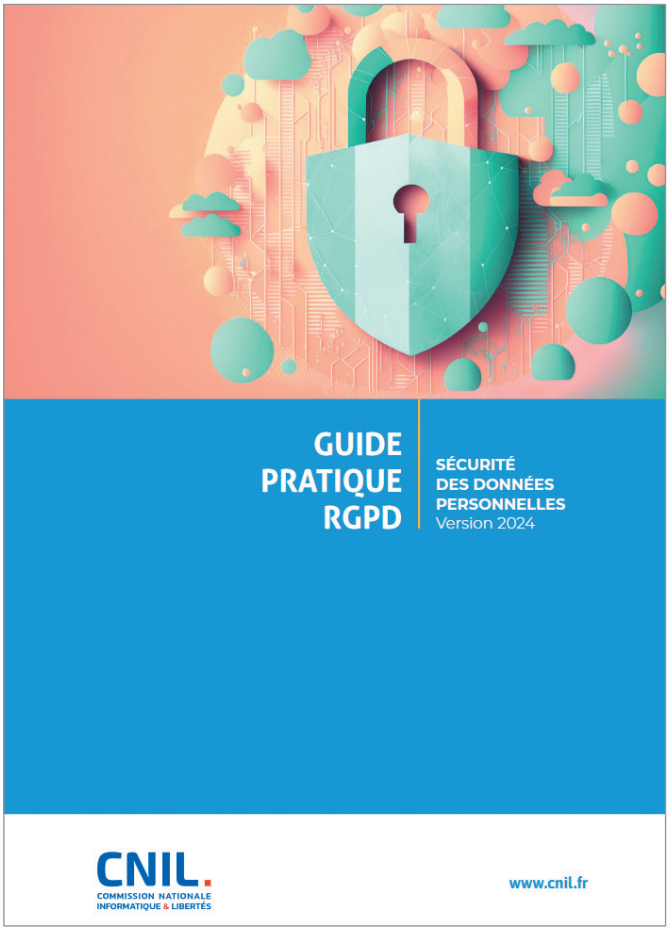
- les précautions élémentaires à mettre en œuvre, qui reprennent les bonnes pratiques essentielles ;
- les mauvaises pratiques, à proscrire ;
- les mesures complémentaires, pour aller plus loin.

Ce qui change dans la nouvelle version

Le guide a été structuré en 5 grands chapitres (« Les utilisateurs », « Mon informatique, mes équipements », « Ma maîtrise des données », « Se préparer à un accident », et des « Focus » sur des points spécifiques) afin de faciliter la navigation entre ses 25 fiches. De nouvelles fiches ont été créées, notamment pour refléter les évolutions technologiques. Elles sont dédiées à l'informatique en nuage (*cloud*), aux applications mobiles, à l'intelligence artificielle, aux interfaces de programmation applicative (*API*)…

Entre autres améliorations, les pratiques actuelles, telles que l'utilisation d'équipements personnels en environnement professionnel (*BYOD*), viennent enrichir les fiches existantes.

Un journal des modifications a été créé pour aider à identifier les changements apportés plus rapidement.



À qui s'adresse ce guide ?

Ce guide constitue une référence pour les délégués à la protection des données (DPO), responsables de la sécurité des systèmes d'information (RSSI), informaticiens et juristes. Ils pourront s'en saisir dans le cadre de leur activité liée à la sécurité des données. C'est également le guide de référence utilisé par la CNIL pour son appréciation de la sécurité des traitements de données personnelles.

Guide de la sécurité des données personnelles : nouvelle édition 2024

En bref : les mesures prioritaires pour protéger les données

Se protéger contre les violations de données nécessite d'adopter des mesures adaptées aux risques. À partir des notifications qu'elle reçoit, la CNIL constate que **des mesures techniques simples, complétées par la vigilance de tous**, permettent de réduire significativement les risques qu'une telle violation survienne.

Parmi les mesures basiques les plus indispensables, on peut citer :

- effectuer les mises à jour sans tarder, afin d'éviter l'exploitation d'une faille de sécurité ;
- adopter des mots de passe suffisamment robustes, différents pour chaque compte ;
- réaliser une sensibilisation périodique des utilisateurs, pour inclure l'humain comme acteur de la sécurité ;
- protéger les accès à la messagerie pour qu'elle ne serve pas de point d'entrée d'une attaque ;
- effectuer des sauvegardes régulières, dont une déconnectée, pour être en capacité de retrouver des données saines.

D'autres mesures techniques, plus avancées et recommandées par la CNIL et l'ANSSI, peuvent renforcer significativement la sécurité, notamment :

- la mise en place d'une authentification multifacteur, en particulier pour les accès à distance par les employés, partenaires et sous-traitants, et la systématisation des comptes nominatifs individuels ;
- la limitation de l'accès au réseau aux seuls équipements authentifiés ;
- la capacité à détecter rapidement les activités anormales sur le système d'information, par exemple via une analyse automatique des journaux et la mise en place d'équipes pour analyser les alertes.

La CNIL propose, sur son site web, 3 niveaux progressifs pour protéger ses données, adaptés aux moyens et aux besoins ce chaque organisme.

3 niveaux progressifs pour la sécurité des données

Deux fiches pratiques consacrées à la sécurité sur le *cloud*

La CNIL a reçu de nombreuses questions sur le recours à l'informatique en nuage (*cloud*), notamment au regard de la compatibilité des offres disponibles avec le RGPD. Sa précédente recommandation datant de 2012, elle a publié en janvier 2024 deux nouvelles fiches pratiques pour aider les entreprises à appréhender les questions de sécurité et de conformité qu'impliquent le recours au *cloud*, notamment vis-à-vis des questions de transferts. Ces fiches concernent, d'une part, le chiffrement des données sur le *cloud* – la CNIL y propose une analyse détaillée des différents types de chiffrement – et, d'autre part, les outils pour sécuriser un service *cloud*. Elle y opère une distinction claire entre des fonctionnalités de sécurité (anti-*DDoS*, *WAF*) et des fonctionnalités de performance (*CDN*, *load balancer*) qui sont souvent commercialisées de manière groupée.

Les fiches sur l'informatique en nuage (*cloud*)

La CNIL alerte sur les risques d'une certification européenne sur la sécurité du *cloud* qui ne tiendrait pas compte du risque d'accès non autorisé par des autorités extra-européennes

Un projet de certification européenne pour les services de *cloud* (*EUCS*) est en cours de discussion. Ce texte est amené à se substituer aux certifications ou qualifications nationales, telles que SecNumCloud. En juillet 2024, la CNIL a souligné les risques de la version étudiée en ce moment. En l'état, cette directive ne permettrait plus de garantir la protection des données stockées contre tout accès par une puissance étrangère, à l'inverse de ce que permet aujourd'hui la qualification SecNumCloud 3.2 en France. La CNIL appelle donc à réhausser le niveau de protection des données au niveau européen. Elle **recommande depuis longtemps**, pour les bases de données personnelles les plus sensibles (telles que le système national des données de santé ou les données qui concernent des mineurs), d'assurer une protection contre les possibilités de divulgation à des autorités publiques de pays tiers.

Données de santé : piqûre de rappel sur l'accès au dossier patient informatisé

La CNIL a mis en demeure plusieurs établissements de santé de prendre les mesures nécessaires pour assurer la sécurité du dossier patient informatisé. Elle a rappelé que **les données des patients ne devaient être accessibles qu'aux personnes habilitées**.

13 contrôles depuis 2020

La CNIL a été alertée, à plusieurs reprises, au sujet d'accès illégitimes à des dossiers patient informatisés (voir définition ci-contre). Cela l'a conduite à procéder, entre 2020 et 2024, à treize contrôles auprès d'établissements de santé. Ils ont permis de constater que les mesures de sécurité informatique et la politique de gestion des habilitations étaient parfois inadaptées. Des professionnels de santé pouvaient, par exemple, accéder à des informations sensibles concernant des patients s'agissant desquels ils ne participaient pas à la prise en charge. La présidente de la CNIL a donc mis en demeure, début 2024, plusieurs établissements de prendre les mesures permettant de préserver la sécurité et la confidentialité des données du DPI.

Qu'est-ce que le dossier patient informatisé ?

Le dossier patient informatisé (DPI) centralise l'ensemble des données de santé d'un patient. Il comporte les comptes rendus des consultations et séjours hospitaliers, les examens biologiques et radiologiques, et les prescriptions médicales. Le DPI permet ainsi aux professionnels de santé d'accéder facilement à l'exhaustivité des informations médicales. Objectif : améliorer la prise en charge des patients, notamment grâce à une meilleure coordination entre professionnels de santé.

Au regard de la sensibilité et du volume des données qu'il contient, le DPI doit bénéficier de mesures de sécurité renforcées.

Trois mesures de sécurité prioritaires à mettre en place

Ces mises en demeure ont été l'occasion de rappeler les mesures de sécurité, organisationnelles ou techniques, à mettre en œuvre pour répondre au contexte spécifique du DPI. Elles sont de trois types :

- sécuriser les accès au système grâce à une politique d'authentification robuste (notamment des mots de passe suffisamment complexes) ;
- prévoir des habilitations spécifiques pour que chaque professionnel de santé ou agent de l'établissement ne puisse accéder qu'aux dossiers qui le concerne ;
- mettre en place une traçabilité des accès au DPI. Elle doit non seulement permettre d'indiquer **qui s'est connecté et à quel moment**, mais, plus précisément, **qui a accédé à quoi**.
  Des contrôles réguliers de ces accès doivent être opérés, afin d'identifier ceux susceptibles d'être frauduleux ou illégitimes.

Les règles de gestion des habilitations

La politique d'habilitations, qui conditionne « qui peut accéder à quoi », doit combiner deux critères :

- d'une part, le métier exercé. Un agent responsable de l'accueil des patients ne doit ainsi pouvoir accéder qu'au dossier administratif du patient et non aux données médicales ;
- d'autre part, les habilitations doivent tenir compte de la notion d'équipe de soins, telle que définie par la loi (art. L. 1110-12 du code de la santé publique), afin que seuls les professionnels effectivement impliqués dans la prise en charge d'un patient puissent avoir accès aux informations couvertes par le secret médical.

Les habilitations accordées peuvent être complétées d'un mode « bris de glace », qui permet aux agents administratifs et professionnels de santé, en cas d'urgence, d'avoir accès à d'autres données pour tout patient. Ce mode doit en revanche faire l'objet d'une traçabilité particulière pour éviter les abus.

La CNIL recommande par ailleurs de prévoir des mesures de confidentialité renforcées pour certains dossiers particuliers, ceux des patients provenant d'un établissement pénitentiaire par exemple.

Sur la base de ces manquements constatés et des besoins des établissements concernés, la CNIL lance, au premier trimestre 2025, une consultation publique sur un projet de guide contenant 14 fiches illustrées d'exemples concrets pour sécuriser le DPI.

Des coopérations renforcées en France, en Europe et à l'international

PARTENARIATS EN FRANCE 56

COOPÉRATION EUROPÉENNE 58

ACTIONS AU NIVEAU INTERNATIONAL 59

Entretien avec

Anne Debet

vice-présidente de la CNIL et membre du Collège en charge des affaires européennes et des outils de la conformité

« Grâce à la coopération européenne, des sanctions très importantes sont prononcées »

Comment la CNIL a-t-elle participé à la régulation européenne cette année ?

–

La CNIL joue un rôle clé au sein du Comité européen de la protection des données (CEPD). C'est le service des affaires européennes et internationales, ainsi que de manière très transversale tous les autres services de notre autorité qui préparent, avec leurs homologues, au sein de différents groupes de travail, la rédaction des documents adoptés.
En 2024, les demandes d'avis au CEPD concernant le *« Pay or Consent »** proposé par les grandes plateformes en ligne ainsi que celle relative au développement et au déploiement des modèles d'IA ont été ainsi l'occasion de collaborer avec les autres autorités européennes pour apporter des éclaircissements attendus sur ces sujets.

Quelles sont les manifestations concrètes de cette coopération européenne ?

–

Une grande partie de la coopération européenne porte sur le traitement conjoint des plaintes et de leurs suites : grâce à la coopération européenne, des sanctions très importantes sont prononcées. La CNIL a ainsi reçu 630 projets de décision de ses homologues européens en 2024 en sa qualité d'autorité concernée, dont 12 portant sur des sanctions financières de plus de 20 000 €. En particulier, la CNIL a été associée très étroitement par son homologue néerlandais à la procédure concernant Uber B.V, qui a abouti au prononcé d'une sanction de 290 millions d'euros pour des transferts de données non conformes.
La CNIL a aussi lancé des investigations dans le cadre du programme d'action coordonnée européenne (*CEF* en anglais) qui portait, en 2024, sur le droit d'accès. Ce programme permet aux autorités de mettre en place des actions coordonnées en se concentrant toutes, la même année, sur un thème choisi ensemble au niveau du CEPD.

* Payer ou Consentir

Une coopération renforcée en France : les partenariats qui ont marqué l'année 2024

–

Avec l'Arcom et la DGCCRF

Le 27 juin 2024, l'Arcom, la DGCCRF et la CNIL ont signé une convention précisant les modalités de leur coopération pour la mise en œuvre du règlement sur les services numériques. Ce texte européen a pour objectif de responsabiliser les acteurs de l'économie numérique en leur imposant un ensemble d'obligations en matière de lutte contre les contenus illicites et de transparence sur le fonctionnement des algorithmes. Cette convention facilite la coopération entre les trois administrations et acte les engagements volontaires pris par chaque organisation. Elle précise également les modalités de partage d'informations relatives aux enquêtes visant des acteurs régulés et au traitement des plaintes d'utilisateurs des plateformes.

Avec Départements de France

Le 12 juin 2024, l'association qui représente les départements français et la CNIL ont renouvelé leur partenariat, avec deux priorités pour la période 2024-2027 : favoriser la circulation des données **au service de la transparence, de l'évaluation et du pilotage des politiques publiques, et accompagner l'utilisation de l'IA pour améliorer la qualité des services dans le respect** du RGPD.

Avec le Conseil supérieur de l'ordre des experts-comptables

Le 27 juin 2024, cet ordre, qui compte 22 000 professionnels et 170 000 collaborateurs, et la CNIL ont renouvelé leur convention de partenariat initiée en 2020. Avec notamment l'objectif de diffuser une culture « protection des données personnelles » auprès des experts-comptables, pour leur propre structure mais aussi dans leur rôle de conseil auprès des TPE-PME.

Avec la Conférence des grandes écoles

Le 19 février 2024, la Conférence, qui rassemble plus de 240 grandes écoles, et la CNIL ont signé une nouvelle convention de partenariat afin de poursuivre leurs actions de sensibilisation et d'information à destination des personnels et des étudiants sur le respect du RGPD.

Avec la DGCCRF

Le 18 novembre 2024, la DGCCRF et la CNIL ont signé un nouveau protocole de coopération mettant à jour la convention initiale de 2011 (lire ci-contre).

15 propositions pour favoriser les synergies avec l'Autorité de la concurrence

Bruno Lasserre, membre du Collège de la CNIL et ancien président de l'Autorité de la concurrence (ADLC), a rendu le 28 novembre 2024 les conclusions de la mission que lui avait confiée la présidente de la CNIL. Alors que la CNIL et l'Autorité de la concurrence approfondissent leur coopération, Marie-Laure Denis souhaitait des propositions pour une meilleure articulation entre protection des données et concurrence. Le constat de départ est que les deux réglementations ne peuvent pas, dans l'économie numérique d'aujourd'hui, fonctionner « en silos », leurs objectifs étant partiellement convergents et les impacts de leurs actions étant dépendants les uns des autres dans bien des cas.

« *Protéger la vie privée et les données personnelles passe par une meilleure prise en compte des réalités économiques et concurrentielles* » souligne Bruno Lasserre. « *Même si le RGPD n'est pas une régulation économique mais relevant des libertés fondamentales, l'angle économique et concurrentiel concourt de manière significative à son effectivité et à son impact.* » La mission qu'il a dirigée fait 15 propositions opérationnelles pour favoriser les synergies entre la CNIL et l'ADLC, comme « *instaurer au sein de chaque autorité un point de contact chargé de piloter la coopération* » ou encourager la saisine de la CNIL par l'Autorité de la concurrence « *lorsque la vie privée et les données personnelles sont en jeu dans un dossier de concentration* ».

Entretien avec

Sarah Lacoche

directrice générale de la DGCCRF

« Protection des consommateurs et protection des données sont des enjeux liés et complémentaires »

Quels sont les enjeux du nouveau protocole de coopération entre la CNIL et la DGCCRF ?

–

Dans l'économie numérique, les achats en ligne et les services fournis aux consommateurs s'accompagnent le plus souvent de l'exploitation commerciale de leurs données personnelles. La progression constante de cette dimension numérique dans les échanges économiques fait de la protection des consommateurs et de la protection des données des enjeux liés et complémentaires, nécessitant une coopération étroite entre les autorités compétentes.

Un premier protocole a été signé en 2011. Quel bilan tirez-vous de cette collaboration ?

–

Les deux autorités ont échangé plusieurs dizaines de signalements, luttant ainsi contre les pratiques commerciales abusives et non conformes à la protection des données, sur des sujets tels que la prospection liée à la rénovation énergétique, au démarchage téléphonique abusif ou la gestion des programmes de fidélité. Ce type de pratique fait l'objet de signalements systématiques à la CNIL, seule autorité habilitée à sanctionner le non-respect des dispositions du RGPD.

Pourquoi renouveler et renforcer cette coopération ?

–

Le renforcement de notre collaboration va notamment permettre de dégager des interprétations harmonisées entre nos deux cadres juridiques et de veiller à la cohérence de leur application, de mutualiser les expertises sur les outils et les techniques d'enquête, et de mettre en œuvre des analyses économiques communes, notamment sur les effets de mécanismes tels que les procédés manipulatoires sur les sites commerciaux (*dark patterns*). Dès 2025, des actions communes de formation vont être mises en place entre la CNIL et la DGCCRF.

Ce partenariat renforcé vient aussi compléter la convention de coopération, signée également avec l'Arcom, pour la mise en œuvre du nouveau règlement européen sur les services numériques en ligne.

La coopération européenne au quotidien : les travaux du CEPD

Une clarification de la notion de « traçage » de la directive ePrivacy

Pour tracer les internautes dans une logique de ciblage commercial, l'écosystème publicitaire recourt de plus en plus à des méthodes alternatives aux cookies. Ces nouvelles méthodes restent néanmoins soumises aux mêmes règles vis-à-vis de la protection de la vie privée, notamment la directive ePrivacy. Afin de clarifier et de réaffirmer ces règles, la CNIL a souhaité la consolidation d'une position commune au niveau européen. Après une consultation publique lancée fin 2023, le Comité européen de la protection des données (CEPD) a adopté le 7 octobre 2024 la version finale des lignes directrices relatives à la directive ePrivacy.

Ces lignes directrices précisent des **notions clés**, à savoir celles d'« information », d'« équipement terminal d'un abonné ou d'un utilisateur » et de « stockage d'informations, ou […] obtention de l'accès à des informations déjà stockées ». Elles comportent aussi un ensemble de **cas d'usages** représentatif des pratiques de l'écosystème publicitaire, notamment **les liens et pixels de suivi, les identifiants uniques et le traitement local de données.**

« Consentir ou Payer » : donner un vrai choix à l'internaute

Le 17 avril 2024, le CEPD s'est prononcé sur le modèle « Consentir ou Payer », une nouvelle option proposée par certaines grandes plateformes : elles invitent les utilisateurs soit **à consentir au traitement de leurs données personnelles** à des fins de publicité comportementale, soit à **payer une redevance** afin que leurs données ne soient pas traitées. Le CEPD met en avant la nécessité de donner un véritable choix aux utilisateurs. Il précise que, dans la plupart des cas, il ne sera pas possible pour les opérateurs de respecter les exigences relatives à un consentement valable si les utilisateurs se voient proposer seulement un choix binaire entre le consentement au traitement des données personnelles à des fins de publicité comportementale et le paiement d'une redevance. L'avis invite donc fortement les grandes plateformes à proposer une alternative supplémentaire qui devrait être gratuite et dépourvue de publicité comportementale (par ex. la publicité contextuelle).

LES PRODUCTIONS DU CEPD EN 2024

4 **lignes directrices européennes**

59 **autres documents** (déclarations, bonnes pratiques, rapports…)

Vers une meilleure coopération en matière répressive

À la suite d'une initiative du CEPD, la Commission européenne a publié en juillet 2023 une proposition de règles harmonisées de procédure visant à renforcer la coopération en matière répressive dans le cadre du RGPD. Toutefois, certaines dispositions comportent des risques, en particulier de surcharge procédurale pour les autorités de protection des données. La CNIL s'est fortement investie dans le suivi de ce texte et notamment dans la préparation de l'avis conjoint du CEPD et du Contrôleur de la protection des données adopté en septembre 2023 et dans la déclaration d'octobre 2024 faisant suite à l'adoption des positions du Parlement européen et du Conseil. Le projet de règlement est toujours en cours de négociation. Un texte final pourrait être adopté en 2025.

Avis sur la reconnaissance faciale dans les aéroports

Le 24 mai 2024, le CEPD a adopté un avis sur la reconnaissance faciale utilisée par les exploitants d'aéroports et les compagnies aériennes pour rationaliser le flux de passagers. Il considère que les scénarios compatibles avec le RGPD sont ceux où les individus gardent le contrôle sur leurs données biométriques. Autrement dit, dans la plupart des cas, les solutions qui passent par un stockage ou une activation via le téléphone portable des usagers. Cet avis fait suite à une demande de la CNIL d'avoir une position harmonisée à l'échelle européenne face à une pratique qui tend à se répandre en Europe et au-delà. Il ne couvre toutefois pas l'utilisation de la reconnaissance faciale à des fins de sécurité, de contrôle des frontières ou par les services répressifs.

Concilier protection des données, concurrence et protection du consommateur

En mars 2023, le CEPD a créé en son sein une *task force*, dont la CNIL est un des coordinateurs, chargée de réfléchir à l'articulation entre protection des données, concurrence et protection du consommateur, et à l'amélioration de la coopération entre régulateurs nationaux dans ces domaines. Fin 2024, cette *task force* s'est transformée en sous-groupe appelé *Cross-Regulatory Interplay and Cooperation (*CIC*),* chargé également de l'interrégulation entre la protection des données et le paquet numérique européen, avec un regard transversal sur les aspects de gouvernance.

Toute l'actualité du CEPD

International

Les autorités de protection des données du G7 affirment leur rôle dans la gouvernance de l'IA

Réunies à Rome du 7 au 11 octobre 2024 sous la présidence de l'autorité italienne, les autorités de protection des données du G7 ont notamment adopté une position commune sur leur rôle dans la promotion d'une intelligence artificielle digne de confiance. Elles ont aussi souligné la nécessité de protéger les droits fondamentaux des mineurs dans le contexte du développement de l'IA.

Coopération avec l'Agence californienne de protection de la vie privée

L'Agence californienne de protection de la vie privée (CPPA) et la CNIL ont signé une déclaration de coopération le 25 juin 2024, à Paris. Elle prévoit notamment :

- la conduite de recherches conjointes liées aux nouvelles technologies et aux questions de protection des données ;
- le partage de bonnes pratiques et d'expériences, y compris dans le cadre de leurs enquêtes ;
- l'organisation d'ateliers de travail.

Toute l'actualité internationale

« Ma mission nécessite à la fois de bonnes capacités d'organisation et d'anticipation, mais aussi le sens du compromis »

Anne est juriste expert au service des affaires européennes et internationales

Comment fonctionne la coopération entre autorités dans le cadre des travaux au sein du CEPD sur le sujet des transferts de données hors Union européenne ?

Le CEPD est composé d'une vingtaine de sous-groupes thématiques. Ils préparent les documents qu'adopte la plénière du CEPD, réunissant les présidents des autorités de protection des données européennes. C'est donc au sein des sous-groupes que se joue le cœur du travail de coopération européenne. Le sujet des transferts est traité par le sous-groupe ITS (*International Transfers*) dont le mandat couvre tous les instruments définis par le RGPD pour encadrer les transferts : adéquations, codes de conduite et certifications, des règles d'entreprises contraignantes (BCR en anglais), clauses contractuelles types, etc.

Quel est votre rôle au sein de ce sous-groupe ?

J'ai été désignée coordinatrice de l'ITS en 2022 avec mon homologue de l'autorité danoise. Nous préparons et animons les réunions mensuelles qui rassemblent une quarantaine d'agents de toutes les autorités européennes. Des réunions qui peuvent durer un jour et demi. Ma mission nécessite à la fois de bonnes capacités d'organisation et d'anticipation, mais aussi le sens du compromis pour dégager une position commune dans des délais raisonnables tout en veillant à ce que chaque participant s'exprime.

En 2024, plusieurs travaux ont abouti, dont l'adoption des lignes directrices sur l'article 48 du RGPD dont je suis rapporteur principal. Ce document clarifie, de façon synthétique, ce que les entités dans l'Union peuvent faire si elles reçoivent des requêtes d'autorités étrangères demandant à ce que des données leur soient communiquées.

Les ressources humaines et financières

Entretien avec

Jean-Marc Salmon

directeur administratif et financier

« Chaque année, la CNIL s'applique à gérer efficacement et rigoureusement les crédits et les effectifs qui lui sont alloués. »

Quels sont les événements marquants d'un point de vue budgétaire ?

En 2024, la CNIL a poursuivi ses missions classiques, toujours en forte croissance notamment concernant les plaintes et les sanctions, et s'en est vu confier de nouvelles, exigeantes, en particulier s'agissant de celles prévues par le législateur européen et français (par exemple au titre du « paquet numérique européen » ou pour la mise en œuvre du « filtre cyber »). La CNIL a dû réaliser tout cela dans un contexte budgétaire difficile.
En effet, comme la plupart des administrations et des opérateurs de l'État, la CNIL a subi, fin février 2024 donc en cours d'exercice, une annulation d'une partie de ses crédits de masse salariale et de fonctionnement. En dépit de ces contraintes conjoncturelles et de moyens réduits, la CNIL s'est appliquée, comme chaque année, à gérer efficacement et rigoureusement les crédits et les effectifs qui lui sont alloués.

Et du point de vue des ressources humaines ?

Le contexte budgétaire en 2024 a conduit la CNIL à décaler en fin d'année certains remplacements d'agents et plusieurs nouveaux recrutements, pourtant cruciaux pour l'atteinte de ses objectifs. Elle a également dû réduire des recrutements d'apprentis et des contrats temporaires.
Ainsi, dans un contexte budgétaire s'annonçant d'ores et déjà difficile aussi pour 2025 et les années à venir, de nouvelles remises en cause de ses moyens financiers et humains, mettraient en risque la capacité de la CNIL à assurer de manière satisfaisante des missions pourtant essentielles à la préservation des libertés fondamentales de chacun.

Une maitrise budgétaire maintenue

En 2024, le budget alloué à la CNIL s'est élevé à 28 238 114 € en autorisations d'engagement (AE) et en crédits de paiement (CP) après l'application des réserves de précaution et d'aléas de gestion répartis comme suit :

- 23 980 774 € pour la masse salariale (titre 2)
- 4 255 663 € en AE et en CP pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6).

Dotation minorée

Le gouvernement a procédé à des économies sur les crédits accordés aux administrations et opérateurs de l'État, dans le cadre du budget 2024. Elles se sont traduites pour la CNIL par :

142 000 €
d'annulations sur les crédits de masse salariale
et de **16 743 €** sur les crédits de fonctionnement.

180 000 €
de crédits de fonctionnement
obtenus en fin de gestion, en provenance du programme 308 « Protection des droits et libertés », afin de financer la mise à jour et le renouvellement de son parc informatique.

99 % **des crédits de dépenses de personnel**
consommés
et **97 %** du plafond d'emploi

100 % de la dotation allouée en AE pour dépenses de fonctionnement a été utilisées
et **91 %** de la dotation allouée en CP.

87 % de charges incompressibles

L'exécution réalisée en 2024 atteste donc d'une gestion rigoureuse. À titre d'illustration, sur un budget de fonctionnement de 4 M€, 87 % représentent des charges incompressibles (frais de fonctionnement courant, actions sociales, formations…), laissant seulement une marge de manœuvre de 600 K€ pour financer des projets innovants.
Une réduction budgétaire en 2025 compromettrait ainsi la capacité de la CNIL à mettre correctement en œuvre ses missions.

23 980 774 €
pour la masse salariale

4 255 663 €
en AE et en CP pour les dépenses de fonctionnement, d'investissement et d'intervention

BUDGET OPÉRATIONNEL DE PROGRAMME 2024	AUTORISATIONS D'ENGAGEMENT	CRÉDITS DE PAIEMENT
Total budget PLF - crédits demandés	**28 646 143**	**28 646 143**
PLF Titre 2	24 243 904	24 243 904
PLF Hors Titre 2	4 402 239	4 402 239
Taxation interministérielle T2	-	-
Taxation interministérielle HT2	-	-
Amendement	-	-
Total budget LFI - crédits votés	**28 646 143**	**28 646 143**
LFI Titre 2	24 243 904	24 243 904
LFI Hors Titre 2	4 402 239	4 402 239
Réserve précaution T2	- 121 220	- 121 220
Réserve précaution HT2	- 242 123	- 242 123
Gel et Sur-Gel de crédits HT2	- 66 034	- 66 034
Crédits complémentaires ou annulations T2	- 141 910	- 141 910
Crédits complémentaires ou annulations HT2	163 257	163 257
Total budget Ouvert	**28 238 114**	**28 238 114**
Budget T2	23 980 774	23 980 774
Budget Hors Titre 2	4 257 339	4 257 339
Total Remontés de crédits au SPM	**1 676**	**1 676**
Budget T2 (NC →2014)	-	-
Budget Hors Titre 2	1 676	1 676
Total budget Ouvert	**28 236 438**	**28 236 438**
Budget T2	23 980 774	23 980 774
Budget Hors Titre 2	4 255 663	4 255 663
Total budget Consommé	**28 056 243**	**27 690 276**
Budget T2	23 809 424	23 809 424
Budget Hors Titre 2	4 246 819	3 880 852
Solde	**180 195**	**546 162**
Budget T2	171 350	171 350
Budget Hors Titre 2	8 844	374 811
% de consommation / budget ouvert	**99%**	**98%**
% de consommation / budget ouvert T2	**99%**	**99%**
% de consommation / budget ouvert HT2	**100%**	**91%**
Postes	**298**	
Plafond d'emploi en ETPT	**292**	
Création de postes	**10**	

Les ressources humaines

En 2024, dans la continuité des années précédentes, la CNIL a bénéficié de 10 créations de postes, portant son effectif de 288 à 298 équivalents temps plein (ETP). Ces recrutements ont été essentiels pour accompagner l'évolution de ses missions, classiques et nouvelles, et répondre ainsi à l'augmentation des sollicitations.

Renforcement des effectifs

Les nouvelles créations de postes ont notamment permis :

- le renforcement de la chaîne répressive avec 2 nouveaux postes à la direction de la protection des droits et des sanctions (devenue la Direction de l'exercice des droits et des plaintes et la Direction des contrôles et des sanctions en 2025) ;
- la professionnalisation des métiers, incluant 1 nouveau chef(fe) de projet SI ;
- le renforcement de l'encadrement de proximité, avec 1 nouveau chef(fe) de service adjoint(e).

Rémunérations et gestion budgétaire

Dans un souci d'attractivité et de reconnaissance des compétences, la CNIL a poursuivi ses actions en faveur des rémunérations, notamment à travers une revalorisation des compléments individuels de rémunération (CIR), ciblée sur les agents les plus méritants et les experts.

Cependant, la gestion des crédits T2 a été impactée par des annulations de crédits en cours d'année à hauteur de 142 000 €. Pour faire face à cette contrainte, des mesures d'économies strictes ont été mises en place, incluant :

- le report de certains remplacements et recrutements ;
- la réduction du nombre d'apprentis et de contrats temporaires.

Ce ralentissement des recrutements en début d'année pour raison budgétaire n'a pas pu être entièrement compensé en fin de gestion, ce qui n'a pas permis d'atteindre complètement le plafond d'emplois fixé pour 2024 à 292 ETPT. Le schéma d'emplois fixé a néanmoins été respecté à +12.

Optimisation du plafond d'emplois

Malgré ces contraintes, la CNIL a optimisé les marges dégagées par les vacances de postes, résultant des délais de recrutement et du renouvellement naturel des effectifs. Cette gestion fine a permis :

- un soutien renforcé aux directions métiers, via l'attribution de mois supplémentaires de contrats non permanents ;
- une consommation du plafond d'emplois de 97 %, malgré les tensions généralisées sur le marché du travail.

DONNÉES SOCIALES

298
emplois fin 2024

Âge moyen
40 ans

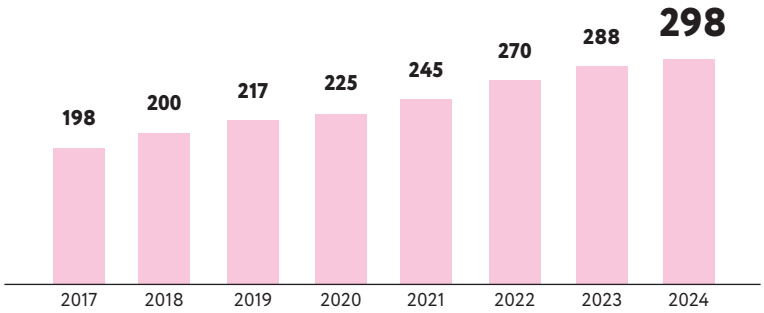
62 % des agents travaillant à la CNIL sont **arrivés entre 2019 et 2024**

84 %
des agents occupent un **poste de catégorie A**

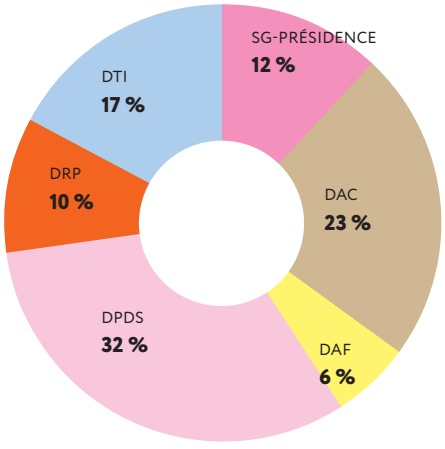
62 %
de femmes
38 %
d'hommes

L'ancienneté moyenne à la CNIL est de
7 ans et 1 mois.

ÉVOLUTION DU NOMBRE D'EMPLOIS EN ETP



RÉPARTITION DES EFFECTIFS AU 31/12/2024



COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS
–
3, PLACE DE FONTENOY
TSA 80715
75334 PARIS CEDEX 07
TÉL. 01 53 73 22 22

cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles