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

COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS
–
RAPPORT ANNUEL 2025

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 2025 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 proactif pour un numérique de confiance 20

COMMENT LA CNIL ACCOMPAGNE LES PARTIS POLITIQUES, LES CANDIDATS, ET LEURS SOUS-TRAITANTS 21

DES OUTILS AU SERVICE DES PROFESSIONNELS 23

APPLICATIONS MOBILES : LA CNIL ENRICHIT SES RECOMMANDATIONS 25

SILVER ÉCONOMIE : 6 PROJETS INNOVANTS SONT ACCOMPAGNÉS 25

VIDÉOPROTECTION ET CAMÉRAS AUGMENTÉES : ZOOM SUR CE QUI EST AUTORISÉ 25

7 CONSULTATIONS LANCÉES EN 2025 26

AFFICHAGE DES LISTES DE CLASSES : LES BONNES PRATIQUES POUR PROTÉGER LES ÉLÈVES 27

LA CNIL INTERROGE LES FRANÇAIS SUR LES ABONNEMENTS PAYANTS 27

LES ÉVÉNEMENTS DÉDIÉS AUX PROFESSIONNELS 28

2. Plaintes, contrôles, sanctions : des actions rigoureuses, efficaces et équilibrées 29

LA HAUSSE DES PLAINTES S'ACCÉLÈRE 30

LA PROCÉDURE DU GUICHET UNIQUE POUR LES PLAINTES TRANSFRONTALIÈRES 31

DES RAPPELS À LA RÉGLEMENTATION CONCERNANT LA TÉLÉSURVEILLANCE D'EXAMENS ET LA VIDÉOPROTECTION EXCESSIVE DANS LES COMMUNES 31

LE FICOBA NE DÉPEND PLUS DE L'EXERCICE DES DROITS INDIRECTS GÉRÉ PAR LA CNIL 32

LE LINC PUBLIE LE BILAN DE L'OBSERVATOIRE DU DROIT D'ACCÈS SUR LES RÉSEAUX SOCIAUX 32

4 THÉMATIQUES DE CONTRÔLE PRIORITAIRES 33

LES CONTRÔLES EN COOPÉRATION AU NIVEAU EUROPÉEN 34

COMMENT SE PASSE UN CONTRÔLE DE LA CNIL ? 34

UN NOMBRE D'AMENDES STABLE MAIS AVEC DES MONTANTS IMPORTANTS 35

DEUX SANCTIONS MARQUANTES EN 2025 37

L'ACTIVITÉ CONTENTIEUSE 37

Mentions légales

Commission nationale
de l'informatique et des libertés

3, place de Fontenoy – 75007 PARIS

www.cnil.fr / Tel. 01 53 73 22 22

Conception et réalisation graphique :
La Netscouade
www.lanetscouade.com

Impression :
Direction de l'information légale
et administrative

Conception éditoriale :
CNIL / Citizen Press

Crédits photos :
John Nguyen : page 7
Inria / G. Murat : page 42

Date de publication : Mai 2026

Prévu par l'article 11 de la 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.

3. **La régulation de l'IA et le soutien à l'innovation** 38

LES NOUVELLES RECOMMANDATIONS CONCERNANT L'IA 39

MOBILISATION AUTOUR DU SOMMET POUR L'ACTION SUR L'IA 40

BILAN DU « BAC À SABLE » SUR L'IA ET LES SERVICES PUBLICS 40

DEUX FAQ SUR L'UTILISATION DE L'IA DANS LES ÉTABLISSEMENTS SCOLAIRES 41

PANAME : UN PARTENARIAT POUR L'AUDIT DE LA CONFIDENTIALITÉ DES MODÈLES D'IA 41

UN OUTIL POUR LA TRAÇABILITÉ DES MODÈLES D'IA PUBLIÉS EN SOURCE OUVERTE 42

EXPLIQUER L'EXPLICABILITÉ DE L'IA 42

LES ÉVÉNEMENTS LIÉS À L'INNOVATION ET À L'ÉTHIQUE 43

LA MORT NUMÉRIQUE, THÈME DE AIR2025 ET DU CAHIER INNOVATION ET PROSPECTIVE 43

4. **Jeunes, familles, adultes : la sensibilisation au plus près des publics** 44

LES PARTENARIATS DE LA CNIL POUR S'ADRESSER AU GRAND PUBLIC ET AUX JEUNES 45

LES ACTIONS SUR LE TERRAIN 46

LES NOUVELLES RESSOURCES POUR LES JEUNES ET LEURS FAMILLES 47

UN FORT ATTRAIT DU PUBLIC POUR LES ACTIONS ET LES PUBLICATIONS DE LA CNIL 49

5. **Le défi permanent de la sécurité des données** 51

LES VIOLATIONS DE DONNÉES ATTEIGNENT UN NIVEAU EXCEPTIONNEL 52

LA CNIL RAPPELLE SES CONSIGNES POUR RENFORCER LA SÉCURITÉ DES GRANDES BASES DE DONNÉES 54

CONFORTER LE CHIFFREMENT DES COMMUNICATIONS COMME SOURCE DE CONFIANCE DANS LES USAGES NUMÉRIQUES 54

ÉDUCATION NATIONALE : DEUX GUIDES PRATIQUES SUR LES VIOLATIONS DE DONNÉES 54

ÉCONOMIE DE LA CYBERSÉCURITÉ ET BÉNÉFICES DU RGPD 55

COMMENT CONCILIER SOLUTIONS DE CYBERSÉCURITÉ ET PROTECTION DES DONNÉES ? 55

PARTICIPATION AU FORUM INCYBER 55

COMMENT SE PROTÉGER FACE À L'HAMEÇONNAGE ? 56

6. **Le développement des coopérations en France, en Europe et à l'international** 57

LES 3 AXES DE LA STRATÉGIE EUROPÉENNE ET INTERNATIONALE DE LA CNIL POUR 2025-2028 58

LES PARTENARIATS QUI ONT MARQUÉ 2025 59

COOPÉRATION EUROPÉENNE : LES GRANDES DÉCISIONS DU CEPD EN 2025 60

INNOVATION RESPONSABLE ET PROTECTION DES MINEURS : DEUX PRIORITÉS POUR LES AUTORITÉS DE PROTECTION DES DONNÉES DU G7 61

LA CNIL ACCUEILLE EN 2026 LA TABLE RONDE DES AUTORITÉS DE PROTECTION DES DONNÉES DU G7 61

7. **Les ressources humaines et financières** 62

UNE GESTION AU PLUS PRÈS DES CRÉDITS ACCORDÉS DANS UN CONTEXTE BUDGÉTAIRE CONTRAINT 63

DES MOYENS À RENFORCER POUR ASSURER LES NOUVELLES MISSIONS 63

LES RESSOURCES HUMAINES 64

La CNIL, régulateur des données personnelles

4 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 la possibilité de mener des investigations, que sur la capacité de prononcer des sanctions, notamment sous la forme d'amendes.

2018
entrée en application 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 renforcés.

2025
entrée en application progressive du règlement sur l'IA (RIA)

Face à l'essor de l'intelligence artificielle, le règlement européen sur l'IA (RIA) est la première législation générale au monde en la matière. S'appliquant progressivement depuis le 2 février 2025, il encadre le développement, la mise sur le marché et l'utilisation de systèmes d'IA susceptibles de présenter des risques pour la santé, la sécurité ou les droits fondamentaux. Dans ce contexte, la CNIL a officiellement été désignée en 2025 en tant qu'autorité de protection des droits fondamentaux, ce qui lui confère une fonction d'alerte et de contrôle sur les systèmes d'IA à haut risque. D'autres compétences devraient lui être attribuées en 2026.

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.

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.).

303
agents en 2025

30,2 M€
de budget en 2025

Contacter la CNIL

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

Par téléphone,
tous les jours ouvrés de 9 h 30 à 17 h 00 :
01 53 73 22 22

Par courrier :
CNIL, 3 place de Fontenoy, 75007 PARIS

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

Quels sont les sujets sur lesquels la CNIL s'est particulièrement mobilisée en 2025 ? Quels enseignements en tirez-vous ?

La CNIL est un acteur transversal, qui agit partout où il y a des données personnelles. Cette situation, dans un contexte d'accélération de la numérisation de la société, fait qu'elle est chaque jour interpellée sur une multitude de sujets, avec une forte attente de ses différents interlocuteurs : administrations, entreprises et particuliers.

Ceci étant, malgré le foisonnement des sollicitations, plusieurs sujets ressortent particulièrement dans le bilan de l'année 2025.

Le premier concerne les violations de données personnelles. L'année 2024 établissait un record. Il a malheureusement été dépassé en 2025 avec presque 10 % de notifications supplémentaires. Ce qui frappe, c'est la diversité des cibles : opérateurs de téléphonie, ministères régaliens, fédérations sportives. Face à cette menace qui concerne tous les secteurs, la mobilisation de la CNIL s'inscrit à chaque étape : en amont, pour prévenir les risques ; au moment de l'incident, pour accompagner la gestion de crise ; et, lorsque cela s'avère nécessaire, après coup, pour contrôler et sanctionner.

À ce stade, trois enseignements peuvent être tirés des notifications faites à la CNIL : personne n'est épargné ; les violations sont de plus en plus massives ; elles impliquent souvent des prestataires. En réaction, au printemps 2025, nous avons fortement incité les organismes gérant de grandes bases de données à, notamment, mettre en place une authentification multifacteur pour les accès à distance. Après avoir laissé un temps d'adaptation aux acteurs, des contrôles seront réalisés tout au long de l'année 2026.

> *« L'année 2025 constitue une année charnière pour la CNIL, en ce qu'elle se voit attribuer, par l'exécutif sous réserve de la confirmation du Parlement, quatre rôles distincts et complémentaires en matière de régulation de l'IA. »*

Marie-Laure Denis
présidente de la CNIL

Le deuxième sujet est celui de l'intelligence artificielle.

L'année 2025 constitue une année charnière pour la CNIL, en ce qu'elle se voit attribuer, par l'exécutif sous réserve de la confirmation du Parlement, quatre rôles distincts et complémentaires en matière de régulation de l'IA.

Tout d'abord, la CNIL conserve sa fonction historique d'autorité de protection des données régulant les algorithmes utilisant des données personnelles. Ensuite, elle contrôlera l'absence d'usage de systèmes d'IA interdits, et, parallèlement, aura une fonction d'alerte en tant qu'autorité de protection des droits fondamentaux. Enfin, elle agira comme autorité de surveillance du marché pour une large partie des systèmes d'IA à haut risque, notamment dans les domaines de la biométrie, de l'emploi, de la migration ou encore des usages répressifs.

J'y vois la reconnaissance de l'expertise de la CNIL et de l'implication dont elle a fait preuve depuis 2023 pour accompagner le déploiement de systèmes d'IA éthiques et respectueux des droits.

Le troisième thème concerne les mineurs et leur protection dans l'univers numérique. En pratique, l'action de la CNIL se matérialise par de nombreux contenus pédagogiques – vidéos, affiches, livrets d'information pour les parents – afin d'accompagner les jeunes et leur entourage. En 2025, les productions ont été orientées vers les adolescents car ils sont particulièrement exposés. Les deux réalisations emblématiques sont un manga, qui aborde de manière ludique des sujets essentiels comme la protection de la vie privée ou le cyberharcèlement, et une application mobile, FantomApp, développée sur fonds européens, qui facilite notamment la possibilité pour les jeunes de s'opposer à la diffusion d'informations les concernant sur les réseaux sociaux.

Parallèlement, dans le cadre de contrôles menés en 2024 et 2025 concernant la protection des données des mineurs en ligne, la CNIL a notamment constaté que, bien souvent, les acteurs n'adaptent pas les mentions d'information à ce type de public. Une dizaine de mises en demeure a été adressée aux organismes concernés. Compte tenu de la faible maturité constatée, la CNIL poursuivra son action en 2026.

Les trois sujets que je viens d'évoquer ont suscité de nombreuses demandes : entreprises souhaitant être accompagnées dans le déploiement de l'IA, particuliers adressant une plainte à la suite d'une violation de données ou parlementaires sollicitant un éclairage sur la régulation à mettre en place pour protéger les jeunes de l'exposition précoce aux écrans.

Ils constituent, par ailleurs, l'ossature du plan stratégique 2025-2028, confirmant dans les faits que la CNIL est connectée aux enjeux numériques d'aujourd'hui.

Comment la CNIL aborde-t-elle son rôle dans la régulation de l'intelligence artificielle et comment s'y prépare-t-elle ? Quels sont les principaux défis ?
–

Dès 2023, la CNIL a fait le choix d'anticiper ces évolutions avec la création d'un service de l'intelligence artificielle, qui compte aujourd'hui six personnes et qui devra être renforcé. Cela nous a permis de réaliser un travail conséquent, notamment à travers la publication de nombreuses fiches pratiques destinées à guider les organismes publics et privés sur la manière de concilier développement et usage de l'IA avec la protection des données personnelles.

Ce travail sera poursuivi, mais il n'est plus suffisant. Avec l'entrée en application du règlement sur l'intelligence artificielle (RIA) et l'attribution de nouvelles compétences, il s'agira désormais de réguler des secteurs d'activité, de procéder à la surveillance de marchés.

En pratique, ces nouvelles missions vont impliquer d'élaborer une doctrine de bon usage de l'IA dans les domaines relevant de notre compétence, d'accompagner les acteurs et de certifier leur conformité dans certains cas. Il appartiendra aussi à la CNIL de contrôler et, le cas échéant, de sanctionner les mauvaises pratiques.

Tout cela, la CNIL le faisait déjà dans le cadre du règlement général sur la protection des données (RGPD). Pour autant, la surveillance de marchés nous place dans un rôle différent. À court terme, nos deux principaux défis sont d'adapter notre façon de travailler à ce nouveau métier et de nous approprier le RIA sous un angle opérationnel.

À cet égard, il est intéressant de relever que les délégués à la protection des données (DPO) font face à des enjeux similaires. Une étude menée en 2025 avec le ministère du Travail et des Solidarités et l'Association française des correspondants à la protection des données (AFCDP) montre que l'IA transforme leur métier : 60 % d'entre eux se déclarent souvent impliqués dans les projets d'IA et manifestent, dans le même temps, un fort besoin d'accompagnement et de montée en compétences, tant sur le plan technique que juridique.

Forts de leur expérience et de leurs compétences en matière de conformité, les DPO disposent des qualités pour jouer un rôle de premier plan dans la conformité au RIA. La CNIL souhaite étendre sa collaboration avec eux sur ce sujet.

Quelles sont les conséquences de la multiplication des textes visant à réguler le numérique sur l'activité de la CNIL ? Comment s'adapte-t-elle ?
–

Au cours des deux dernières années, la CNIL a connu un accroissement sans précédent de ses missions, principalement en raison de textes européens, comme le règlement sur les services numériques (*DSA - Digital Services Act*) concernant la transparence des algorithmes, le ciblage publicitaire et le profilage des mineurs ou le règlement sur la gouvernance des données (*DGA - Data Governance Act*) en matière d'altruisme des données. S'ajoutent également à cela le règlement relatif à la transparence et au ciblage de la publicité à caractère politique et enfin, le plus important de tous en termes d'impact, le RIA.

Ces évolutions renforcent le rôle de la CNIL en tant que régulateur central du numérique et permettent de consolider la cohérence de son action.

Le revers de la médaille est qu'elles augmentent sa charge de travail dans d'importantes proportions, sans que ses moyens humains ou matériels soient augmentés.

Ce surcroît de travail n'est pas uniquement la conséquence mécanique de nouvelles missions à accomplir, mais résulte aussi du fait que leur mise en œuvre implique une concertation accrue avec de nombreux autres régulateurs.

Par exemple, pour le RIA, la CNIL aura des compétences partagées avec la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) ; pour le DGA, la CNIL interagit avec l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep).

Ces exemples illustrent le fait que si, auparavant, en tant que régulateur, nous jouissions d'une sorte de « monopole » dans notre champ de compétence, l'intrication des différents règlements européens visant à réguler le numérique nous conduit à renforcer significativement l'interrégulation. Celle-ci doit permettre une régulation globale des usages numériques et des acteurs, mais implique des procédures robustes, qui souvent restent à construire, ainsi que des moyens à la hauteur des ambitions fixées.

« L'intrication des différents règlements européens visant à réguler le numérique nous conduit désormais dans une nouvelle ère, celle de l'interrégulation. »

Marie-Laure Denis
présidente de la CNIL

Quels sont les éléments notables concernant la coopération européenne et internationale en matière de protection des données en 2025 ? Quels sont les grands rendez-vous à venir ?
–

Sur le plan européen, l'année passée a principalement été marquée par la déclaration dite d'Helsinki. En juillet 2025, l'ensemble des présidents des autorités de protection des données en Europe se sont réunis et ont pris d'importants engagements, retranscrits dans une déclaration formellement endossée par le Comité européen de la protection des données (CEPD). Cette démarche résulte d'une prise de conscience de la nécessité de faciliter la conformité au RGPD, en particulier pour les petites et moyennes organisations.

Elle se traduit en pratique par un plan d'action dans le cadre duquel les autorités, à travers le CEPD, s'engagent notamment à adopter des positions plus opérationnelles pour simplifier l'application du RGPD, mais aussi à renforcer la cohérence des interprétations. Enfin, des mesures doivent permettre de favoriser une coopération structurée avec les régulateurs d'autres domaines que celui de la protection des données.

Au niveau international, la CNIL et une vingtaine d'autorités de protection des données issues de différents pays ont signé une déclaration commune appelant à construire un cadre de gouvernance fiable pour une IA de confiance. Cette initiative, portée lors de la 47e édition de l'Assemblée mondiale de la protection de la vie privée (*Global Privacy Assembly*) à Séoul, marque un engagement mondial étendu en faveur d'une IA innovante et respectueuse de la vie privée.

Le sujet de l'IA figurera également à l'ordre du jour de la prochaine réunion des autorités de protection des données des pays du G7 que la CNIL organisera en juin 2026 à Paris, en marge du G7 des États présidé par la France.

Chiffres clés

Accompagner & conseiller

20
auditions parlementaires

133
délibérations
dont 90 avis sur projets de texte

1 351
demandes de conseil traitées

Contrôler & sanctionner

323
contrôles

83
sanctions *dont*
486 839 500 €
d'amendes

31
rappels aux obligations légales de la présidente

143
mises en demeure

Anticiper & innover

600
participants à l'événement *air2025*

900
participants au *Privacy Research Day*

26
articles et dossiers publiés sur le site linc.cnil.fr

Informer & protéger

35 403
appels répondus

266
actions de sensibilisation sur le terrain

20 150
plaintes reçues

18 123
plaintes traitées

6 999
demandes d'exercice des droits indirect (EDI) reçues

32 262
demandes d'EDI traitées
dont 80 % demandes FICOBA de 2024

10,5
millions de visites sur les sites web de la CNIL

6 167
notifications de violation de données personnelles

Les temps forts 2025

Janvier

23 janvier
En amont du Sommet pour l'action sur l'intelligence artificielle de février 2025, la CNIL, l'Université Paris-Saclay et l'Université de Caen Normandie organisent un événement intitulé « Protéger la voix et l'image des personnes à l'heure de l'IA ».

30 janvier
Publication par le Laboratoire d'innovation numérique de la CNIL (LINC) de l'Observatoire du droit d'accès sur les réseaux sociaux qui évalue les pratiques de dix plateformes.

Février

6-11 février
La CNIL participe à plusieurs événements et tables rondes dans le cadre du Sommet pour l'action sur l'IA organisé à Paris. Objectif : promouvoir une IA respectueuse des droits fondamentaux tout en permettant le développement de l'innovation européenne.

Mars

12-15 mars
Participation au Salon des seniors à Paris-Porte de Versailles.

Avril

1-3 avril
Participation au Forum INCYBER à Lille, l'un des plus grands événements européens sur les questions de sécurité numérique.

4-5 avril
Participation au Festival Hauts-de-Seine Digital Games, à la fois rendez-vous des amateurs de jeu vidéo et événement de sensibilisation des jeunes et de leurs familles.

24 avril
- Journée RGPD à Caen
- Lancement d'une consultation publique sur un projet de recommandation concernant le recueil du consentement multi-terminaux.

Mai

14 mai
Journée RGPD à Lille

20 mai
Organisation avec la Direction générale du Trésor d'un événement académique international pour évaluer l'impact économique du RGPD.

21 mai
Attribution des huitièmes « Trophées des classes », un concours ouvert aux classes de CM1 à la 3e pour sensibiliser les élèves à leurs droits numériques et à la citoyenneté en ligne.

Juin

12 juin
La CNIL publie *L'Agence Privacy*, pour sensibiliser les adolescents aux risques numériques — piratage, cyberharcèlement, usurpation d'identité — à travers un format inspiré des codes du manga.

17-20 juin
Réunion à Ottawa des autorités de protection des données des pays du G7 sous la présidence du Commissariat à la protection de la vie privée du Canada.

Juillet-Août

1er juillet
Quatrième édition de la « Journée de recherche sur la vie privée » (*Privacy Research Day*).

3 juillet
Réuni à Helsinki, le Comité européen de la protection des données (CEPD) adopte une importante déclaration visant à renforcer la clarté du RGPD, le dialogue avec les entreprises et la coopération entre autorités.

17 juillet
Le Conseil national des barreaux, qui représente les 76 000 avocats de France, et la CNIL renouvellent leur partenariat.

22 juillet
Publication des premières recommandations sur l'application du RGPD au développement des systèmes d'IA. Objectif : aider les professionnels à concilier innovation et respect des droits des personnes.

Septembre

1er septembre
Prononcé de deux amendes à l'encontre de Google (325 millions d'euros) et Shein (150 millions d'euros) pour non-respect de la législation sur les cookies.

30 septembre
Première édition ouverte au public des Rencontres Informatique & Libertés, événement organisé par la CNIL et visant à favoriser le dialogue avec les différents acteurs du droit.

Octobre

15 octobre
Organisation avec la Bibliothèque nationale de France de la journée de réflexion air2025 (Avenir, Innovations, Révolutions) sur le thème : « Intimité des disparus, mémoire des vivants : quelle éthique pour les traces numériques ? ».

Novembre

18-20 novembre
Participation au Salon des maires et des collectivités locales, afin de présenter notamment la nouvelle réglementation européenne concernant la prospection politique.

19 novembre
Lancement d'une consultation publique sur des projets de fiches et de référentiels destinés au secteur du logement social.

Décembre

9 décembre
Journée RGPD à Nantes

11-18 décembre
Large diffusion par les chaînes du groupe France Télévisions du clip « Réfléchissez avant de publier » réalisé avec l'autorité de protection des données irlandaise afin de sensibiliser les parents aux risques liés à la diffusion des images de leurs enfants sur les réseaux sociaux.

15 décembre
Participation à la deuxième réunion plénière du Réseau national de coordination de la régulation des services numériques (REN).

16 décembre
Lancement de l'application FantomApp pour aider les adolescents à se protéger en ligne et à trouver facilement de l'aide en cas de problème dans leurs usages numériques.

L'éclairage
du secrétaire général et du secrétaire général adjoint

Mieux prioriser pour répondre aux nouveaux défis

La CNIL fait face à deux tendances convergentes qui accroissent fortement son activité.

Tout d'abord elle est davantage sollicitée au titre de ses missions traditionnelles. En effet, le RGPD est désormais mieux connu des particuliers, qui n'hésitent plus à le mobiliser pour faire valoir leurs droits ; cette tendance se reflète notamment dans l'augmentation continue du nombre de plaintes enregistrées chaque année, qui conduit aussi, par ricochet, à une intensification de l'activité répressive. La CNIL constate également une attente croissante des responsables de traitement, qui cherchent à obtenir des éclairages – au travers d'outils de droit souple ou de réponses individuelles – pour les aider à résoudre les difficultés concrètes auxquelles ils sont confrontés dans l'application du droit de la protection des données. Ensuite, plusieurs textes, nationaux comme européens, ont confié des attributions supplémentaires à la CNIL (*DSA*, *DGA*, loi SREN, RIA, RPP…), ce qui implique à chaque fois le développement d'expertises nouvelles, ainsi qu'une adaptation des outils et des procédures.

Cette double tendance de fond – et alors que le contexte budgétaire ne permet pas une augmentation des effectifs en proportion – oblige la CNIL à mieux prioriser son activité. Amorcée à l'automne 2025, cette démarche de fond a nécessité d'impliquer l'ensemble des agents, et donc tous les métiers, pour connaître les points d'amélioration et identifier les irritants. Elle a déjà permis de dégager des mesures concrètes, dont la mise en œuvre devrait permettre à l'institution de mieux satisfaire aux attentes, toujours plus nombreuses, placées en elle. Ce travail itératif se poursuit en 2026.

> *« Le RGPD est désormais mieux connu des particuliers, qui n'hésitent plus à le mobiliser pour faire valoir leurs droits. »*

Mathias Moulin
secrétaire général adjoint

Intégrer deux règlements européens structurants

Parmi les textes récents qui modifient les attributions de la CNIL, deux sont destinés à avoir un impact particulièrement fort sur l'institution.

Le premier est le règlement sur l'intelligence artificielle. Le schéma national de gouvernance, en cours d'examen au Parlement, confie en effet des prérogatives étendues à la CNIL en la matière, et ce sur un grand nombre de domaines (champ régalien, éducation, travail, processus démocratiques). Ces prérogatives vont exiger de l'institution qu'elle s'approprie des rôles nouveaux – et notamment celui d'autorité de surveillance de marché (ASM). C'est pour anticiper ces responsabilités supplémentaires que la CNIL a mis en place, en 2025, un groupe de travail interne – qui se nourrit de l'expérience des ASM existantes et travaille avec les autres régulateurs pressentis – et qu'elle a exploré en détail la question de l'articulation entre IA et RGPD, avec l'ambition de formaliser une doctrine cohérente et prévisible pour les développeurs et les déployeurs.

Le second texte est le règlement du 26 novembre 2025 établissant des règles de procédure supplémentaires relatives à l'application du RGPD. Ce texte, bien que plus technique, renouvelle considérablement le cadre procédural applicable aux plaintes transfrontalières, notamment s'agissant de la place reconnue aux plaignants et des mécanismes de coopération entre autorités nationales. Là encore, sa bonne mise en œuvre à compter d'avril 2027 nécessite, d'ores et déjà, de conduire un lourd travail de fond pour ajuster nos textes et nos procédures, en collaboration avec nos homologues européens.

Travailler en réseau avec les autres autorités

Si la CNIL est la seule autorité nationale responsable pour le RGPD, elle n'est que l'une des autorités compétentes au titre des autres textes dont elle est chargée de la mise en œuvre. Cette situation implique pour la CNIL d'enrichir ses méthodes de travail, pour approfondir ses échanges avec les autres régulateurs (ARCOM, ARCEP, DGCCRF…). Cette logique en réseau exige en effet un dialogue constant, formel comme informel, pour bien articuler les compétences respectives de chacun et pour assurer la cohérence des positions prises – ce qui constitue une légitime attente des régulés. Par capillarité, même dans le champ RGPD, la CNIL s'efforce plus que jamais de croiser les regards avec les autres régulateurs pour enrichir ses analyses : c'est en ce sens, par exemple, qu'en mars 2025, la CNIL et l'Autorité de la concurrence ont échangé lors d'un séminaire sur les liens entre protection des données et concurrence s'agissant du développement de l'IA générative – dans le prolongement du travail déjà accompli en commun à propos des applications mobiles.

Innover pour mieux faire connaître le droit à la protection des données

En 2025, en plus de ses vecteurs classiques, la CNIL a multiplié les initiatives créatives pour porter ses sujets auprès de tous les publics, en mobilisant des équipes pluridisciplinaires et en adaptant ses moyens à des formats nouveaux. Trois exemples en témoignent tout particulièrement.

À l'été, la production du manga *L'Agence Privacy* a mobilisé plusieurs services en interne, combinant expertise juridique, pédagogique et communication, ainsi que des équipes de conception graphique et de rédaction. Ce projet, destiné aux adolescents, a nécessité une coordination étroite entre les différentes compétences de la CNIL pour traduire des concepts techniques en contenus accessibles et attractifs. Le deuxième tome est prévu pour 2026, ce qui implique déjà une planification et des ressources dédiées pour sa production.

En décembre dernier, le lancement de l'application mobile FantomApp a également engagé des moyens internes importants, tant sur le plan technique que pédagogique. Celle-ci vise là encore les adolescents, pour les aider à se protéger sur les réseaux sociaux (outils, tutos, conseils en cas de problèmes). Novatrice dans son format, cette initiative l'est aussi dans les modalités qui ont présidé à sa conception puisqu'elle a été pensée à la suite de nombreux échanges avec des collégiens, en réponse directe aux besoins qu'ils avaient exprimés.

Enfin, dans le cadre de son partenariat avec Radio France, la CNIL collabore avec les antennes ICI (ex France Bleu), ce qui conduit à ce que deux chroniques soient dédiées chaque week-end aux thématiques relatives à la protection des données personnelles. Ces émissions, qui s'adressent à un public large et non-spécialiste, illustrent la manière dont la protection de la vie privée fait aussi écho à des problématiques du quotidien et permettent ainsi d'accroître la conscience collective autour de ces enjeux.

> *« En 2025, en plus de ses vecteurs classiques, la CNIL a multiplié les initiatives créatives pour porter ses sujets auprès de tous les publics. »*

Vincent Villette
secrétaire général

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.

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 séances plénières

Les 18 membres de la CNIL se réunissent en séance plénière une fois par semaine sur un ordre du jour établi à l'initiative de la présidente.

Une partie importante de ces séances est consacrée à l'examen de projets de loi et de décrets soumis à la CNIL pour avis par le gouvernement. Le Collège est également en charge de l'analyse des actes de droit souple tels que les lignes directrices, les référentiels ou les recommandations.

Lors d'une séance, un rapporteur présente son rapport ainsi que le projet de délibération aux membres du Collège.

Ces derniers sont ensuite invités par la présidente à prendre la parole pour une discussion générale. À tout moment, pour éclairer les débats, la présidente peut donner la parole au secrétaire général ou à un autre agent de la CNIL en charge du dossier. En cas de besoin, le vice-président délégué exerce les attributions de la présidente.

La formation restreinte

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

Les membres de la CNIL

Le bureau

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

Sophie LAMBREMON
Conseillère 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

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 Inria Grenoble
Secteur : Intelligence artificielle

Christophe CHAILLOU
Sénateur du Loiret
Secteur : Intérieur

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

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

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

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

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

Les membres élus de la formation restreinte

Philippe-Pierre CABOURDIN
(président de la formation restreinte)

Vincent LESCLOUS

Laurence FRANCESCHINI

Isabelle LATOURNARIE-WILLEMS

Bertrand DU MARAIS

Didier KLING

Commissaire du gouvernement

Damien MILIC

Céline BOYER
Adjointe

Organigramme des directions et services

Marie-Laure DENIS
Présidente

Vincent VILLETTE
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**
- **Service de la gestion de la connaissance**

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

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 proactif pour un numérique de confiance

COMMENT LA CNIL ACCOMPAGNE LES PARTIS POLITIQUES, LES CANDIDATS, ET LEURS SOUS-TRAITANTS 21

DES OUTILS AU SERVICE DES PROFESSIONNELS 23

APPLICATIONS MOBILES : LA CNIL ENRICHIT SES RECOMMANDATIONS 25

SILVER ÉCONOMIE : 6 PROJETS INNOVANTS SONT ACCOMPAGNÉS 25

VIDÉOPROTECTION ET CAMÉRAS AUGMENTÉES : ZOOM SUR CE QUI EST AUTORISÉ 25

7 CONSULTATIONS LANCÉES EN 2025 26

AFFICHAGE DES LISTES DE CLASSES : LES BONNES PRATIQUES POUR PROTÉGER LES ÉLÈVES 27

LA CNIL INTERROGE LES FRANÇAIS SUR LES ABONNEMENTS PAYANTS 27

LES ÉVÉNEMENTS DÉDIÉS AUX PROFESSIONNELS 28

Entretien avec

Laurence Franceschini,

membre du Collège de la CNIL en charge de la vie politique et citoyenne.

« L'usage de données personnelles pour la communication politique doit être licite, loyal et transparent »

Quels sont les enjeux liés à l'usage croissant des outils numériques dans la communication politique ?

–

Pour leurs opérations de communication politique, la CNIL a observé que les candidats et les partis ont de plus en plus recours à des traitements de données personnelles (par téléphone, courriel, SMS, etc.). Cela induit évidemment des risques au regard de la protection des données personnelles, en particulier avec l'essor des techniques de ciblage politique reposant sur des logiciels et outils numériques.

Les risques identifiés concernent principalement le respect des droits des personnes : difficultés à exercer les droits à l'effacement ou d'opposition, mais aussi le défaut d'information sur leurs données.

Comment assurer le respect des droits des électeurs ?

–

Avec son observatoire des élections, la CNIL sensibilise les électeurs et les partis politiques aux règles applicables. Ainsi, l'usage de données personnelles pour la communication politique doit être licite, loyal et transparent, que la collecte auprès des personnes soit directe ou indirecte. Les finalités des traitements doivent être clairement définies et respectées, les données sécurisées et les droits des personnes garantis.

Avec l'entrée en application, depuis le 10 octobre 2025, du règlement européen sur le ciblage politique, la CNIL a conduit un plan d'action pour clarifier les règles applicables aux partis politiques, candidats et sous-traitants et les accompagner dans leur mise en conformité, notamment en publiant de nouvelles fiches pratiques sur son site web. Par ailleurs, elle met à disposition des électeurs une fiche pratique rappelant leurs droits, ainsi qu'un formulaire permettant de signaler des pratiques jugées irrégulières lors des campagnes.

Comment la CNIL accompagne les partis politiques, les candidats, et leurs sous-traitants

–

Pour préparer les élections municipales dans le contexte d'une nouvelle réglementation européenne, la CNIL a déployé de nouveaux outils pour accompagner les différentes parties prenantes. Elle a aussi réactivé son observatoire des élections.

6 fiches pratiques pour accompagner l'ensemble des acteurs

Les élections municipales ont été marquées par de nouvelles règles concernant la prospection politique, imposant **plus de transparence et de respect des données personnelles.** Elles résultent d'un nouveau règlement européen qui s'applique depuis le 10 octobre 2025. Ce texte complète le RGPD afin d'encadrer l'usage croissant des outils numériques dans la sphère politique.

Parmi les nouvelles obligations :

- les données utilisées pour du ciblage et pour diffuser des publicités à caractère politique en ligne doivent être collectées par le responsable de traitement directement auprès des personnes concernées ;
- la seule base légale admise est le consentement de la personne concernée ;
- le profilage utilisant des données sensibles est interdit ;
- le ciblage des mineurs de moins de 17 ans est interdit.

Pour faciliter la mise en conformité, la CNIL a initié un cycle de consultations avec les partis politiques et les autres autorités concernées, dont l'ARCOM, également chargée d'appliquer certaines dispositions du texte. À l'issue de ces échanges, elle a publié six nouvelles fiches pratiques portant sur :

- les outils de communication politique ;
- les fichiers de communication politique ;
- l'utilisation de listes d'électeurs pour la communication politique ;
- les fichiers qui ne peuvent pas être utilisés pour la communication politique ;
- les fichiers du secteur privé ;
- la responsabilité des acteurs politiques.

En complément, un tableau récapitulatif présente les mentions que doivent rendre publiques les responsables de traitement et les éditeurs selon le type de publicité politique.

Des échanges au Salon des maires et des collectivités locales

La CNIL est venue à la rencontre des élus locaux et des agents territoriaux à l'occasion du Salon des maires et des collectivités locales, qui s'est déroulé du 18 au 20 novembre 2025 à Paris. Pendant toute la durée de l'événement, elle a répondu aux questions et présenté ses fiches pratiques. Elle a aussi organisé avec l'ARCOM une conférence dédiée au nouveau règlement européen et intitulée : « Municipales 2026 : quelles règles applicables en matière de prospection politique ? ».

Le plan d'action pour les municipales

À l'approche des élections municipales, la CNIL a réactivé son observatoire des élections, créé en 2012. Ses missions : surveiller les pratiques de communication politique, dialoguer avec les partis et candidats et informer les électeurs sur leurs droits.

La CNIL a notamment envoyé aux partis politiques et aux principaux sous-traitants une série de courriers pour leur rappeler les nouvelles règles et les bonnes pratiques à adopter. Elle a aussi mené des actions de sensibilisation des élus locaux avec l'Association des maires de France (AMF) et la revue *Maires de France*.

Pour les électeurs, une fiche pratique rappelant leurs droits et un formulaire de signalement des pratiques jugées interdites ont été mis en ligne.

Préparation d'une nouvelle recommandation sur le vote par correspondance électronique

Toujours en 2025, la CNIL a entamé la mise à jour de sa recommandation sur le vote par correspondance électronique, dont la dernière version remonte à 2019. Elle a ainsi mené une large consultation publique autour d'un nouveau texte. Parmi les modifications envisagées :

- un ajustement des critères servant à évaluer le niveau de risque que présente un scrutin ;
- l'intégration d'un questionnaire d'auto-évaluation pour aider les acteurs à évaluer ce niveau de risque ;
- l'ajout de nouveaux objectifs de sécurité comme l'obligation de publication du code source du scrutin en amont du vote, etc.

La nouvelle recommandation sera publiée en 2026.

Les outils de la CNIL pour les partis politiques et les candidats

5

candidats aux élections européennes et législatives 2024 ont été sanctionnés par la CNIL en 2025.

En cause : l'envoi de messages de prospection politique à des électeurs sans respecter les règles encadrant la protection des données personnelles. Le montant cumulé des amendes s'élève à 23 500 euros.

3 948

signalements ont été reçus par la CNIL à l'occasion des élections municipales de 2020. La grande majorité portait sur les SMS (45 %) et appels téléphoniques (36 %), le reste sur les courriers électroniques, les courriers et les réseaux sociaux.

Des outils au service des professionnels

Une recommandation pour les enquêtes de mesure de la diversité au travail

Dans un contexte de sensibilisation accrue à la lutte contre les discriminations, de plus en plus d'organismes souhaitent mesurer la diversité au sein de leurs effectifs. La CNIL a publié en juin 2025 une recommandation pour les aider à mettre en œuvre ces enquêtes dans le respect du RGPD. Très concret, ce document fournit notamment des exemples de questions autorisées et interdites.

Consulter la recommandation

Un rappel des vérifications nécessaires en cas de réutilisation de bases de données

Que ce soit pour de la recherche scientifique, le développement de systèmes d'IA ou encore de la prospection commerciale, des organismes réutilisent des bases de données personnelles, soit librement mises à disposition sur Internet, soit fournies par un tiers comme un courtier en données. La CNIL a rappelé en janvier 2025 les vérifications à réaliser, alertant sur les points de vigilance.

Les vérifications à réaliser

Un outil pour aider au déploiement des cookies mesurant l'audience

La CNIL a précisé en juillet 2025 les conditions qui permettent d'exempter de consentement les cookies (traceurs) utilisés pour mesurer l'audience d'un site ou d'une application. Afin d'aider les fournisseurs de solutions techniques à identifier si leur solution peut ou non entrer dans le champ de l'exemption, la CNIL a mis à leur disposition un outil d'auto-évaluation.

L'outil d'auto-évaluation

Un guide pour l'analyse d'impact des transferts de données

La CNIL a publié en janvier 2025 la version finale de son guide sur les analyses d'impact des transferts de données (AITD) dont l'objectif est d'accompagner les organismes qui transfèrent des données en dehors de l'Espace économique européen. Cet outil leur permet d'évaluer les garanties supplémentaires à mettre en place par rapport au niveau de protection du pays de destination des données.

Le guide pratique

Les clés pour bien identifier son rôle en tant que responsable du traitement ou sous-traitant

Responsable de traitement ? Seul ou conjointement avec d'autres organismes ? Sous-traitant ? La CNIL a rappelé en juin 2025 les critères permettant d'identifier le rôle de chaque acteur. Cette qualification ne dépend pas d'un choix contractuel mais des faits : qui décide de quoi ? qui exécute quoi ? etc. Il en résulte des obligations et des responsabilités spécifiques.

Les critères et les conséquences pratiques

Quels bénéfices économiques du DPO en entreprise ?

La CNIL a publié en juillet 2025 une étude sur les bénéfices économiques liés à la présence d'un délégué à la protection des données (DPO) au sein des entreprises. L'analyse montre qu'elle est souvent profitable, en particulier pour les entreprises adoptant une approche positive de la conformité RGPD.

L'étude en détail

Nouveaux webinaires pour les professionnels

Sept nouveaux webinaires thématiques, sur le dossier patient informatisé, les transferts de données hors UE ou encore les fiches IA, ont été organisés en 2025 pour aider les professionnels à se mettre en conformité avec la réglementation. **2 400 personnes y ont participé, dont 60 % du secteur privé.**

Les webinaires de la CNIL

Le MOOC de la CNIL s'élargit aux données RH

L'Atelier RGPD – le MOOC de la CNIL – reçoit environ **13 000 connexions par mois.** Depuis le mois de mai 2025, il propose un nouveau module intitulé « Travail et données personnelles ». Interactif et basé sur des cas concrets, il couvre toutes les étapes de la vie professionnelle, du recrutement à la gestion courante des données, jusqu'au départ du salarié.

Le nouveau module de l'Atelier RGPD

Un parcours de déclaration simplifié pour les traitements de données de santé

Un traitement de données de santé ayant une finalité d'intérêt public comme une recherche, étude ou évaluation en santé ou une base de données en santé (par ex. : entrepôts) nécessite une déclaration de conformité à un référentiel ou, à défaut d'une conformité totale, une demande d'autorisation. En 2025, afin d'aider les professionnels à effectuer leurs demandes d'autorisation et répondre à leurs différents besoins en la matière, la CNIL a mis en place un nouveau téléservice, plus moderne, qui accompagne le dépôt du projet pas à pas.

539
dossiers ont été traités en santé (demandes d'autorisation)

dont

406
dossiers en recherche en santé

Entretien avec

Philippe Latombe,

membre du Collège de la CNIL en charge du secteur social

« Protéger la vie privée tout en accompagnant les transformations numériques »

La CNIL propose un accompagnement renforcé pour les acteurs de la *silver* économie. Quels sont les enjeux spécifiques, en termes de protection des données, de ce secteur ?

–

Les nouvelles technologies telles que l'IA avec les caméras algorithmiques, mais aussi les dispositifs connectés comme les gyroscopes sont devenues concrètes et accessibles. Elles peuvent permettre d'accompagner plus spécifiquement les personnes âgées, dépendantes ou non, en assurant notamment une surveillance médicale et une prévention accrue. Pour cela, de nombreuses données sont nécessaires ; il est donc important de s'assurer que les traitements sont mis en œuvre dans le respect des droits et libertés, aussi parce qu'ils comportent souvent des données de santé. Un accompagnement de la CNIL dès le début de l'utilisation de ces nouvelles technologies est un bon moyen de concilier efficacité et préservation de la vie privée de nos aînés.

Pourquoi avoir lancé une consultation sur de nouveaux référentiels et fiches destinés au secteur du logement social ?

–

La rareté des disponibilités en logement social, couplée à une plus grande demande de la population, rend le sujet de la décision d'attribution par les OPH* hyper sensible. De fait, les demandes de pièces justificatives, et donc de données personnelles, revêtent un caractère stratégique dans le processus. L'utilisation des nouvelles technologies numériques pour traiter ces données est essentielle mais présente des risques de biais et de discriminations. Les processus administratifs ayant changé, il était nécessaire que soient établis de nouveaux référentiels en la matière pour plus de transparence et de sécurité pour nos concitoyens. La CNIL se devait donc de lancer une telle consultation pour recueillir les avis des professionnels du secteur et leurs suggestions ou remarques opérationnelles. Il s'agit d'une bonne méthode pour coller aux réalités du terrain tout en ayant une vue globale synthétique et pratique.

* Offices publics d'habitat

Applications mobiles : la CNIL enrichit ses recommandations

La CNIL poursuit son accompagnement des professionnels pour le déploiement d'applications mobiles, détaillant notamment le rôle clé des permissions d'accès. En avril, elle a mis à jour, avec quelques clarifications, ses recommandations adoptées en 2024 pour mieux protéger la vie privée des utilisateurs. Une version anglaise a également été publiée.

La CNIL s'est aussi intéressée à deux situations de la vie courante :

- en juillet, elle a rappelé aux banques les règles à respecter lorsqu'elles veulent s'assurer que leurs clients ne sont pas sous l'influence d'un fraudeur au moment où ils réalisent une opération bancaire ;
- en novembre, elle a publié des conseils pour aider celles et ceux qui utilisent une application de rencontres à protéger leur intimité et à garder le contrôle sur leurs données.

Enfin, comme elle l'avait annoncée en 2024, la CNIL a fait du contrôle de la collecte de données par les applications mobiles un de ses thèmes prioritaires de contrôles (lire page 33).

Comment protéger son intimité sur les applications de rencontres ?

Silver économie : 6 projets innovants sont accompagnés

La CNIL a sélectionné trois projets de la *silver* économie (économie des seniors), O_2, OSO-AI et Neural Vision, pour participer à son nouveau « bac à sable ». O_2 vise à sécuriser les flux de données entre partenaires sociaux, médicaux-sociaux et administratifs ainsi que le repérage des fragilités chez certains des seniors accompagnés. OSO-AI développe une solution basée sur l'IA pour détecter des sons critiques et alerter les soignants. Neural Vision (MISSIA) développe une application mobile permettant à la famille de suivre au quotidien son parent et d'être alertée en cas de situations dangereuses ou inhabituelles. Ils bénéficient d'un accompagnement personnalisé sur plusieurs mois.

Trois autres projets présentant un intérêt pour la protection des données, Cdiet, Diwall et Sonaid, sont aussi conseillés. Les enseignements tirés de ces accompagnements seront publiés pour en faire bénéficier l'ensemble des innovateurs de la filière. Engagée auprès de ce secteur, la CNIL était par ailleurs présente au Salon des seniors en mars à Paris et au Festival SilverEco en octobre à Cannes.

Vidéoprotection et caméras augmentées : zoom sur ce qui est autorisé

Dans la rue, au volant, dans les magasins, dans les transports en commun, à l'école... difficile d'échapper aujourd'hui aux caméras de vidéoprotection. La CNIL explore attentivement les différents usages de ces caméras, en précisant à chaque fois le cadre légal et en fournissant des recommandations. Elle s'est intéressée en 2025 à cinq thèmes clés : les caméras individuelles (ou caméras-piétons) portées par des agents pour enregistrer certaines interventions, les drones équipés de caméras pour la sécurité publique, les caméras embarquées par certains services de sécurité publique, les dispositifs vidéo dans les établissements scolaires et les dispositifs de lecture de plaques d'immatriculation (LAPI).

La CNIL est aussi attentive au déploiement de caméras « augmentées » qui associent vidéo et IA pour une analyse en temps réel des images par des algorithmes. Elle a ainsi rappelé en mai 2025 les règles à respecter pour l'installation de caméras augmentées au niveau des caisses automatiques dans certaines enseignes.

Parallèlement, la CNIL a pris position sur les dispositifs vidéo de vérification de l'âge des clients utilisés par des buralistes pour éviter de vendre aux mineurs des produits interdits (tabac, alcool, jeux d'argent, etc.). Après analyse, ce type de dispositif n'apparaît ni nécessaire ni proportionné. Les buralistes restent soumis à leur obligation de demander à leurs clients une preuve de majorité.

Caméras et autres dispositifs vidéo : les règles à respecter

7 consultations lancées en 2025

Pour élaborer des recommandations au plus près des pratiques, la CNIL suscite les contributions des différentes parties prenantes au travers de consultations et de concertations publiques. Voici sept exemples.

Mars - Les données de localisation des véhicules connectés

Dans le cadre de son club conformité dédié aux acteurs du véhicule connecté et de la mobilité, la CNIL a établi un projet de recommandation pour accompagner et encadrer les usages des données de localisation. Il a été soumis à consultation publique du 25 mars au 20 mai. Parallèlement, le club conformité a commencé à travailler sur une nouvelle thématique : les caméras embarquées.

Les **clubs conformité** de la CNIL sont des groupes d'échanges réunissant des professionnels (DPO, juristes, responsables conformité, etc.) autour des enjeux de protection des données.

Leur objectif est de :

- partager des bonnes pratiques ;
- échanger sur des cas concrets et des difficultés rencontrées ;
- bénéficier d'éclairages de la CNIL sur la réglementation (RGPD) ;
- favoriser une mise en conformité plus opérationnelle.

Mars - Conformité et sécurité des dossiers médicaux

À la suite de plusieurs contrôles dans des établissements de santé et des constats faits à cette occasion, la CNIL a élaboré un projet de recommandation pour la conformité et la sécurité du dossier patient informatisé (DPI). Ce dossier contient de nombreuses données sensibles et doit bénéficier de mesures de sécurité renforcées. La consultation publique s'est déroulée du 20 mars au 16 juin.

Mai - L'évaluation de la solvabilité pour un octroi de crédit

Renforcer la transparence et la conformité des traitements de données liés à l'évaluation de la capacité de remboursement des demandeurs de crédit. C'est l'objectif du projet de référentiel soumis à consultation entre le 23 mai et le 18 juillet. Il propose des recommandations concrètes sur les opérations les plus courantes : consultation du Fichier des incidents de remboursement, utilisation d'outils de notation (*scoring*), collecte de données…

Avril - Les outils d'enregistrement et de relecture de session de navigation

Ces outils, également appelés outils de rejeu de session, servent à reconstituer le parcours complet de navigation sur un site web ou une application mobile. Ils enregistrent les mouvements de souris, les interactions tactiles, les clics, le défilement des pages, etc. Pour mieux appréhender les enjeux associés à ces outils, la CNIL a lancé une concertation avec les acteurs concernés et des associations de la société civile.

Avril - Recueil du consentement multi-terminaux

Les utilisateurs interagissent désormais avec des sites web ou des applications mobiles via plusieurs appareils : ordinateur, téléphone, tablette, télévision connectée… Dans ce contexte, certains acteurs du numérique cherchent à obtenir un consentement unique, valable sur tous les terminaux d'un même utilisateur. La CNIL a établi un projet de recommandation permettant de recueillir un consentement multi-terminaux (aussi appelé *cross-device*) conforme aux exigences du RGPD. Il a été soumis à consultation publique du 24 avril au 5 juin et la recommandation a été publiée en janvier 2026.

La recommandation finale

Juin - L'utilisation des pixels de suivi dans les courriels

Les pixels de suivi sont une méthode de traçage alternative aux cookies. Ils prennent la forme d'une image de 1 pixel par 1 pixel, invisible pour l'utilisateur mais contenant un identifiant qui permet de savoir s'il a visité une page ou lu un courriel. Cette pratique répandue a suscité auprès de la CNIL un certain nombre de plaintes. Après des échanges avec des professionnels et des associations de la société civile, la CNIL a élaboré un projet de recommandation concernant notamment l'information et le consentement des destinataires. Il a été soumis à consultation publique entre le 12 juin et le 24 juillet.

Novembre - Logement social et RGPD

Pour guider les organismes dans la mise en conformité de leurs traitements, la CNIL a lancé une consultation publique sur des projets de fiches et de référentiels destinés aux acteurs du logement social : offices publics de l'habitat, sociétés d'HLM, sociétés d'économie mixte immobilières, services de l'État, collectivités territoriales... Ont été soumis à consultation dix fiches reprenant les principes « Informatique et Libertés », trois fiches thématiques (vidéosurveillance et accès aux immeubles, enquêtes menées par les bailleurs sociaux, objets connectés) et trois référentiels dédiés aux traitements les plus courants (demandes de logement social, de relogement et de mutation, gestion locative, accession sociale à la propriété).

Affichage des listes de classes : les bonnes pratiques pour protéger les élèves

La publication des listes scolaires est une pratique usuelle. L'affichage de la composition des classes n'est pourtant pas sans risque. Dévoiler la localisation d'un élève peut l'exposer à des situations sensibles en cas de déchéance de l'autorité d'un des parents ou dans un contexte de harcèlement. La CNIL a publié en avril 2025 un rappel des règles et une synthèse des bonnes pratiques. Comme limiter les noms des élèves à leur seul prénom, éventuellement avec l'initiale du nom de famille.

Les conseils pour la publication des listes scolaires

La CNIL interroge les Français sur les abonnements payants

Les Français sont-ils prêts à payer pour des services en ligne sans publicité ciblée ? Selon les secteurs, entre 25 % et 48 % des internautes interrogés ont répondu positivement, dans le cadre d'une enquête commandée par la CNIL et réalisée par l'institut Harris Interactive. *« Il existe donc un vivier important de personnes intéressées par des offres payantes leur permettant de mieux protéger leurs données personnelles »*, souligne l'étude dévoilée en octobre 2025.

Tous les enseignements du sondage

Les événements dédiés aux professionnels

Les Rencontres Informatique et Libertés s'ouvrent au public

La CNIL a organisé, le 30 septembre 2025, la première édition ouverte au public de ses Rencontres Informatique et Libertés. Cet événement vise à favoriser le dialogue avec les différents acteurs du droit : juristes, avocats, étudiants, DPO, universitaires... Organisée au siège de la CNIL et diffusée en direct en ligne, la manifestation a fait salle comble. Deux thématiques ont été abordées :

- la vie privée au travail : comment allier performance, sécurité et respect des libertés individuelles au sein du monde du travail ?
- le RGPD et le règlement européen sur l'IA : comment concilier ces deux règlements et s'assurer que les systèmes d'IA respectent la vie privée des citoyens ?

Voir la rediffusion de l'événement

Enquête sur le métier de DPO à l'heure de l'IA

Depuis 2018, la Délégation générale à l'emploi et à la formation professionnelle du ministère du Travail et des Solidarités et la CNIL, en partenariat avec l'Association française des correspondants à la protection des données à caractère personnel, étudient l'évolution de la fonction de délégué à la protection des données (DPO). En 2025, cette enquête s'est concentrée sur les défis que pose l'intégration rapide de systèmes d'IA dans les pratiques professionnelles. Quel impact sur le champ d'action du DPO ? Sur quelles compétences peut-il capitaliser ? Avec quels besoins en termes d'outillage et de formation ? Les résultats, publiés au premier semestre 2026, permettront d'orienter les travaux de la CNIL pour aider les DPO à intégrer les nouveaux enjeux réglementaires.

Nouvelles journées RGPD

La CNIL poursuit ses déplacements en France pour échanger sur la mise en œuvre du RGPD. En 2025, ces journées se sont déroulées à **Caen**, en collaboration avec l'université de Caen-Normandie et l'Association française des correspondants à la protection des données à caractère personnel (AFCDP), à **Lille**, en collaboration avec le Centre de recherche de la Faculté de Droit (C3RD) de l'Université catholique de Lille, à **Paris**, en collaboration avec le Conservatoire national des arts et métiers (Cnam), et à **Nantes**, en collaboration avec Nantes Métropole.

Mise à jour des Tables Informatique et Libertés

Une nouvelle édition des Tables Informatique et Libertés a été publiée au printemps 2025. Destiné aux professionnels de la protection des données et aux universitaires, cet outil rassemble l'ensemble des prises de position doctrinales de la CNIL et de juridictions nationales et européennes. L'édition 2026 est d'ores et déjà disponible.

Les Tables Informatique & Libertés

109 249

organismes privés et publics ont au total désigné un délégué à la protection des données, en hausse de 5,5 % par rapport à 2024

39 174

délégués à la protection des données étaient en poste en 2025, plusieurs organismes pouvant désigner le même délégué.

Plaintes, contrôles, sanctions : des actions rigoureuses, efficaces et équilibrées

LA HAUSSE DES PLAINTES S'ACCÉLÈRE 30

LA PROCÉDURE DU GUICHET UNIQUE POUR LES PLAINTES TRANSFRONTALIÈRES 31

DES RAPPELS À LA RÉGLEMENTATION CONCERNANT LA TÉLÉSURVEILLANCE D'EXAMENS ET LA VIDÉOPROTECTION EXCESSIVE DANS LES COMMUNES 31

LE FICOBA NE DÉPEND PLUS DE L'EXERCICE DES DROITS INDIRECTS GÉRÉ PAR LA CNIL 32

LE LINC PUBLIE LE BILAN DE L'OBSERVATOIRE DU DROIT D'ACCÈS SUR LES RÉSEAUX SOCIAUX 32

4 THÉMATIQUES DE CONTRÔLE PRIORITAIRES 33

LES CONTRÔLES EN COOPÉRATION AU NIVEAU EUROPÉEN 34

COMMENT SE PASSE UN CONTRÔLE DE LA CNIL ? 34

UN NOMBRE D'AMENDES STABLE MAIS AVEC DES MONTANTS IMPORTANTS 35

DEUX SANCTIONS MARQUANTES EN 2025 37

L'ACTIVITÉ CONTENTIEUSE 37

Entretien avec

Delphine Legoherel,

directrice de l'exercice des droits et des plaintes

« Notre objectif : traiter plus de plaintes tout en garantissant un service public de qualité »

Pourquoi la direction de l'exercice des droits et des plaintes (DEDP) a-t-elle été créée en janvier 2025 ?

–

Elle a été créée suite à la réorganisation des directions de la CNIL pour renforcer l'équipe encadrante et permettre une gestion plus ciblée des flux. J'en ai été nommée directrice avec la mission d'organiser les services tout en continuant à assurer une gestion efficace du traitement des saisines, c'est-à-dire à la fois l'exercice des droits indirects et les plaintes.

La direction est composée d'une cinquantaine d'agents, dont le défi majeur est de faire face à l'augmentation des saisines. Elles ont atteint en 2025 de nouveaux records, ce qui implique de réfléchir aux méthodes de travail et à la granularité des actions menées pour assurer un service public de qualité et ainsi garantir efficacement la protection des droits fondamentaux.

L'équipe de la DEDP a relevé ce défi pour sa première année puisqu'elle a traité plus de plaintes en 2025 qu'en 2024.

Au-delà du traitement des plaintes, quelles sont les autres actions que vous menez avec des acteurs extérieurs ?

–

La DEDP mène des actions avec divers acteurs pour une protection toujours plus efficace des données personnelles comme des représentants d'organes de presse sur la nécessaire conciliation entre le droit à l'information et la protection des données personnelles ; le ministère de l'Économie et des Finances, de la Justice et l'INPI sur la diffusion des données personnelles pour la création d'une société et le parquet cybercriminalité en cas de dénonciations d'atteintes à la protection des données relevant de dispositions pénales.

20 150

plaintes reçues par la CNIL en 2025

La hausse des plaintes s'accélère

–

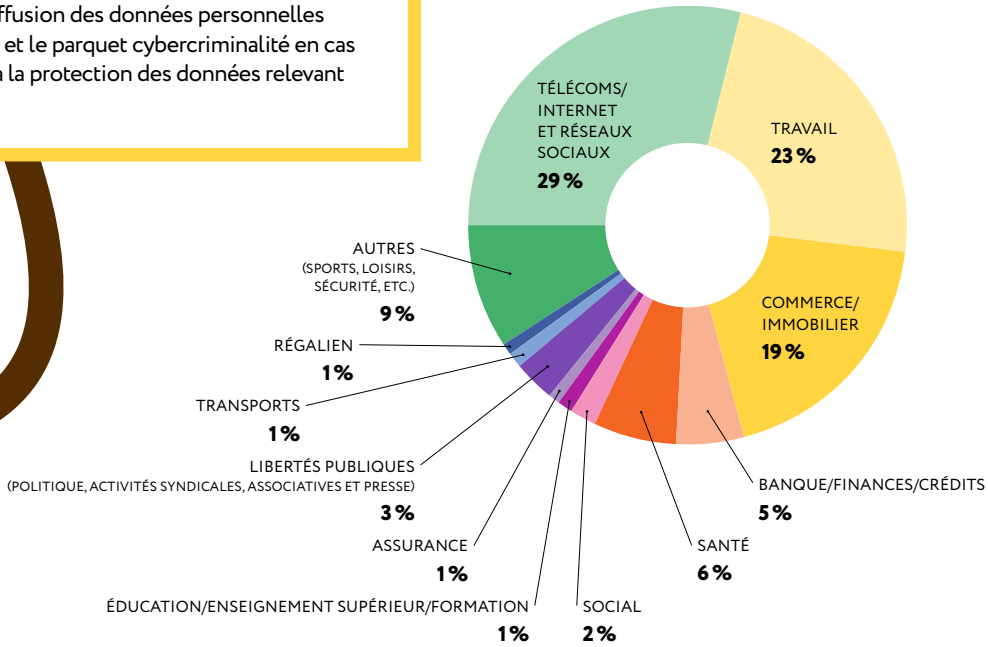
Un record avait été établi en 2024, avec 17 772 plaintes reçues par la CNIL, en hausse de plus de 8 % par rapport à l'année précédente. Il a été battu en 2025. L'augmentation est de plus de 10 %. Comme en 2024, elle s'explique notamment par les violations de données de grande ampleur qui ont touché des bases de données d'acteurs du secteur privé et public (voir page 52).

Les plaintes sont systématiquement instruites par la direction de l'exercice des droits et des plaintes (DEDP), qui revient ensuite vers les plaignants pour leur indiquer le résultat des investigations et, le cas échéant, la mesure correctrice adoptée.

Un exemple de traitement de plainte

Une femme victime de violences conjugales a déposé en 2025 une plainte à la CNIL contre un opérateur téléphonique pour manquement à la sécurité de ses données. Alors qu'elle aurait dû être placée en liste rouge, ses coordonnées étaient restées accessibles, ce qui a eu pour conséquence une usurpation d'identité par son ex-conjoint violent. La DEDP est intervenue très rapidement auprès de cet opérateur afin de mettre fin à la diffusion des données.

L'objet des plaintes



La procédure du guichet unique pour les plaintes transfrontalières

Les plaintes portant sur des traitements de données transfrontaliers (mis en œuvre dans plusieurs pays de l'Union européenne) sont gérées dans le cadre du mécanisme de « guichet unique ». Ainsi, si une solution ne peut être trouvée après un premier contact avec l'organisme mis en cause, l'autorité qui a reçu la plainte la transmet alors à l'autorité « chef de file », c'est-à-dire l'autorité de protection des données du pays où se situe l'établissement principal de l'organisme. Cette autorité procède à l'instruction et soumet un projet de décision aux autres autorités concernées afin d'aboutir à une décision consensuelle. En cas de désaccord, la décision peut faire l'objet d'une procédure de résolution des conflits auprès du Comité européen de la protection des données (CEPD). Il regroupe l'ensemble des autorités de protection des données européennes et ses décisions s'imposent à l'autorité « chef de file ».

En 2025, la CNIL a transmis plus de **230 plaintes transfrontalières.** Elle a examiné et répondu à plus de **600 sollicitations** provenant de ses homologues et publié une vingtaine de décisions à l'issue de l'instruction de plaintes transfrontalières.

Des rappels à la réglementation concernant la télésurveillance d'examens et la vidéoprotection excessive dans les communes

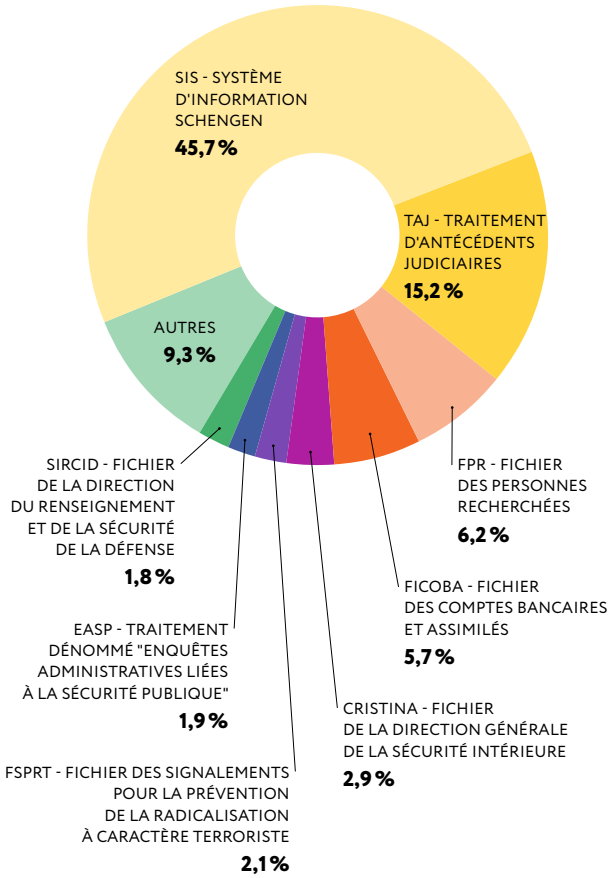
En 2025, la CNIL est intervenue auprès de nombreux organismes pour leur rappeler la réglementation applicable concernant le recours à des dispositifs de télésurveillance d'épreuves d'examen et de vidéoprotection :

- la CNIL a été saisie de plaintes relatives au projet envisagé par une université de procéder à des enregistrements vidéo et sonores des étudiants pendant des épreuves d'examen à distance. La CNIL a étudié les conditions de ce dispositif et la présidente a adressé un avertissement à l'université l'invitant à « revoir sa copie » avant la mise en place effective de ce projet, notamment sur l'impératif de réaliser une analyse d'impact, sur les risques du dispositif, et sur l'obligation de fournir une information précise aux personnes concernées ;
- la CNIL a rappelé à plusieurs communes que les systèmes de vidéoprotection doivent être mis en œuvre conformément au code de la sécurité intérieure (CSI) et au RGPD. Elle a aussi souligné que lorsque le dispositif de vidéoprotection apparaît particulièrement étendu au regard du nombre de caméras comparé au nombre d'habitants et à la superficie de la commune, avec une exploitation à grande échelle des données personnelles, il constitue un risque élevé d'atteinte aux droits fondamentaux nécessitant la réalisation d'une analyse d'impact.

Le FICOBA ne dépend plus de l'exercice des droits indirects géré par la CNIL

L'exercice des droits indirects (EDI) consiste à demander à la CNIL qu'elle vérifie le contenu d'un fichier dont la loi n'autorise pas la consultation directe par les personnes concernées. Cela concerne par exemple le Système d'information Schengen, une base de données européenne visant à renforcer la sécurité des frontières de l'espace Schengen. En 2025, la CNIL a reçu **6 999 demandes d'EDI** (voir la répartition ci-dessous).

Depuis le 6 janvier 2025, le FICOBA, notamment utilisé par l'administration en cas de contrôle fiscal, est désormais en accès direct. La démarche peut désormais s'effectuer depuis le site www.impots.gouv.fr. Ce changement de cadre permet une réaffectation des ressources pour les demandes relatives à d'autres fichiers.



Le saviez-vous ? La CNIL participe à la formation des agents de renseignement

Depuis 1978, la CNIL mène des missions de vérification auprès des services de renseignement pour instruire des demandes d'usagers. Elle peut notamment solliciter des rectifications ou des effacements de données pour certains fichiers. Forte de son expérience sur les fichiers de ces services, elle intervient régulièrement dans le cadre des formations de l'Académie du renseignement, qui forme les membres de tous les services de renseignement. C'est l'occasion de diffuser les bonnes pratiques s'agissant de la protection des données personnelles.

32 262
dossiers d'EDI clôturés

*dont **27 492** concernaient des demandes d'accès au Fichier national des comptes bancaires et assimilés (FICOBA) qui relevait de la CNIL jusqu'au 6 janvier 2025.*

Le LINC publie le bilan de l'Observatoire du droit d'accès sur les réseaux sociaux

Le Laboratoire d'innovation numérique de la CNIL (LINC) a mené une étude sur les parcours utilisateurs dans le cadre de l'exercice de leurs droits d'accès sur les réseaux sociaux. À partir d'une grille d'analyse des bonnes pratiques, il s'est intéressé aux dix réseaux sociaux parmi les plus utilisés en Europe et en France : Discord, Facebook, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitch, X et YouTube. De manière générale, l'étude publiée le 30 janvier 2025 fait apparaître que le taux de bonnes pratiques varie entre 44 % et 76,5 % dans les parcours des réseaux sociaux.

Tous les résultats de l'Observatoire du droit d'accès sur les réseaux sociaux

4 thématiques de contrôle prioritaires

En plus des contrôles faisant suite à des plaintes, à des signalements ou en lien avec l'actualité, la CNIL se mobilise tous les ans sur des thématiques prioritaires. Quatre sujets ont été retenus en 2025, représentant environ 30 % des contrôles effectués sur l'année.

1– La collecte de données par les applications mobiles

Les Français téléchargent en moyenne une trentaine d'applications par an. Elles sont ainsi devenues une source d'exploitation importante de données (bancaires, géolocalisation, publicitaires, etc.). Dans le prolongement de sa recommandation sur les applications mobiles d'octobre 2023, la CNIL a contrôlé 10 applications mobiles ou fournisseurs de code embarqué dans ces applications. Les vérifications ont essentiellement porté sur les accès aux données contenues sur le téléphone et la gestion des autorisations.

Les constats ont notamment mis en évidence un manque de transparence dans les informations fournies aux personnes, y compris lors de la collecte du consentement pour l'usage de la géolocalisation.

Comme annoncé dans son plan stratégique pour 2025-2028, ces actions de contrôle se poursuivront dans les prochaines années.

2– La cybersécurité des collectivités territoriales

La cybersécurité fait partie des axes majeurs du plan stratégique de la CNIL. Ces dernières années, de nombreuses cyberattaques ont visé les collectivités territoriales. Or elles traitent un grand nombre de données, pour certaines sensibles : état civil, versement de prestations sociales, données financières, etc.

La CNIL a donc contrôlé les mesures mises en œuvre par ces collectivités afin de protéger les données des usagers. 17 missions de contrôle ont été réalisées auprès de quinze organismes (communes, départements, régions et sous-traitants). Elles ont fait apparaître des manquements récurrents relatifs à la sécurité des données, tels que :

- l'utilisation de serveurs s'appuyant sur des systèmes d'exploitation obsolètes ;
- l'absence d'homologation au référentiel général de sécurité (RGS) ;
- l'utilisation de certificats de sécurité non qualifiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- le maintien d'une diversité de logiciels et téléservices autonomes engendrant des difficultés de gestion des habilitations et des mots de passe.

Ces manquements ne sont pas corrélés à la taille de la collectivité.

3– Les données traitées par l'administration pénitentiaire

L'ensemble des informations relatives aux personnes faisant l'objet d'une mesure restrictive ou privative de liberté est répertorié au sein du traitement de « Gestion nationale des personnes écrouées pour le suivi individualisé et la sécurité » (« GENESIS »). Dans le cadre de cette thématique, huit contrôles sur place ont été menés auprès d'un panel représentatif de structures et de services (centres pénitentiaires, maisons centrales, etc.). Ils ont notamment porté sur la sécurité du traitement, la robustesse du mode d'authentification à l'application et le cloisonnement de certaines données confidentielles.

4– Le droit à l'effacement

Cette thématique s'inscrit dans le cadre d'une action coordonnée (*coordinated enforcement framework*) du Comité européen de la protection des données (CEPD). Pour la quatrième année consécutive, la CNIL et plusieurs de ses homologues européens ont ainsi mené des vérifications sur un même sujet, en l'occurrence le droit à l'effacement.

La CNIL a procédé à des contrôles de 9 organismes, publics ou privés, de tailles et de secteurs d'activité divers, choisis sur la base de plaintes reçues à leur encontre. Il en ressort que ces organismes ont majoritairement mis en œuvre des mesures organisationnelles pour traiter les demandes de droit d'effacement qu'ils reçoivent :

- association du délégué à la protection des données (DPO) au traitement des demandes ;
- documentation du parcours de traitement de la demande, parfois distingué entre les demandes « simples » et « complexes » ;
- formation du personnel.

Toutefois, certains organismes rencontrent des difficultés pour :

- s'assurer que l'effacement est effectué sur l'ensemble du système d'information (y compris les sauvegardes) ;
- procéder à une anonymisation satisfaisante des données, lorsque l'effacement se fait par cette méthode ;
- traiter les demandes lorsqu'elles arrivent en nombre important au même moment.

Les contrôles en coopération au niveau européen

Comme précédemment indiqué (page 31), le RGPD prévoit un mécanisme de coopération dit de « guichet unique » lorsque les traitements mis en œuvre par un organisme établi dans l'espace économique européen concernent des personnes situées dans plusieurs pays de l'Union.

En 2025, près de quatre-vingts décisions ont été soumises aux homologues de la CNIL.

C'est notamment le cas de la procédure ayant donné lieu à une sanction à l'encontre de la société American Express Carte France, notamment en raison d'une collecte excessive de données (enregistrement de l'intégralité des appels téléphoniques reçus par le service client).

La CNIL réalise également des opérations de contrôle conjointes avec d'autres autorités de protection des données. C'est par exemple le cas avec l'autorité néerlandaise, autorité chef de file concernant l'analyse de la conformité des traitements effectués par la société Uber. La CNIL lui apporte son soutien dans le cadre de procédures en cours.

Le mot d'

Aleid Wolfsen,

président de Autoriteit Persoonsgegevens (AP), l'autorité néerlandaise de protection des données

« Une coopération étroite avec la CNIL »

« L'autorité néerlandaise de protection des données coopère étroitement avec la CNIL sur de nombreux dossiers internationaux, dans lesquels nous vérifions de possibles manquements au règlement général sur la protection des données. La CNIL et l'AP ont déjà uni leurs forces par le passé et ont pris des mesures efficaces pour protéger le droit à la protection des données personnelles. »

Comment se passe un contrôle de la CNIL ?

La CNIL a le pouvoir d'effectuer des contrôles auprès de l'ensemble des organismes qui traitent des données personnelles. Ils prennent quatre formes différentes, qui peuvent se combiner :

- **Le contrôle sur place :** une délégation de la CNIL se rend directement au sein des locaux d'un responsable de traitement ou d'un sous-traitant afin de mener des investigations ;
- **L'audition sur convocation :** un courrier est adressé au responsable de traitement ou au sous-traitant afin que des représentants de l'organisme se présentent, à une date donnée, dans les locaux de la CNIL. Ils devront répondre aux questions et, le cas échéant, rendre possible un accès aux ressources informatiques de l'organisme.
- **Le contrôle en ligne :** les agents de la CNIL effectuent des vérifications en consultant notamment des données librement accessibles en ligne, ou rendues accessibles, y compris par imprudence, négligence ou du fait d'un tiers. Ces vérifications peuvent, le cas échéant, être réalisées sous une identité d'emprunt.
- **Le contrôle sur pièces :** les agents de la CNIL adressent un courrier accompagné d'un questionnaire destiné à évaluer la conformité des traitements mis en œuvre par un responsable de traitement ou un sous-traitant. L'organisme visé par le contrôle doit communiquer à la CNIL ses réponses en y joignant tout document utile permettant de les justifier.

323
contrôles en 2025

dont

27 sur pièces

165 sur place

5 sur audition

126 en ligne

Entretien avec

Victor Nicolle,

directeur des contrôles et des sanctions

« Près de 30 % des sanctions sont liées à la cybersécurité »

Pourquoi la direction des contrôles et des sanctions (DCS) a-t-elle été créée ?

–

La DCS a été créée pour assurer cohérence et synergie, au service de l'efficacité de l'action répressive de la CNIL. Le lien entre les services en charge des contrôles et des sanctions est essentiel. La taille de la DCS – désormais comparable aux autres directions – permet des échanges plus structurés, ce qui contribue à enrichir la qualité des constatations et à rationaliser les délais de procédure. Et au sein de la chaîne répressive de la CNIL, les liens avec la direction des plaintes restent quotidiens.

Quels sont les principaux manquements constatés en 2025 ?

–

La cybersécurité domine : un tiers des contrôles, environ un quart des mesures correctrices, près de 30 % des sanctions. De nombreuses procédures sont en cours, notamment auprès des collectivités territoriales, concernant des fichiers de l'État et des entreprises détenant un grand nombre de données.

Constatez-vous une amélioration des pratiques à la suite d'une sanction ?

–

Tout à fait. Par exemple en matière de cookies, des manquements sont encore constatés mais ils portent moins sur des règles élémentaires, telles que l'absence de bandeau d'information. Les mesures correctrices de la CNIL portent leurs fruits et permettent des progrès. Sur la sécurité des protocoles HTTPS, une campagne de contrôles a par exemple montré qu'environ 90 % des sites web qui avaient été mis en demeure sont désormais en conformité. Les actions de communication sur l'action répressive de la CNIL et sa politique de contrôle donnent aussi de vrais résultats.

Un nombre d'amendes stable mais avec des montants importants

–

Alors que le nombre de sanctions est stable, 2025 se distingue par le montant total des amendes prononcées par la CNIL : plus de 486 millions d'euros. Ce niveau inédit s'explique notamment par deux décisions pour non-respect de la législation sur les cookies à l'encontre de Google et Shein.

Les sanctions prononcées

En 2025, 83 sanctions ont été prononcées par la CNIL. Un chiffre relativement stable par rapport à 2024 (87 sanctions). 16 ont été prononcées selon la procédure ordinaire et 67 selon la procédure simplifiée (lire page suivante). Ces sanctions comportent 78 amendes (dont 27 avec injonctions sous astreinte), 3 décisions de liquidation d'astreinte et 2 rappels à l'ordre.

À noter : 4 sanctions ont été adoptées en coopération avec les homologues européens de la CNIL. En parallèle, la CNIL a examiné 9 projets de décision d'homologues européens concernant des personnes résidant en France.

Le montant total des amendes s'élève à 486 839 500 € (contre 55 212 400 € en 2024). Deux sanctions en matière de cookies expliquent l'essentiel de ce chiffre.

259
mesures correctrices au total

83
sanctions *dont 16 selon la procédure ordinaire et 67 selon la procédure simplifiée*

31
rappels aux obligations légales par la présidente

486 839 500 €
d'amendes cumulées

143
mises en demeure

2
rappels à l'ordre

Cookies et autres traceurs : des règles qui ne peuvent plus être ignorées

Cinq ans après la publication de ses lignes directrices et recommandations, la CNIL a poursuivi en 2025 son plan d'action en matière de cookies et autres traceurs. Les contrôles menés ont permis de relever des situations de non-conformité.

21 organismes ont ainsi été sanctionnés, selon la procédure ordinaire ou simplifiée, pour divers manquements aux règles régissant les traceurs : dépôt sans le consentement de l'utilisateur, insuffisance des informations délivrées (ne permettant pas de recueillir un consentement éclairé), ou encore absence de prise en compte effective du refus de l'utilisateur ou du retrait de son consentement.

La CNIL insiste sur l'impact de ces pratiques pour les internautes, dont les données sont parfois traitées à leur insu, et sur le fait que les acteurs sanctionnés ne pouvaient ignorer les règles applicables. C'est notamment la prise en compte de ces éléments qui explique les amendes prononcées à l'encontre de deux acteurs majeurs, Google (325 M€) et Shein (150 M€) (voir page suivante).

Procédure ordinaire, procédure simplifiée, quelles différences ?

La procédure ordinaire relève de la formation restreinte de la CNIL, composée de 5 membres et d'un président distinct du président de la CNIL. Elle peut prononcer des sanctions financières allant jusqu'à 20 M€ ou 4 % du chiffre d'affaires annuel mondial.

La procédure simplifiée, mise en place en 2022, peut être engagée si l'affaire ne présente pas de difficulté particulière. Le dossier est alors examiné par le président de la formation restreinte seul (ou par un des membres qu'il a désigné). En cas d'amende, le montant maximal est de 20 000 €.

Vidéosurveillance permanente des salariés : une atteinte à la protection de la vie privée

16 organismes ont été sanctionnés en 2025 pour non-respect des règles applicables à la vidéosurveillance des salariés. En l'absence de circonstances exceptionnelles, la surveillance vidéo permanente de salariés constitue une atteinte à la protection des données personnelles.

Sont ainsi contraires à ces règles les dispositifs filmant en continu les employés de caisses d'un magasin ou des bureaux. De même, l'installation de caméras dissimulées ne peut intervenir que dans des circonstances exceptionnelles, et à la condition de ménager un juste équilibre entre l'objectif poursuivi (la protection des biens et des personnes) et la protection de la vie privée des salariés.

Obligations des sous-traitants : le respect du RGPD s'impose aussi

Le non-respect des obligations pesant sur les sous-traitants concernant les données qui leur sont confiées a également été sanctionné. L'occasion de rappeler que les sous-traitants doivent :

- mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adéquat ;
- ne traiter les données que sur instruction du responsable de traitement ;
- et supprimer les données à l'issue de leur relation contractuelle avec le responsable de traitement.

Les principaux manquements sanctionnés par la procédure simplifiée

- 14 organismes ont été sanctionnés pour un manquement relatif à la sécurité des données personnelles : ils utilisaient, par exemple, des mots de passe insuffisamment robustes ou des comptes partagés entre utilisateurs.
- 14 organismes (sociétés, professionnels libéraux) ont été sanctionnés pour n'avoir pas répondu aux demandes de la CNIL.
- 14 décisions ont été prises en raison de la non-prise en compte de demandes d'effacement, d'opposition ou d'accès.
- 10 sanctions ont été prononcées pour des manquements liés à la prospection, qu'elle soit commerciale ou politique.

Les mises en demeure

En 2025, la CNIL a adressé 143 mises en demeure (décisions de la présidente de la CNIL ordonnant à un organisme de se mettre en conformité dans un délai fixé).

Plusieurs concernaient le secteur de l'aide sociale à l'enfance (absence de politique rigoureuse de conservation de données, défaut d'information des personnes, gestion défaillante des habilitations et des mots de passe...). D'autres mises en demeure ont visé des applications mobiles et jeux en ligne afin d'améliorer la transparence des traitements et de mieux protéger les données des mineurs qui représentent une part importante des utilisateurs.

Deux sanctions marquantes en 2025

325 millions d'euros d'amendes contre Google

Saisie d'une plainte déposée le 24 août 2022 par l'organisation None Of Your Business (NOYB), la CNIL a mené plusieurs contrôles sur la messagerie électronique Gmail et sur le parcours de création d'un compte Google. Ils ont permis de constater que des annonces publicitaires prenant la forme de courriels s'affichaient au sein de la messagerie Gmail. La CNIL a considéré que l'affichage de telles publicités aurait nécessité le recueil du consentement des utilisateurs.

Par ailleurs, la CNIL a relevé qu'à la création d'un compte Google, les utilisateurs n'étaient pas clairement informés que l'accès aux services de Google est conditionné au dépôt de traceurs à finalité publicitaire. Ce qui constitue un manquement à la loi Informatique et Libertés.

Pour ces manquements, la CNIL a prononcé le 1er septembre 2025 deux amendes d'un montant total de 325 millions d'euros, estimant notamment que Google avait déjà été sanctionné à deux reprises pour des faits comparables.

150 millions d'euros d'amende contre Shein

Lors d'un contrôle en août 2023, la CNIL a constaté que le site web « shein.com » ne respectait pas plusieurs obligations de la loi Informatique et Libertés, en déposant certains traceurs sans le consentement des internautes, en ne respectant pas leur choix et en ne les informant pas correctement.

La CNIL a prononcé le 1er septembre 2025 une amende de 150 millions d'euros à l'encontre de la société Infinite Styles Services Co. Limited, la filiale irlandaise du groupe Shein, prenant notamment en compte le caractère massif du traitement en cause.

Comment sont recouvrées les amendes de la CNIL ?

Toutes les amendes prononcées par la CNIL, qu'elles concernent les acteurs privés ou publics, sont recouvrées par le Trésor public (Direction générale des finances publiques) et sont versées au budget de l'État.

L'activité contentieuse

Le Conseil d'État a confirmé 97,5 % des décisions de la CNIL contestées

En 2025, 89 recours contentieux ont été communiqués à la CNIL, contre 94 en 2024. Ces recours ont principalement été formés devant le Conseil d'État, mais aussi devant la cour administrative d'appel, le tribunal administratif et le Conseil constitutionnel.

Sur les 80 décisions rendues par le Conseil d'État, 97,5 % ont confirmé les positions de la CNIL.

Les 3 principaux motifs de recours

- 53 recours ont porté contre des décisions de clôture de plainte (les plaignants souhaitaient que la CNIL rouvre une plainte qu'elle avait close après examen des faits) ;
- 11 recours ont concerné des décisions de sanctions (10 sanctions de la formation restreinte de la CNIL et 1 sanction simplifiée) ;
- 6 recours étaient en lien avec des délibérations de la formation plénière de la CNIL (par exemple contre des recommandations de la CNIL ou des autorisations portant sur des traitements de données personnelles).

L'avis de la CNIL sur les caméras « augmentées » est validé

Le 30 janvier 2026, le Conseil d'État a rejeté un recours de la commune de Nice qui contestait une délibération de la CNIL du 15 mai 2025. Elle avait estimé illégal le dispositif de traitement algorithmique des images des caméras de vidéosurveillance mis en place par la commune de Nice à l'entrée des écoles. La ville voulait détecter, grâce à un algorithme, la présence de véhicules stationnant irrégulièrement devant les écoles. Le Conseil d'État a rappelé que le code de la sécurité intérieure autorisait bien la mise en œuvre de systèmes de vidéosurveillance des voies publiques, mais ne permettait pas une analyse systématique et automatisée des images collectées. Il a donc jugé que la CNIL n'avait pas commis d'erreur de droit et validé sa décision.

La régulation de l'IA et le soutien à l'innovation

LES NOUVELLES RECOMMANDATIONS CONCERNANT L'IA 39

MOBILISATION AUTOUR DU SOMMET POUR L'ACTION SUR L'IA 40

BILAN DU « BAC À SABLE » SUR L'IA ET LES SERVICES PUBLICS 40

DEUX FAQ SUR L'UTILISATION DE L'IA DANS LES ÉTABLISSEMENTS SCOLAIRES 41

PANAME : UN PARTENARIAT POUR L'AUDIT DE LA CONFIDENTIALITÉ DES MODÈLES D'IA 41

UN OUTIL POUR LA TRAÇABILITÉ DES MODÈLES D'IA PUBLIÉS EN SOURCE OUVERTE 42

EXPLIQUER L'EXPLICABILITÉ DE L'IA 42

LES ÉVÉNEMENTS LIÉS À L'INNOVATION ET À L'ÉTHIQUE 43

LA MORT NUMÉRIQUE, THÈME DE AIR2025 ET DU CAHIER INNOVATION ET PROSPECTIVE 43

Les nouvelles recommandations concernant l'IA

Entretien avec

Thomas Dautieu,

directeur de l'accompagnement juridique

« *Anticiper l'IA pour mieux la réguler* »

Quel est le rôle de la CNIL dans la régulation de l'IA ?

La CNIL intervient depuis de nombreuses années dans la régulation de l'IA car la majorité des systèmes d'IA ont été créés à partir de données personnelles et s'en nourrissent. Dès 2017, elle publiait un rapport sur les algorithmes qui pointait très clairement les bienfaits, mais aussi les risques, liés à cette technologie. Au fur et à mesure des dossiers qu'elle a été amenée à traiter, la CNIL a affiné sa doctrine pour garantir un haut niveau de protection des données. Très prochainement, son champ de régulation devrait s'élargir dans le cadre de la mise en œuvre du règlement sur l'IA. La CNIL devrait ainsi être compétente pour réguler la majorité des systèmes d'IA dits « à haut risque ». Cette évolution des missions de la CNIL permettra d'assurer une régulation cohérente entre le RGPD et le RIA, tant au bénéfice des personnes que des entreprises.

Comment la CNIL anticipe-t-elle les innovations de l'IA pour alimenter ses actions ?

La capacité à anticiper et comprendre les innovations et avancées technologiques est essentielle pour un régulateur, en particulier en ce qui concerne l'IA. La CNIL en a d'ailleurs fait un axe essentiel de son plan stratégique 2025-2028. Cette anticipation ne se fait pas « en chambre » et nécessite qu'elle soit à l'écoute des acteurs qui développent des systèmes d'IA et de ceux qui les déploient. C'est un dialogue qui doit être permanent, franc et ouvert, tant sur le plan juridique que technique. La CNIL est résolue à discuter avec tout l'écosystème IA au bénéfice d'une régulation pragmatique, sur une matière exigeante et en perpétuelle évolution.

La CNIL a enrichi en 2025 son corpus de recommandations pour sécuriser les concepteurs et les développeurs de systèmes d'IA. Une série de fiches pratiques, complétée par une liste de vérifications, permettent une approche très opérationnelle.

La CNIL a publié plusieurs recommandations en 2025 sur le développement des systèmes d'IA. L'enjeu : clarifier le cadre juridique pour sécuriser les acteurs et favoriser l'innovation tout en assurant le respect des droits fondamentaux. En décembre 2024, un avis du Comité européen de la protection des données (CEPD) avait précisé que le RGPD s'appliquait bien, dans de nombreux cas, aux modèles d'IA entraînés sur des données personnelles en raison de leurs capacités de mémorisation. Il revenait donc à la CNIL d'aider les professionnels à avancer et à innover en toute sécurité juridique, en étant sûrs de leur conformité.

L'ensemble des fiches mises à disposition par la CNIL a été élaboré à la suite de consultations publiques. Entreprises, chercheurs, universitaires, associations, conseils juridiques et techniques, syndicats, fédérations, etc., ont ainsi pu s'exprimer pour aboutir à des recommandations au plus proche de leurs préoccupations et de la réalité des usages de l'IA. Des bases avaient déjà été posées depuis le lancement en mai 2023 du plan d'action de la CNIL sur l'IA.

Comment informer et faciliter l'exercice des droits des personnes ?

Le corpus de recommandations s'est d'abord enrichi en février 2025 de deux documents proposant des solutions concrètes et proportionnées pour informer et faciliter l'exercice des droits des personnes.

La première recommandation concerne ainsi l'information des personnes. La CNIL précise les obligations d'information lorsque des données personnelles servent à l'entraînement d'un modèle d'IA et sont potentiellement mémorisées par celui-ci.

La seconde recommandation concerne l'exercice des droits des personnes concernées. La réglementation européenne prévoit des droits d'accès, de rectification, d'opposition et d'effacement des données personnelles. Mais ces droits peuvent être difficiles à mettre en œuvre dans le cadre de modèles d'IA. La recommandation de la CNIL apporte des réponses opérationnelles aux concepteurs et aux développeurs.

À quelles conditions mobiliser l'intérêt légitime ?

En juin, la CNIL a consacré une recommandation au sujet de l'intérêt légitime en tant que base légale à la mise en œuvre d'un système d'IA. Il est souvent invoqué comme alternative au recueil du consentement. Pour que cela fonctionne, il y a trois conditions à respecter que la CNIL a détaillées et illustrées :

- l'intérêt poursuivi doit être « légitime » ;
- le traitement envisagé doit être « nécessaire » ;
- et il ne doit pas porter une atteinte disproportionnée aux droits et intérêts des personnes concernées.

En synthèse, 13 fiches pratiques IA et une liste de vérifications

Ces nouvelles recommandations ont permis à la CNIL de finaliser la rédaction de 13 fiches pratiques. Elles couvrent l'ensemble des étapes du développement d'un système d'IA, en commençant par déterminer le régime juridique applicable.

Dans cette logique très opérationnelle, la CNIL a aussi publié en 2025 une liste de vérifications issue de ses recommandations. Celle-ci permet aux concepteurs et aux développeurs de systèmes d'IA de s'assurer que, dès le départ, les principes du RGPD sont correctement mis en œuvre : finalité, minimisation, sécurité, information, droits des personnes, transparence et gouvernance.

Mobilisation autour du Sommet pour l'action sur l'IA

Du 6 au 11 février à Paris, la CNIL a participé à de nombreux événements organisés dans le cadre du Sommet pour l'action sur l'IA. L'objectif était de promouvoir l'idée que le développement de l'IA était compatible avec la protection des données personnelles et devait s'inscrire dans une démarche éthique. La présidente de la CNIL, Marie-Laure Denis, et plusieurs agents de la CNIL ont notamment pris part à plusieurs tables rondes lors du Sommet lui-même ainsi qu'en marge de l'événement.

Comment la CNIL a-t-elle travaillé pour élaborer ces recommandations ?

La réponse de Nacéra,
cheffe du service des affaires économiques

« Les nouvelles recommandations de la CNIL sur l'IA s'inscrivent dans un travail engagé depuis plusieurs années. Nous avons fait le choix de nous concentrer, dans un premier temps, sur la phase de conception pour répondre aux sollicitations des acteurs et par conviction : intégrer, dès l'origine, les exigences de protection des données permet de déployer des systèmes plus respectueux des libertés individuelles. Fidèle à une démarche de régulation inclusive, la CNIL a étroitement dialogué avec les acteurs afin de proposer des repères concrets, actionnables, assortis d'outils pratiques pour les TPE-PME (contenu synthétique, listes de vérifications opérationnelles). »

Systèmes d'IA : les recommandations de la CNIL pour respecter le RGPD

Bilan du « bac à sable » sur l'IA et les services publics

En 2024, la CNIL a accompagné trois projets visant à améliorer les services publics grâce à l'IA : « Conseils Personnalisés » de France Travail, « Ekonom IA » de Nantes Métropole et « PRIV-IA » avec la RATP. Cet appui juridique et technique s'est fait dans le cadre du programme « bac à sable », qui prévoit de partager les enseignements tirés de cet accompagnement pour en faire bénéficier l'ensemble des innovateurs sur leurs propres projets. Les équipes ont notamment travaillé sur les enjeux de la constitution d'une base de données à des fins d'apprentissage, sur la notion d'intervention humaine significative, sur la minimisation des données d'une IA générative ou encore sur une nouvelle forme de captation vidéo. La synthèse des recommandations de la CNIL a été publiée en avril 2025.

La synthèse du bac à sable

Deux FAQ sur l'utilisation de l'IA dans les établissements scolaires

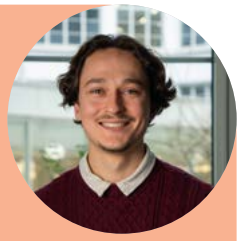
Diminution de tâches répétitives pour les enseignants, production d'exercices et aide à la correction, aide aux devoirs pour les élèves… le recours à des systèmes d'IA ouvre de nouvelles perspectives dans le domaine de l'éducation. Ils doivent toutefois être encadrés car ils concernent des élèves la plupart du temps mineurs, plus vulnérables face aux risques numériques (confiance excessive vis-à-vis des résultats fournis, recherche de réponses toutes faites, perte de confidentialité…). Ces technologies peuvent également impacter les enseignants et l'ensemble de l'écosystème éducatif en encourageant, par exemple, une approche trop standardisée de l'enseignement et de l'évaluation.

Pour accompagner enseignants et responsables d'établissement, la CNIL a mis à disposition en juin 2025 des recommandations concrètes sous la forme de deux foires aux questions :

- l'une pour les enseignants, centrée sur les usages pédagogiques concrets, les bonnes pratiques et les précautions à prendre en classe ;
- l'autre pour les responsables de traitement (chefs d'établissement, ministère, autorités académiques), axée sur les obligations légales et les conditions de mise en conformité.

Les FAQ

Comment s'opposer à la réutilisation de ses données personnelles pour l'entraînement des agents conversationnels ?



La réponse de Romain, ingénieur IA à la CNIL

« Utiliser un agent conversationnel en ligne implique souvent la transmission de données personnelles lors des interactions avec ce dernier. Les conversations contenant ces données sont stockées dans l'historique de l'utilisateur, qui peut les supprimer à tout moment. Cependant, elles sont aussi susceptibles d'être réutilisées par les fournisseurs de ces agents pour entraîner les modèles d'IA générative, dont la performance repose en partie sur la quantité, la diversité et la qualité de données d'entraînement.

Tout utilisateur peut s'opposer à la réutilisation de ses données à cette fin. Les modalités d'exercice du droit d'opposition sont propres à chaque fournisseur et peuvent prendre des formes différentes. Pour s'y retrouver, la CNIL a publié un article sur son site qui détaille les modalités d'exercice du droit d'opposition pour les principaux fournisseurs de systèmes d'IA. »

La marche à suivre selon les principales plateformes

PANAME : un partenariat pour l'audit de la confidentialité des modèles d'IA

Le projet PANAME (*Privacy AuditiNg of Ai ModEls*), lancé en juin 2025, vise à développer une bibliothèque logicielle destinée à évaluer si un modèle traite ou non des données personnelles. Cet outil permettra d'offrir des solutions techniques opérationnelles aux développeurs et utilisateurs de modèles d'IA pour appliquer les recommandations de la CNIL. Il associe des équipes de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de la CNIL, d'Inria et du Pôle d'expertise de la régulation numérique (PEReN).

Entretien avec

Bruno Sportisse,

président - directeur général d'Inria, l'Institut national de recherche en sciences et technologies du numérique

« *Notre partenariat va faire dialoguer innovation et régulation pour une IA de confiance* »

Pourquoi avoir signé en 2025 un nouveau partenariat entre Inria et la CNIL ?

–

Ce partenariat s'inscrit dans une relation déjà ancienne entre Inria et la CNIL. Depuis près d'une dizaine d'années, nous travaillons ensemble sur des sujets concrets, notamment autour de la protection de la vie privée. Le nouvel accord renforce cette collaboration et l'élargit à de nouveaux enjeux, en particulier l'évaluation des systèmes d'IA.

La diffusion massive de l'IA soulève de nouvelles questions en matière de confidentialité et de respect des droits fondamentaux. Nous devons être capables d'analyser ces systèmes, de les auditer et de développer des méthodes scientifiques permettant de vérifier, par exemple, que des données personnelles utilisées lors de l'apprentissage ne sont pas restituées de manière inappropriée. Dans ce contexte, travailler étroitement avec une autorité de régulation comme la CNIL est essentiel pour apporter une expertise scientifique à l'appui des politiques publiques et accompagner la mise en œuvre du cadre européen, qu'il s'agisse du RGPD ou du règlement sur l'IA.

Quelles formes va prendre ce partenariat ?

–

Il se traduira par des projets de recherche communs, des échanges d'expertise, des mobilités entre équipes et le développement d'outils technologiques dédiés à l'évaluation des systèmes d'IA. Nous avons déjà engagé des initiatives en ce sens, comme le projet PANAME, consacré à l'audit du respect de la vie privée dans les modèles d'IA, mené avec plusieurs partenaires publics (lire page 41).

Au-delà de ces réalisations opérationnelles, l'enjeu central est de créer, le plus en amont possible, un dialogue structuré entre innovation et régulation. Dans un environnement européen au cadre normatif très structurant, innovation et régulation ne doivent pas s'opposer, mais avancer ensemble pour garantir notre capacité à innover et à développer une IA digne de confiance.

Un outil pour la traçabilité des modèles d'IA publiés en source ouverte

–

La CNIL a mis à disposition en décembre 2025 un outil expérimental pour explorer comment les droits des personnes (comme les droits d'opposition, d'accès ou d'effacement) pourraient être exercés si leurs informations personnelles se retrouvaient dans un modèle d'IA. Une des difficultés est que ces données peuvent être mémorisées dans un modèle en source ouverte, puis utilisées et mémorisées par d'autres modèles. Il devient donc essentiel de pouvoir naviguer dans la généalogie des modèles échangés pour pouvoir efficacement exercer ses droits.

La présentation de l'expérimentation

Expliquer l'explicabilité de l'IA

–

Le LINC, le Laboratoire d'innovation numérique de la CNIL, a publié en juillet les premiers résultats de ses recherches sur l'explicabilité de l'IA (*explainable AI ou xAI*). Ce champ scientifique vise à expliquer les informations, les prédictions ou les décisions générées par des systèmes d'IA. Le LINC s'intéresse notamment au contexte social et institutionnel qui permet le développement de l'xAI.

Les travaux de recherche du LINC sur l'xAI

Les événements liés à l'innovation et à l'éthique

Nouvelle édition de la Journée de recherche sur la vie privée

La 4e édition de la Journée de recherche sur la vie privée, le *Privacy Research Day*, s'est déroulée le 1er juillet à la CNIL et en ligne. Cet événement interdisciplinaire a pour vocation de créer des échanges inédits entre des juristes, des informaticiens, des designers ou encore des chercheurs en sciences sociales. Cinq grands thèmes ont nourri la journée : « Perceptions des risques et stratégies des utilisateurs », « Protéger les données à l'ère des réseaux sociaux », « Limites et leviers de la mise en conformité transnationale », « Défis pour la protection des données à l'heure de l'IA » et « Protéger les données de santé ». Une rediffusion de l'événement est disponible sur le site de la CNIL.

Retrouver l'événement en vidéo

Le premier prix CNIL/EHESS est décerné à Laurène Assailly

Fruit du partenariat entre la CNIL et l'École des hautes études en sciences sociales, ce prix a été créé en 2025 pour promouvoir des travaux de recherche en sciences sociales portant sur la protection de la vie privée et des libertés. Il a été remis lors de la Journée de recherche sur la vie privée à Laurène Assailly pour sa thèse sur la régulation des données de santé. Docteure en science politique au laboratoire SAGE et ATER à Sciences Po Strasbourg, ses recherches portent notamment sur les stratégies de réutilisation des données cliniques pour la recherche dans les hôpitaux.

Publication des actes de l'école d'automne CNIL/EHESS

Dans le cadre du partenariat entre les deux organismes, le LINC a publié en 2025 les actes de l'école d'automne coorganisée par la CNIL et l'EHESS. Cet événement international a réuni, pour une semaine d'échanges intensifs, des chercheuses et des chercheurs en début de carrière et d'autres de premier plan, issus de disciplines variées. Il en ressort des discussions de haut niveau sur des sujets tels que l'histoire des données en ligne, les approches infrastructurelles de la régulation des données, la géopolitique des routes de l'Internet et les défis de la distribution des données.

La mort numérique, thème de air2025 et du Cahier Innovation et Prospective

La CNIL a consacré deux temps forts en 2025 aux questions liées à la gestion des données *post mortem*. Ce sujet devient un enjeu de société : d'après une enquête réalisée par Harris Interactive pour la CNIL, près d'un tiers des Français indique avoir déjà été confronté à des contenus sur les réseaux sociaux émanant de comptes de personnes décédées. La mort numérique a ainsi été au cœur de l'événement air2025 (Avenir, Innovations, Révolutions), moment de réflexion éthique qui s'est déroulé le 15 octobre en partenariat avec la Bibliothèque nationale de France. Thème de la journée : « Intimité des disparus, mémoire des vivants : quelle éthique pour les traces numériques ? ».

L'autre temps fort sur ces questions a été la publication par le LINC du Cahier Innovation et Prospective n°10 sur le thème : « Nos données après nous - explorer les enjeux de la mort numérique ». Un numéro qui interroge la gestion des comptes, la transmission des données et l'émergence d'agents conversationnels fondés sur les données des défunts.

[Rediffusion] Évènement air2025

Jeunes, familles, adultes : la sensibilisation au plus près des publics

LES PARTENARIATS DE LA CNIL POUR S'ADRESSER AU GRAND PUBLIC ET AUX JEUNES 45

LES ACTIONS SUR LE TERRAIN 46

LES NOUVELLES RESSOURCES POUR LES JEUNES ET LEURS FAMILLES 47

UN FORT ATTRAIT DU PUBLIC POUR LES ACTIONS ET LES PUBLICATIONS DE LA CNIL 49

Entretien avec

Catherine Morin-Desailly,

membre du Collège de la CNIL en charge du secteur de l'éducation et de l'enseignement supérieur

« Dans notre société entièrement numérisée, notre citoyenneté se prolonge aujourd'hui en ligne »

Quels sont les principaux risques encourus par les mineurs en ligne ?

–

Les mineurs en ligne sont victimes du modèle toxique des plateformes qui privilégient le profit à leur bien-être. Les risques pour leur santé mentale sont bien documentés, les recherches scientifiques et les témoignages des familles sont nombreux : troubles de l'attention et du sommeil, difficultés d'apprentissage et de concentration, exposition à des contenus choquants ou dégradants… Les filles, en particulier, visionnent des images qui altèrent le rapport à leur corps et peuvent exacerber des troubles alimentaires. Par ailleurs, les cyberviolences et le cyberharcèlement se multiplient. Enfin, les mineurs, comme les adultes, peuvent subir de la désinformation accentuée par les algorithmes.

Quels sont les premiers réflexes que les adolescents peuvent adopter pour se protéger ?

–

Il existe des premiers gestes simples relevant du paramétrage de leur compte : inscription sous un pseudonyme, création d'un compte privé, suppression de la géolocalisation… Pour cela, et pour lutter contre l'ensemble des risques, il faut aussi un plan d'action global pour former et informer l'ensemble des adultes qui les entourent.

La CNIL évoque régulièrement la notion de citoyenneté numérique, de quoi s'agit-il ?

–

Dans notre société entièrement numérisée, notre citoyenneté se prolonge aujourd'hui en ligne. Comme nous apprenons à vivre ensemble hors ligne, il faut aussi acquérir les compétences et les connaissances nécessaires à un usage responsable des outils numériques.

Les partenariats de la CNIL pour s'adresser au grand public et aux jeunes

–

Avec Radio France

La CNIL et Radio France s'associent pour une toute nouvelle chronique « Vie numérique, vie privée ». Chaque samedi et dimanche, depuis fin août 2025, les 44 antennes locales de la radio ICI explorent avec la journaliste Valentine Letesse un sujet du quotidien des Français en lien avec le numérique et donnent les clés pour bien protéger sa vie privée.

Rediffusions de Radio France « Vie numérique, vie privée »

Avec France Télévisions

Du 11 au 18 décembre 2025, les 6 chaînes du Groupe France Télévisions ont diffusé 250 fois le clip vidéo « Réfléchissez avant de publier » réalisé avec l'autorité de protection des données irlandaise, la Data Protection Commission. 9,6 millions de téléspectateurs de plus de 4 ans l'ont vu (voir aussi page 49).

Avec Geek Junior

Disponible sur abonnement, Geek Junior est un magazine mensuel d'éducation numérique pour les collégiens et les lycéens. Assistants vocaux, droits d'accès et d'effacement, pseudos, jeux vidéo, IA génératives, paramètres de réseaux sociaux, etc., n'ont plus de secrets pour ses lecteurs. La CNIL propose dans chaque numéro un tutoriel pour mieux agir en faveur de la protection de ses données personnelles.

Avec SNCF Voyageurs

Les voyageurs sont nombreux à sortir leurs écrans dans les trains. Mais pendant la pause au wagon-bar ou avant d'aller aux toilettes, trop peu pensent à verrouiller leur ordinateur. À l'arrivée en gare, il n'est pas rare d'oublier sa clé USB ou son téléphone. Alors, pour inciter à rester vigilant et protéger ses données personnelles quand on voyage, la CNIL et SNCF Voyageurs se sont associés. Les écrans à bord des wagons diffusent des conseils de la CNIL. Une infographie pédagogique est également accessible depuis les portails Wi-Fi à bord des trains.

Avec 107.7 FM, la radio des autoroutes

Sur la route des vacances, dans la deuxième quinzaine du mois d'août et pendant les congés de fin d'année, la CNIL propose des spots sur 107.7 FM, la radio des autoroutes. Ils ont notamment permis de toucher plus de 16 millions d'auditeurs en évoquant la sécurisation de l'accès à son téléphone portable ou encore l'application FantomApp (voir page 47).

Avec l'Éducation nationale

Pour leur 8e édition, les « Trophées des classes » ont été décernés le 21 mai 2025. Ce concours promeut une culture citoyenne des usages du numérique dans le cadre de l'éducation aux médias et à l'information (EMI). Ouvert du CM1 à la 3e ainsi qu'aux lycées français à l'étranger, il est organisé par la CNIL et le ministère de l'Éducation nationale, en partenariat avec Radio France, le collectif Educnum et les établissements scolaires du dispositif eTwinning, déployé par le réseau Canopé. Cette année, trois collèges et quatre écoles élémentaires ont vu leurs productions récompensées autour des thèmes « Civisme numérique » et « Connaître ses droits numériques en France, en Europe ».

266
actions menées sur le terrain, dont 73 ciblant des mineurs

+ de 20 000
personnes sensibilisées

Les actions sur le terrain

Pour la première fois à Paris Plage

L'été 2025, sur les quais du canal de l'Ourcq dans le 18e arrondissement, les Parisiens et les touristes ont pu échanger avec les agents de la CNIL dans le village Santé créé par la Ville de Paris qui regroupait des acteurs de la prévention. 31 agents de la CNIL se sont ainsi mobilisés sur 19 journées pour aller à la rencontre de plusieurs centaines de personnes de tous âges, volontaires et participatives.

Le jeu « L'Odyssée du numérique », outil de dialogue entre adultes et enfants, conçu par le ministère de l'Éducation nationale avec la CNIL, l'Arcom, l'UNAF et Tralalère, a rencontré un vif succès. Lien entre les générations, ce jeu de plateau a permis, entre rires et arguments chevronnés, d'engager des discussions autour de la citoyenneté numérique et de la protection de ses données.

Un kit pour sensibiliser les parents salariés

L'opération est née d'un double constat : près de 9 salariés sur 10 ont des enfants, et le lieu de travail est le premier endroit de prise en compte des enjeux de cybersécurité. La CNIL et l'Association française des correspondants à la protection des données à caractère personnel (AFCDP) ont ainsi décidé de fournir aux délégués à la protection des données (DPO) un kit clé en main dédié à la parentalité numérique. Objectif : les aider à aborder avec leurs collègues les questions de protection des données et de la vie privée sous l'angle de la protection des enfants. Ce kit permet d'animer un atelier d'1 h 30.

Télécharger le kit

Des jeux et des parcours ludiques au Festival Hauts-de-Seine Digital Games

La CNIL était présente les 4 et 5 avril 2025 à la 4e édition du Festival Hauts-de-Seine Digital Games, organisé par le Département des Hauts-de-Seine, à la Seine Musicale à Boulogne-Billancourt. C'est à la fois le rendez-vous des amateurs de jeu vidéo et un rendez-vous pédagogique et éducatif qui vise à sensibiliser les jeunes et leurs familles. La CNIL proposait des jeux et des parcours ludiques pour évoquer la vie privée, les données personnelles, l'identité en ligne, la citoyenneté numérique…

Échanges et conférences au Salon des seniors

La CNIL a participé du 12 au 15 mars 2025 au Salon des seniors à Paris Expo Porte de Versailles. Elle a répondu sur son stand à toutes les questions sur la protection de la vie numérique au quotidien. Elle a aussi animé trois conférences : « Arnaques en ligne, comment s'en protéger ? », « *Silver* économie et protection des données » et « Faire face aux cyberattaques » avec les équipes de cybermalveillance.gouv.fr.

Entretien avec

Justine Atlan,

directrice générale de l'Association e-Enfance / 3018

« Surexposition, contenus toxiques, cyberharcèlement… Pour les enfants, les risques s'additionnent »

Quels sont les principaux dangers auxquels sont confrontés les enfants et les adolescents en ligne ?
–
Tout d'abord, un risque de surexposition aux écrans, de précocité et de temps passé excessif, liés aux mécanismes de captation de l'attention et au modèle économique des plateformes.
Les enfants et les adolescents y sont particulièrement sensibles, mettant en danger leur développement. Une fois en ligne, ils sont confrontés aux risques internes des plateformes : enfermement algorithmique, exposition à des contenus nuisibles, etc. S'y ajoute le risque de cyberharcèlement sous toutes ses formes.

Quelles actions menez-vous pour protéger les jeunes ?
–
Notre premier axe est la prévention, en intervenant dès 6 ans avec notre programme « Super Héros du Net », et en associant les parents qui jouent un rôle clé dans l'accompagnement des usages numériques. Nous formons également un très large public de professionnels : enseignants, magistrats, gendarmes, pédiatres, travailleurs sociaux, animateurs sportifs…

Nous opérons par ailleurs le numéro national **3018**, dédié au harcèlement – en ligne et hors ligne – et à toutes les violences numériques faites aux mineurs. Ce service permet aussi de signaler rapidement des contenus préjudiciables grâce à notre statut de « signaleur de confiance », attribué par l'ARCOM dans le cadre du *DSA*. Le 3018 nous permet également d'alerter l'Éducation nationale, Pharos ou les services sociaux lorsque la situation l'exige.

Comment s'articule votre partenariat avec la CNIL ?
–
Nous travaillons étroitement avec la CNIL depuis plus de dix ans au sein du collectif EducNum, dont nous sommes membres fondateurs. Ensemble, nous élaborons des ressources et des actions de sensibilisation à destination des jeunes, des familles et des professionnels.

Le partenariat s'est renforcé avec le lancement récent de l'application mobile FantomApp de la CNIL, coordonnée avec notre Application 3018, pour orienter les jeunes et leurs parents vers le service adapté. Historiquement, nous avons également collaboré dans le cadre de la mise en œuvre du RGPD et de la définition de la majorité numérique en France à 15 ans dès 2018, en soulignant l'importance d'impliquer d'emblée l'enfant aux côtés de ses parents dans le consentement.

Les nouvelles ressources pour les jeunes et leurs familles

–

L'application FantomApp pour aider les adolescents à se protéger en ligne

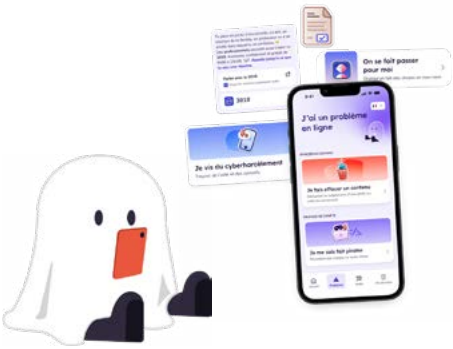
« Protéger les mineurs et leurs données dans l'univers numérique. » C'est l'un des quatre axes du plan stratégique 2025-2028 de la CNIL. Il a trouvé une traduction très concrète en décembre 2025 avec le lancement de l'application gratuite FantomApp destinée aux 10-15 ans et à leurs parents. Objectif : aider à mieux protéger ses données personnelles sur les réseaux sociaux, à connaître ses droits et à trouver facilement de l'aide en cas de problème.

Conçue à partir d'une enquête menée dans plusieurs collèges, l'application a associé des adolescents tout au long de son développement afin de proposer un outil réellement pensé par et pour les jeunes. Les ateliers organisés avec des collégiens ont ainsi permis de structurer FantomApp autour de trois grandes fonctionnalités :

- **des informations claires et des contacts de confiance** pour faire face à des situations problématiques : cyberharcèlement, vol de données ou de comptes, tentatives d'arnaque, chantage sexuel… ;
- **des outils pratiques** pour protéger leur présence en ligne : floutage de photos, test de la robustesse des mots de passe, analyse du niveau de visibilité des pseudonymes ;
- **des tutoriels** pour accompagner les jeunes dans la sécurisation de leurs comptes et la protection de leur vie privée (par exemple : savoir quel paramètre désactiver ou activer).

FantomApp a été financée par l'Union européenne. Ses contenus vont être traduits et adaptés dans plusieurs pays partenaires.

Visualiser FantomApp dans sa version web

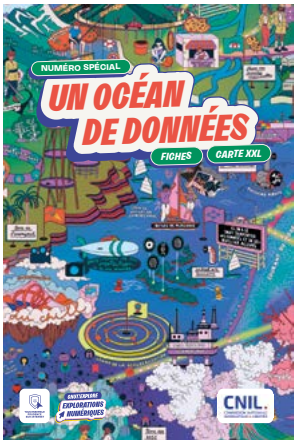


« Un océan de données » pour apprendre à naviguer en toute sécurité

Depuis le mois de mars 2025, la CNIL propose de nouvelles ressources pédagogiques et ludiques destinées aux jeunes de 11 à 15 ans, ainsi qu'aux parents, enseignants et éducateurs. L'enjeu : permettre aux adolescents de mieux appréhender leur environnement numérique et de développer des réflexes pour se protéger. Ces nouveaux contenus sont regroupés dans un dispositif dénommé « Un océan de données » comprenant une carte XXL qui représente l'expérience numérique, des fiches, un livret, un podcast… Ils complètent des ressources déjà disponibles pour les 8-10 ans.

À l'attention des adultes et des enseignants, un livret aborde sept sujets concrets pour mieux accompagner les adolescents dans leur vie numérique : le premier téléphone, la géolocalisation (« suivre ses enfants pour les protéger, c'est gênant ? »), le cyberharcèlement, etc.

Les ressources pour les 11-15 ans



Un « manga » pour susciter chez les 11-15 ans la discussion autour de la vie privée en ligne

La CNIL multiplie les initiatives pour sensibiliser les 11-15 ans à la protection des données personnelles et à la vie privée en ligne. En juin 2025, elle a publié *L'Agence Privacy*, un manga qui aborde sans détour les risques numériques qui concernent les jeunes. Le premier tome suit les aventures de deux enquêteurs chargés d'élucider une affaire mêlant cyberharcèlement, piratage et usurpation d'identité. Scénarisée par Faouzi Boughida et illustrée par Grelin, la version papier du premier tome de *L'Agence Privacy* a été diffusée auprès de tous les collèges de France, du réseau de partenaires institutionnels de la CNIL, ainsi qu'à certaines bibliothèques municipales partenaires. Outil de médiation, le manga est également distribué lors d'actions de sensibilisation réalisées dans les établissements scolaires et lors d'événements auxquels la CNIL participe.

La version numérique du manga

79 %

des enfants ont accès à un téléphone portable avant 11 ans, d'après une enquête CSA pour la CNIL de novembre 2023

Un jeu de cartes pour comprendre pourquoi et comment protéger ses informations

La CNIL a revisité début 2025 le classique jeu de paires consistant à associer des images identiques. Renommé « Données paires-sonnelles », il s'inscrit dans l'univers des données personnelles et des données sensibles pour des parties qui durent une quinzaine de minutes. Accessible à partir de 7 ans, ce jeu est notamment utilisé lors d'actions de sensibilisation sur le terrain, par exemple dans les établissements scolaires pour créer du lien avec les parents et discuter avec eux de la vie numérique de la famille.

Télécharger et imprimer le jeu « Données paires-sonnelles »

Une vidéo pour sensibiliser les parents aux risques de partager des photos de leurs enfants

D'après l'Observatoire de la parentalité et de l'éducation numérique, plus de la moitié des parents français ont déjà partagé sur les réseaux sociaux du contenu sur leurs enfants. Avec un risque réel que ces images soient détournées à des fins malveillantes. La Fondation pour l'Enfance estime ainsi que 50 % des photos ou des vidéos d'enfants échangées sur les forums pédocriminels ont été initialement publiées par leurs parents sur Internet. Face à ce constat, l'autorité irlandaise, la Data Protection Commission (DPC), et la CNIL ont souhaité renforcer la sensibilisation des parents grâce à une vidéo intitulée « Réfléchissez avant de publier ». Elle met en scène une famille abordée dans un centre commercial par des adultes inconnus qui semblent tout connaître de la vie de la fillette. La CNIL en profite pour rappeler sur son site les bons réflexes à adopter.

La vidéo « Réfléchissez avant de publier » et les conseils de la CNIL

53 %

des parents français ont déjà partagé sur les réseaux sociaux du contenu sur leurs enfants.

Source : Observatoire de la parentalité et de l'éducation numérique (OPEN)-POTLOC, 2023

Un fort attrait du public pour les actions et les publications de la CNIL

Sur cnil.fr

Les sites web de la CNIL (cnil.fr et linc.cnil.fr) ont cumulé environ 10,5 millions de visites en 2025, un chiffre en légère baisse par rapport à 2024 (11,6 millions). Cet écart peut s'expliquer en partie par un déplacement, difficilement quantifiable, de demandes vers les agents conversationnels reposant sur des systèmes d'IA, au détriment des requêtes « traditionnelles » sur les moteurs de recherche. Une vigilance reste toutefois nécessaire quant à la fiabilité des informations obtenues par ces nouveaux outils. Malgré l'évolution des pratiques du public, le niveau de fréquentation de cnil.fr reste élevé, notamment sur des sujets d'actualité, ce qui confirme l'intérêt constant des professionnels comme du grand public pour les questions de protection des données.

Les contenus les plus consultés sur cnil.fr

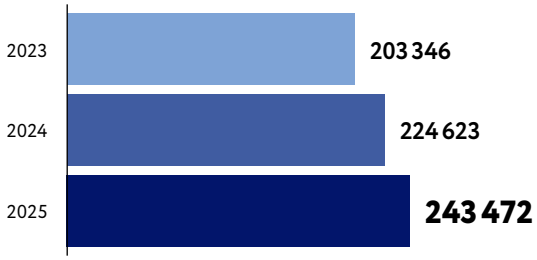
Titre de la publication	Visites uniques
Le règlement général sur la protection des données	**289 456**
Cookies et traceurs : que dit la loi ?	**228 218**
Générer un mot de passe solide	**190 164**
IA : Meta entraînera ses systèmes d'IA avec les données des utilisateurs européens dès fin mai 2025	**157 473**
Adresser une plainte à la CNIL	**146 570**

Sur les réseaux sociaux

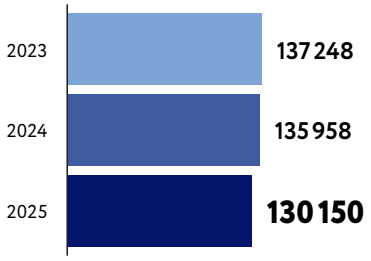
LinkedIn demeure le réseau social le plus plébiscité par le grand public pour suivre la CNIL (+ 8,5 % d'abonnés), devant X et Mastodon. Parmi les communications les plus réussies figure la campagne de prévention sur le partage de vidéos ou photos d'enfants par les parents (ou *sharenting* en anglais), qui a généré 2 500 « j'aime », un millier de reposts et 46 commentaires. Ces chiffres s'ajoutent aux 9,6 millions de téléspectateurs touchés à la télévision. Cette campagne a permis de générer 91 % de visites supplémentaires sur la fiche dédiée sur cnil.fr en l'espace d'une quinzaine de jours.

ÉVOLUTION DU NOMBRE D'ABONNÉS SUR LES RÉSEAUX SOCIAUX

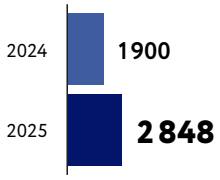
Abonnés LinkedIn



Abonnés X



Abonnés Mastodon

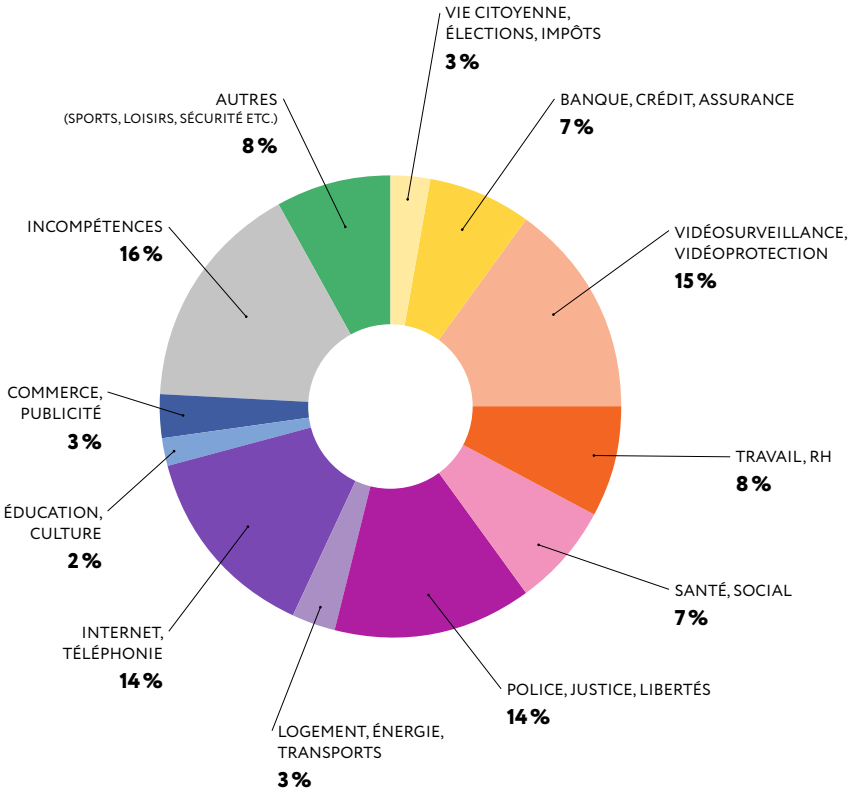


Les principales thématiques des questions adressées à la CNIL

La CNIL a répondu à 35 403 appels et à **18 775** demandes écrites reçues via son formulaire de contact en ligne ou par courrier postal.

Pour chaque demande, la CNIL aide chacun à comprendre ses droits et ses obligations qui peuvent être répartis en plusieurs thématiques.

Entre 2024 et 2025, le nombre de questions concernant les banques, crédits et assurances a baissé de douze points, ce qui s'explique par une diminution des questions liées au fichier des comptes bancaires et assimilés (FICOBA). À l'inverse, les questions relatives à la police, à la justice et aux libertés publiques sont en hausse de six points, en raison d'une augmentation de questions relatives au fichier Schengen (SIS-II).



Le défi permanent de la sécurité des données

LES VIOLATIONS DE DONNÉES ATTEIGNENT UN NIVEAU EXCEPTIONNEL 52

LA CNIL RAPPELLE SES CONSIGNES POUR RENFORCER LA SÉCURITÉ DES GRANDES BASES DE DONNÉES 54

CONFORTER LE CHIFFREMENT DES COMMUNICATIONS COMME SOURCE DE CONFIANCE DANS LES USAGES NUMÉRIQUES 54

ÉDUCATION NATIONALE : DEUX GUIDES PRATIQUES SUR LES VIOLATIONS DE DONNÉES 54

ÉCONOMIE DE LA CYBERSÉCURITÉ ET BÉNÉFICES DU RGPD 55

COMMENT CONCILIER SOLUTIONS DE CYBERSÉCURITÉ ET PROTECTION DES DONNÉES ? 55

PARTICIPATION AU FORUM INCYBER 55

COMMENT SE PROTÉGER FACE À L'HAMEÇONNAGE ? 56

Entretien avec

Fabien Tarissan,

membre du Collège en charge des secteurs de la cybersécurité et technologies innovantes

« Malgré la montée en compétence des acteurs, des failles de sécurité restent récurrentes »

Quelles sont les tendances en matière d'atteinte à la cybersécurité ?

–

Depuis 2018, le nombre de notifications de violations de données est en hausse régulière. Ces violations sont dues pour moitié à des piratages, révélant des failles de sécurité récurrentes et généralisées. Ainsi, malgré une montée en compétence des acteurs au fil des ans, la sécurisation des accès, la gestion des habilitations ou encore l'analyse active de la journalisation restent des éléments critiques.

Par-delà cette indispensable prise de conscience, on observe également la nécessité pour les acteurs de penser une défense en profondeur, afin de ne pas faire reposer toute la sécurité sur quelques éléments renforcés, aussi robustes soient-ils.

Comment la CNIL coopère-t-elle avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ?

–

L'ANSSI est un acteur important pour la CNIL et notre collaboration est étroite depuis des années, que ce soit en matière de sensibilisation, d'accompagnement ou d'élaboration d'outils de droit souple. Toutes les recommandations de la CNIL qui touchent à la sécurité (comme la recommandation sur l'authentification multifacteur ou celle sur le vote électronique par exemple) font ainsi l'objet d'échanges poussés avec l'ANSSI.

Ce lien va naturellement se renforcer avec NIS 2*, mais son articulation avec le RGPD demande un peu de clarification sur nos rôles respectifs, notamment en cas d'incidents de sécurité. Cette coordination est cruciale afin d'assurer la cohérence et la lisibilité pour les acteurs concernés. Elle s'étendra également à la supervision des portefeuilles européens d'identité numérique et de leurs usages, appelés à se déployer dès cette année.

Les violations de données atteignent un niveau exceptionnel

–

Un record a de nouveau été battu en 2025 : la CNIL a été notifiée de **17 802** violations de données personnelles, contre… **5 630** en 2024. Ce chiffre exceptionnel s'explique notamment par des attaques qui ont touché deux éditeurs de solutions, l'un pour les professionnels du conseil patrimonial, l'autre pour les professionnels de santé libéraux. À elles seules, ces deux violations ont entraîné un volume inédit de notifications (11 635) de la part des entreprises clientes, en tant que responsables de traitement, quand bien même il s'agit à l'origine du même incident.

Afin de refléter le plus fidèlement possible la tendance, la CNIL a décidé de ne pas inclure ces deux incidents dans son bilan chiffré. Dans une situation similaire, l'autorité de contrôle néerlandaise a adopté la même approche. Avec cet ajustement, la CNIL s'est vue en définitive notifiée de **6 167** violations en 2025, ce qui représente tout de même une hausse de **9,5 %** par rapport à 2024.

3 tendances qui se confirment

1. Comme les années précédentes, le piratage continue d'être la nature d'incident la plus fréquemment déclarée (50 % en 2025). Cela recouvre le vol de données (depuis un compte utilisateur légitime), le « rançongiciel », l'hameçonnage, le bourrage d'identifiants à partir de couples identifiant/mot de passe volés (*credential stuffing*), etc. Viennent ensuite l'envoi de données personnelles à un mauvais destinataire (13 %), le vol ou la perte de matériel et de données (7 %) et la publication non intentionnelle d'informations (7 %).
2. Certaines attaques relèvent de campagnes ciblées. 2025 a notamment été marquée par une série de vols de données visant les entreprises clientes d'un éditeur de solution de CRM et par une autre ciblant les fédérations sportives.
3. Les violations de données susceptibles de concerner plus d'un million de personnes restent importantes. Il y en a eu une quarantaine en 2025 (une trentaine en 2024).

* En matière de cybersécurité, la directive européenne NIS 2 (*Network and Information Security*) impose des mesures plus strictes de prévention, de gestion des incidents et de coopération entre États membres.

Les 5 secteurs les plus concernés par les violations de données

6 167

violations de données notifiées à la CNIL en 2025

+ 9,5 %

par rapport à 2024

Entretien avec

Johanna Brousse,

vice-procureure en charge de la cybercriminalité au parquet de Paris

« *La CNIL est un partenaire essentiel dans la lutte contre la cybercriminalité* »

Sur quels dossiers intervenez-vous ?

–

Le parquet de Paris dispose d'une compétence nationale concurrente : il peut se saisir de tout dossier de cybercriminalité en France. En pratique, nous intervenons sur les affaires les plus complexes ou stratégiques. Cela concerne notamment les attaques visant des opérateurs d'importance vitale ou des entités sensibles, des dossiers généralement confiés à la DGSI (Direction générale de la sécurité intérieure). Le parquet traite également les attaques par *ransomware* (rançongiciel en français) qui nécessitent une coordination nationale. Autre sujet majeur : les fuites de données, en forte recrudescence. Autrefois, les données volées étaient principalement revendues à des fins d'escroquerie. Désormais, elles sont exploitées par la criminalité organisée pour préparer des infractions plus graves et plus ciblées, en s'en prenant par exemple à des détenteurs de cryptomonnaies. Le parquet traite également les infractions liées aux grandes plateformes, comme TikTok, Telegram, Coco, X…

Comment travaillez-vous avec la CNIL ?

–

La CNIL est un partenaire essentiel. D'abord par ses signalements, lorsqu'une violation de données présente un niveau de gravité significatif. Ces transmissions sont cruciales : certaines organisations hésitent à déposer plainte, alors même que les faits peuvent révéler l'action de groupes structurés. La CNIL apporte également une expertise technique précieuse. Le parquet peut lui adresser des réquisitions afin d'obtenir un éclairage spécialisé sur des questions complexes, notamment dans des dossiers impliquant de grandes plateformes. Enfin, la CNIL est un partenaire de réflexion stratégique. Une problématique actuelle concerne la prise en charge des victimes de fuites de données massives. Lorsqu'un incident concerne des dizaines de millions de personnes, il est matériellement impossible de traiter autant de plaintes individuelles sans engorger les services de police et de justice. Nous menons donc une réflexion commune sur la façon d'adapter les procédures et d'améliorer la prise en charge des victimes.

La CNIL rappelle ses consignes pour renforcer la sécurité des grandes bases de données

Une trentaine en 2024, une quarantaine en 2025… le nombre de violations de données touchant plusieurs millions de personnes s'établit sur des niveaux élevés, concernant à la fois des organismes publics et privés. Face au phénomène, la CNIL a rappelé au printemps 2025 les mesures indispensables pour sécuriser les grandes bases de données. L'occasion de souligner que les attaques reposent souvent sur les mêmes modes opératoires :

- les couples « identifiant + mot de passe » d'utilisateurs légitimes ont été usurpés ;
- une part significative des incidents implique un sous-traitant à la sécurité défaillante ;
- les intrusions n'ont pas été détectées par l'organisme avant la mise en vente ou l'exploitation des jeux de données volés.

En l'absence de mesures de sécurité adéquates, la CNIL peut prononcer une amende allant jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu.

Les grandes mesures à mettre en œuvre :

- sécuriser les accès externes au système d'information via une authentification multifacteur. Près de 80 % des violations de grande ampleur constatées par la CNIL en 2024 ont été permises par l'usurpation d'un compte protégé uniquement par un mot de passe ;
- journaliser, analyser et fixer des limites sur les flux de données qui transitent sur le système d'information ;
- considérer l'humain comme un acteur de la sécurité. Autrement dit, organiser des sensibilisations régulières adaptées aux profils d'utilisateurs (collaborateurs, développeurs, dirigeants, sous-traitants, etc.) ;
- encadrer la sécurité des données avec les sous-traitants.

Le détail des consignes à respecter

Conforter le chiffrement des communications comme source de confiance dans les usages numériques

En 2025, de nombreux débats législatifs ont porté, en France comme en Europe, sur l'accès aux données par les forces de l'ordre dans le cadre de leurs missions (lutte contre la pédocriminalité, le terrorisme, le narcotrafic, etc.). Le développement d'outils de chiffrement efficaces peut limiter les capacités d'investigation des autorités dans l'espace numérique. La CNIL, tout en reconnaissant que ces initiatives législatives poursuivent des objectifs légitimes, a rappelé que les mesures doivent être proportionnées au regard de leur impact sur les personnes. Elle insiste notamment sur le fait que le chiffrement de bout en bout reste un outil essentiel pour garantir la sécurité et la confidentialité des communications électroniques, ainsi que du patrimoine informationnel.

Elle souhaite continuer à assister le législateur dans la recherche de solutions techniquement réalistes permettant de garantir un équilibre entre la sécurité des personnes et le respect de leurs droits fondamentaux.

Éducation nationale : deux guides pratiques sur les violations de données

Inscriptions scolaires, environnement numérique de travail, suivi infirmier des élèves, etc. Les établissements scolaires traitent de nombreuses données personnelles. Pour les aider à réagir rapidement en cas de violations de données et à prévenir ces incidents, la CNIL a publié en mai 2025 deux guides pratiques. L'un s'adresse aux délégués à la protection des données (DPO), l'autre aux directeurs d'école du premier degré, chefs d'établissement du second degré et personnel administratif. Ces guides partent de situations concrètes : vol ou perte de matériel (ordinateur, clé USB, etc.), vol d'identifiants ou de mots de passe, cyberattaques, etc. Et ils livrent les actions à entreprendre rapidement et les bonnes pratiques pour éviter que cela ne se reproduise.

Les guides pratiques pour réagir face aux violations de données

Économie de la cybersécurité et bénéfices du RGPD

Les études économiques sur l'impact du RGPD se concentrent le plus souvent sur les coûts. Dans une étude publiée en juin 2025, la CNIL a choisi de prendre le contrepied et de s'intéresser aux bénéfices du RGPD sous l'angle de la cybersécurité. À titre d'exemple, la seule obligation de révéler aux personnes concernées les fuites de données graves diminue le nombre d'usurpations d'identité. Ce qui aurait permis d'éviter entre 90 et 219 millions d'euros de pertes en France depuis 2018 (entre 585 millions et 1,4 milliard à l'échelle de l'UE). Et ce n'est qu'une faible partie des gains totaux dus au RGPD en matière de réduction du cybercrime.

Les bénéfices du RGPD sous l'angle de la cybersécurité

Comment concilier solutions de cybersécurité et protection des données ?

La CNIL souhaite promouvoir des solutions de cybersécurité conformes au RGPD, tant dans leur usage que dès leur conception. Elle a ainsi publié au printemps une recommandation relative à l'authentification multifacteur (MFA en anglais pour *multi-factor authentication*). Son but est de sécuriser juridiquement les utilisateurs de telles solutions et d'encourager les fournisseurs à intégrer la protection de la vie privée dès la conception de leurs produits ou services. Elle passe en revue les conditions dans lesquelles le recours à la MFA est opportun, le choix des facteurs d'authentification, les modalités de conservation des données, etc.

Dans la même logique, la CNIL a lancé en juillet 2025 une consultation sur un projet de recommandation concernant les passerelles web filtrantes, souvent appelées proxy web filtrant. Ces dispositifs sont utilisés pour contrôler et surveiller les accès Internet en filtrant le contenu web selon des politiques prédéfinies. Ils reposent sur des traitements de données dont la conformité au RGPD doit être assurée.

La recommandation relative à l'authentification multifacteur

Participation au Forum InCyber

Du 1er au 3 avril 2025, la CNIL était présente au Forum InCyber (FIC) à Lille Grand Palais pour répondre aux questions du public et des professionnels. Il s'agit d'un des principaux événements européens sur les questions de sécurité numérique. La présidente de la CNIL, Marie-Laure Denis, est intervenue lors du sommet d'ouverture, traduisant l'importance que la CNIL apporte aux questions de cybersécurité.

Fraude au virement de salaire : de quoi s'agit-il et comment réagir?

La réponse de Célestin,

ingénieur expert au service de l'expertise technologique

« Voici un signalement que la CNIL a reçu. En faisant ses courses, un salarié voit son paiement par carte bleue refusé. Il contacte son conseiller bancaire, qui lui annonce que son salaire n'a pas été versé ce mois-ci, ce qui a mis son compte dans le rouge. Il se tourne alors immédiatement vers les ressources humaines de son entreprise, qui lui répondent que son salaire a bien été versé sur son nouveau compte en banque, conformément à sa demande. Après une enquête interne, il ressort qu'un mail usurpant l'identité du salarié a été envoyé aux RH avec un nouveau RIB pour recevoir le salaire. Trois autres salariés, qui apparaissaient aussi dans le magazine externe de l'entreprise, ont également été victimes de cette fraude. Une fois la crise gérée, de nouvelles procédures ont été mises en place pour sécuriser les demandes de changement de RIB. Il est à noter que ce type d'acte malveillant sera désormais plus ardu, car depuis octobre 2025, la vérification de la concordance entre l'IBAN et le nom du bénéficiaire doit être effectuée par les établissements bancaires. »

L'étude de cas en détail

Comment se protéger face à l'hameçonnage ?

Face à l'augmentation régulière des tentatives d'escroquerie suite à des violations de données, la CNIL a publié plusieurs conseils en 2025 à l'attention du grand public. En mars, elle a ainsi partagé les bonnes pratiques pour se protéger en cas d'hameçonnage (*phishing* en anglais). Cette publication est intervenue à la suite d'une campagne de faux courriels « *Amazon Prime Family* ». Ces messages frauduleux annonçaient l'activation d'un abonnement à 480 € par an, avec un lien pour annuler la souscription. Ce service « *Amazon Prime Family* » n'existait pas, mais face à la peur d'un prélèvement, certains cliquaient sur le lien et livraient leurs données bancaires. En médiatisant cette tentative d'escroquerie, le premier objectif de la CNIL était d'alerter l'opinion et d'inviter à supprimer immédiatement le message.

Les conseils clés pour renforcer sa sécurité face aux tentatives d'hameçonnage

- en cas de doute sur un message reçu, ne cliquez pas sur le lien proposé, mais saisissez vous-même, depuis votre navigateur, l'adresse du site officiel du service pour vous connecter à votre compte ;
- surveillez régulièrement les opérations sur votre compte bancaire et faites opposition si nécessaire. Rapprochez-vous de votre conseiller bancaire habituel en cas de doute ;
- sécurisez l'accès à vos comptes en choisissant des mots de passe solides, en évitant d'utiliser plusieurs fois les mêmes, et en ayant recours à un gestionnaire de mots de passe ;
- partagez l'information : si vous détectez une tentative d'escroquerie, prévenez votre entourage, en particulier les personnes vulnérables.

Si vous avez cliqué sur un courriel frauduleux :

Signalez sans attendre l'escroquerie sur la plateforme 17Cyber ou portez directement plainte auprès de la police ou de la gendarmerie.

L'hameçonnage ou *phishing*, c'est quoi ?

L'hameçonnage ou *phishing* en anglais est une technique frauduleuse pour obtenir des données personnelles, comme un mot de passe ou des coordonnées bancaires. Le fraudeur se fait passer pour un organisme qui vous est familier (banque, administration fiscale, service public…). Vous pouvez, par exemple, recevoir un courriel dans lequel il vous est demandé de « mettre à jour » vos coordonnées bancaires. Cela peut aussi être le SMS d'un livreur vous prévenant que le colis n'entre pas dans votre boîte aux lettres, avec un lien pour récupérer votre commande.

Le développement des coopérations en France, en Europe et à l'international

LES 3 AXES DE LA STRATÉGIE EUROPÉENNE ET INTERNATIONALE DE LA CNIL POUR 2025-2028 58

LES PARTENARIATS QUI ONT MARQUÉ 2025 59

COOPÉRATION EUROPÉENNE : LES GRANDES DÉCISIONS DU CEPD EN 2025 60

INNOVATION RESPONSABLE ET PROTECTION DES MINEURS : DEUX PRIORITÉS POUR LES AUTORITÉS DE PROTECTION DES DONNÉES DU G7 61

LA CNIL ACCUEILLE EN 2026 LA TABLE RONDE DES AUTORITÉS DE PROTECTION DES DONNÉES DU G7 61

Entretien avec

Anne Debet,

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

« Au niveau européen, aider les organismes avec des outils plus clairs et plus accessibles »

Qu'est-ce qui a changé dans les méthodes de travail du Comité européen de la protection des données (CEPD) en 2025 ?

–

Conscient de la complexité croissante du cadre réglementaire, le CEPD a adopté une déclaration à Helsinki, le 3 juillet 2025, pour faciliter la mise en conformité au RGPD – en particulier pour les petites organisations – dans le respect des droits fondamentaux des personnes. Premier objectif : aider les organismes en produisant des outils plus clairs et accessibles, via des lignes directrices plus concises et plus pratiques et des documents prêts à l'emploi (modèle de notification des violations de données, FAQ…). Plusieurs documents visant à mettre en œuvre ces nouvelles orientations ont déjà été adoptés en décembre. Deuxième objectif : renforcer le dialogue avec les parties prenantes (responsables de traitement, société civile, chercheurs…) par l'organisation d'évènements par exemple en décembre 2025 sur l'arrêt *SRB* de la CJUE et en 2026 sur la publicité politique.

Sur quels sujets le CEPD a-t-il travaillé plus particulièrement en 2025 ?

–

La production de documents a été soutenue sur des sujets variés comme la pseudonymisation, la chaîne de blocs ou les achats en ligne. Un effort particulier a été fait pour clarifier le cadre juridique européen face à la multiplication des textes. Le CEPD a ainsi publié une première version des lignes directrices sur l'interaction entre le RGPD et le règlement sur les services numériques (*DSA*), d'une part, et le règlement sur les marchés numériques (*DMA*) d'autre part, en collaboration avec la Commission européenne. Il a également rendu plusieurs avis sur les propositions de règlement omnibus.

Les 3 axes de la stratégie européenne et internationale de la CNIL pour 2025-2028

–

En complément de son plan stratégique 2025-2028, la CNIL a publié le 14 avril 2025 sa stratégie européenne et internationale. Ce document définit une feuille de route pour protéger les données des citoyens dans un environnement numérique globalisé, tout en affirmant le rôle moteur de l'autorité française sur la scène européenne et mondiale.

Cette stratégie se décline ainsi en trois axes majeurs :

1. **Fluidifier la coopération européenne :** Dans un contexte marqué par le déploiement de règlements majeurs (sur l'intelligence artificielle, sur les services numériques et sur les marchés numériques) complétant le RGPD, la CNIL souhaite renforcer la coordination entre régulateurs afin d'assurer une application cohérente du droit de la protection des données. Cette coopération doit notamment faciliter la gestion des dossiers transfrontaliers, améliorer les mécanismes de décision commune et renforcer les actions conjointes entre autorités nationales.
2. **Promouvoir des standards internationaux élevés :** La CNIL entend diffuser à l'international le modèle européen, conciliant standards élevés de protection des données et accompagnement de l'innovation. Elle développera sa participation aux grandes instances internationales. La CNIL veut par ailleurs conserver un lien étroit avec le gouvernement français sur les questions internationales en matière de protection des données personnelles.
3. **Consolider l'influence européenne et internationale de la CNIL :** La CNIL veut maintenir et asseoir sa position comme un acteur clé et influent dans le domaine de la protection des données à l'échelle européenne et internationale. Pour cela, elle se maintiendra à l'avant-garde des développements juridiques, technologiques et économiques liés à la protection des données.

Télécharger l'intégralité du document stratégique

Les partenariats qui ont marqué 2025

Avec l'Arcom et la DGCCRF

Les trois organismes, Arcom, DGCCRF et CNIL, poursuivent leur collaboration pour la mise en œuvre du règlement sur les services numériques (*DSA* – ou *Digital Services Act*). 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. Une convention tripartite facilite la coopération entre les trois acteurs et précise notamment les modalités de partage d'information en cas, par exemple, de plainte d'un utilisateur de plateforme.

Avec le Conseil national des barreaux

Le 17 juillet, le Conseil national des barreaux, qui représente les 76 000 avocats de France, et la CNIL ont renouvelé leur partenariat pour une durée de trois ans. Objectif : mener des actions communes de sensibilisation et de formation à la réglementation sur la protection des données personnelles auprès des avocats, dans un contexte d'essor de l'IA.

Avec la Caisse des Dépôts

Le 1er décembre, la Caisse des Dépôts et la CNIL ont signé une convention destinée à structurer et à renforcer leur coopération autour des enjeux de protection des données personnelles et de l'IA. Cette collaboration permettra d'accompagner les projets numériques portés par la Caisse des Dépôts dans un cadre sécurisé et conforme aux réglementations en vigueur. La convention prévoit entre autres la sensibilisation à la protection des données personnelles des directions et métiers dans les domaines des retraites, de la formation professionnelle et de la lutte contre la fraude aux aides publiques. Un comité de pilotage annuel permettra de suivre l'avancement des actions et de définir de nouveaux axes de collaboration.

Avec l'Autorité de la concurrence

L'Autorité de la concurrence et la CNIL poursuivent leur coopération pour accompagner les nouvelles règles européennes sur l'IA et promouvoir une IA de confiance pour les citoyens et bénéfique pour l'économie française. Les deux organismes se sont notamment retrouvés le 5 mars pour un séminaire commun. Au programme : le fonctionnement concurrentiel du secteur de l'IA générative, la sécurisation juridique de l'entraînement des modèles d'IA, les enjeux économiques des modèles d'affaires de l'IA et de sa chaîne de valeur, etc.

Avec la Direction générale du Trésor

La Direction générale du Trésor et la CNIL ont organisé le 20 mai un événement académique international pour évaluer l'impact économique de l'entrée en vigueur du RGPD. La rencontre a attiré une large audience de professionnels, d'institutionnels et d'universitaires, rassemblant plus de 350 personnes en ligne et une centaine en présentiel.

Avec le Réseau national de coordination de la régulation des services numériques

Le 15 décembre, aux côtés des autres autorités de régulation du numérique (ADLC, ARCEP, ARCOM, ARPE), la CNIL a participé à la deuxième réunion plénière du Réseau national de coordination de la régulation des services numériques (REN), sous la présidence de Rachida Dati, ministre de la Culture, et d'Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique. Les travaux du REN ont été consacrés en 2025 à la protection des mineurs en ligne (dispositifs de contrôle parental, mise en œuvre de la vérification de l'âge en ligne...).

Coopération européenne : les grandes décisions du CEPD en 2025

Clarification sur le recours à la pseudonymisation

Le 17 janvier 2025, le CEPD a adopté et mis en consultation publique des lignes directrices concernant la « pseudonymisation ». Elles apportent des précisions juridiques sur cette pratique consistant à transformer des données personnelles afin qu'elles ne puissent plus être attribuées à une personne spécifique sans information supplémentaire. Les contributions reçues sont en cours d'analyse en vue de l'adoption d'une version finale.

Contrôle de l'âge en ligne dans le respect des droits

Le 12 février, le CEPD a adopté une déclaration sur le contrôle de l'âge en ligne autour de dix principes clés tirés du RGPD, comme le respect des droits, la minimisation des données, etc. Cette déclaration vise à garantir une approche européenne cohérente de la vérification de l'âge en ligne afin de protéger les mineurs tout en respectant les principes de la protection des données.

Blockchain et protection des données

Compte tenu des difficultés que peuvent poser les technologies de chaîne de blocs (*blockchain* en anglais) en matière de protection des données personnelles, notamment concernant le droit de rectification et d'effacement, le CEPD a adopté le 8 avril des lignes directrices pour aider les organisations qui utilisent ces technologies à se conformer au RGPD.

Simplifier la conformité et encourager la coopération

Réuni à Helsinki les 1er et 2 juillet, le CEPD a adopté une déclaration comprenant plusieurs engagements importants. Elle prévoit de nouvelles initiatives visant à faciliter la conformité au RGPD, en particulier pour les petites et moyennes organisations, à renforcer la cohérence des interprétations et à encourager la coopération entre les autorités. Le CEPD s'engage également à améliorer le dialogue avec les parties prenantes pour recenser les domaines nécessitant un soutien ou des éclaircissements supplémentaires.

Premières lignes directrices sur l'interaction entre le RGPD et le *DMA*

Le 7 octobre 2025, le CEPD a approuvé des lignes directrices sur l'interaction entre le RGPD et le règlement sur les marchés numériques (*Digital Markets Act* ou *DMA* en anglais – ce texte vise à réguler les pratiques des plateformes numériques). Il s'agit des premières lignes directrices conjointes du CEPD et de la Commission européenne. Elles clarifient la manière dont les contrôleurs d'accès (*gatekeepers*) peuvent exercer leurs activités en se conformant à la fois au *DMA* et au RGPD.

Le cadre pour imposer la création d'un compte utilisateur en e-commerce

Début décembre, le CEPD a adopté les lignes directrices sur les conditions dans lesquelles il était possible ou non d'imposer la création d'un compte utilisateur sur les sites de commerce en ligne, notamment sous l'angle de la base légale mobilisable. Le CEPD recommande notamment de laisser la possibilité de pouvoir acheter en utilisant un mode « invité ».

Des avis d'adéquation de l'OEB, du Royaume-Uni et du Brésil

L'objectif d'une décision d'adéquation est de permettre le transfert des données personnelles, sans exigence supplémentaire, depuis les organismes européens vers des organismes de pays tiers (hors de l'Union européenne) ou des organisations internationales.

- Le 12 mai, le CEPD a adopté un avis d'adéquation de l'Office européen de brevets (OEB). Il s'agit de la première décision d'adéquation concernant une organisation internationale et non un pays ou un territoire.
- Le 16 octobre, le CEPD a adopté deux avis d'adéquation pour le Royaume-Uni en vertu du RGPD et de la directive « Police-Justice ».
- Le 4 novembre, le CEPD a pris une décision équivalente pour le Brésil.

L'arrêt « *SRB* » en débat

Le 12 décembre, le CEPD a organisé un événement dédié à l'arrêt « SRB » (*Single Resolution Board* ou Comité de résolution unique en français) du 4 septembre 2025 de la Cour de Justice de l'Union européenne (CJUE). Cet arrêt explicite des critères pour établir, au regard du RGPD, si et à quel point des données partagées avec des tiers sont personnelles (permettent l'identification directe ou indirecte d'une personne). Cette décision suscite toutefois des questions pratiques sur la frontière entre données personnelles et anonymes. En parallèle, la proposition de la Commission européenne, au sein du projet de règlement omnibus numérique du 19 novembre 2025, visant à codifier l'arrêt SRB dans le RGPD, a ouvert un débat sur l'évolution du cadre législatif. La CNIL se mobilise avec ses partenaires européens pour trouver un équilibre qui garantisse à la fois la protection effective des droits et des libertés des personnes concernées et la sécurité juridique des organismes.

Le CEPD, c'est quoi ?

Le Comité européen de la protection des données (CEPD) est l'organisme indépendant qui veille à l'application du RGPD dans l'UE. Il rassemble les autorités de contrôle de chaque État membre et se réunit une fois par mois dans le cadre de réunions plénières. Il adopte notamment des documents d'orientations générales (lignes directrices, recommandations) afin de clarifier les dispositions des actes législatifs européens en matière de protection des données. Il peut aussi adopter des décisions contraignantes en cas de litiges.

Suivre l'actualité du CEPD

Innovation responsable et protection des mineurs : deux priorités pour les autorités de protection des données du G7

Les autorités de protection des données des pays du G7 se sont réunies à Ottawa du 17 au 20 juin 2025 sous la présidence du Commissariat à la protection de la vie privée du Canada. La CNIL était représentée à cet événement par sa présidente, Marie-Laure Denis, et par Bertrand du Marais, membre du Collège de la CNIL en charge des questions internationales.

Cet événement a permis l'adoption d'une déclaration finale commune rappelant que la confiance des personnes dans le respect de leurs droits à la protection des données était indispensable à l'adoption des innovations, qu'il s'agisse de nouvelles technologies ou de nouveaux services numériques. Les autorités de protection des données des pays du G7 attirent en particulier l'attention des organisations innovantes sur l'importance de respecter le principe de protection des données dès la conception afin de faciliter la diffusion d'une innovation responsable. Avec une vigilance accrue concernant les mineurs, particulièrement vulnérables dans l'univers numérique.

La CNIL accueille en 2026 la table ronde des autorités de protection des données du G7

La France assure la présidence du G7 en 2026. La CNIL accueillera ainsi les 25 et 26 juin la prochaine édition de la Table ronde des autorités de protection des données du G7 à Paris. La Journée de recherche sur la vie privée (*Privacy Research Day*) se tiendra la veille de l'événement le 24 juin et sera l'occasion de donner la parole aux autorités de protection des données du G7 sur leur stratégie en matière de veille et d'innovation.

Les ressources humaines et financières

UNE GESTION AU PLUS PRÈS DES CRÉDITS ACCORDÉS DANS UN CONTEXTE BUDGÉTAIRE CONTRAINT 63

DES MOYENS À RENFORCER POUR ASSURER LES NOUVELLES MISSIONS 63

LES RESSOURCES HUMAINES 64

Une gestion au plus près des crédits accordés dans un contexte budgétaire contraint

En 2025, le budget alloué à la CNIL s'est élevé à **30 214 068 €** en autorisations d'engagement (AE) et **30 176 406 €** en crédits de paiement (CP) après l'application des réserves de précaution et d'aléas de gestion répartis comme suit :

- **25 988 519 €** pour la masse salariale (titre 2), dont 25 844 € de financement attribué par la Commission européenne pour l'allocation de ressources humaines au développement de FantomApp, une application destinée aux collégiens ;
- **4 225 549 €** en AE et **4 187 887 €** en CP pour les dépenses de fonctionnement, d'investissement et d'intervention (titres 3, 5 et 6) dont :
- 146 454 € de financement attribué par la Commission européenne, pour le recours à des prestations techniques en lien avec l'application FantomApp ;
- 157 662 € en AE et 120 000 € en CP de dotation supplémentaire ont été accordés en toute fin de gestion par le responsable de programme 308 (programme de 9 autorités administratives indépendantes).

La CNIL a poursuivi et accentué ses efforts de maîtrise budgétaire, qui se traduisent par une consommation des dépenses de personnel et du plafond d'emploi de **97 %** chacun.

Concernant les dépenses de fonctionnement, l'exécution est conforme aux prévisions annoncées dans les différents documents budgétaires puisqu'elle est de **106 %** de la dotation initiale en AE et **102 %** de la dotation initiale en CP.

L'exécution réalisée en 2025 confirme la gestion rigoureuse et au plus près des crédits accordés en loi de finance, malgré un contexte budgétaire contraint.

Des moyens à renforcer pour assurer les nouvelles missions

Pour 2025, la notification budgétaire a été inférieure aux besoins opérationnels. La CNIL a ainsi obtenu un schéma d'emplois de **+6 ETP** contre, en première notification, un schéma d'emplois de **+8 ETP**, alors que 10 ETP étaient prévus dans le quinquennat budgétaire pré-arbitré. En 2026, la CNIL n'a obtenu aucune création de postes malgré ses besoins induits par un accroissement de sa charge sur les missions historiques et l'ajout de nouvelles compétences liées à plusieurs règlements européens, notamment en matière d'intelligence artificielle.

S'agissant des dépenses de fonctionnement, la CNIL a recherché de nouveaux financements externes ciblés sur certains projets cruciaux (accessibilité de son système d'information, outils PRIAM et PUBLIK de traitements des plaintes, développement de l'application mobile FantomApp). Elle a ainsi obtenu 348 k€ de cofinancement DINUM sur la période 2024-2026 (accessibilité) et 172 k€ de la Commission européenne (FantomApp). Ces crédits sont fléchés et ne peuvent être utilisés que pour ces projets dont la réalisation est obligatoire et qui sont clairement identifiés dans la demande de cofinancement.

Plus de 87 % du budget de fonctionnement de **4,2 M€** est consacré à des charges incompressibles (frais de fonctionnement courant, actions sociales, formations...), laissant une marge de manœuvre réduite de **500 k€** environ pour financer des projets innovants.

Budget 2025

30,2 M€

dont

26 M€ *pour la masse salariale*

4,2 M€ *pour les dépenses de fonctionnement, d'investissement et d'intervention*

Comme chaque année, la CNIL a fait de nombreux efforts pour optimiser l'utilisation de ses ressources, tout en s'adaptant aux contraintes budgétaires strictes.

Pour autant, elle continue de souligner la nécessité de bénéficier de renforts matériels et humains, indispensables pour accomplir l'ensemble des missions confiées par le Parlement.

BOP CNIL	2025	
	Autorisations d'engagement	Crédits de paiement
Total budget Ouvert	**30 188 224**	**30 188 224**
Budget T2 *donc cofinancement européen projet FantomApp*	**25 988 519** *25 844*	**25 988 519** *25 844*
Budget Hors Titre 2 *donc cofinancement européen projet FantomApp* *dont crédits complémentaires fin de gestion*	**4 225 549** *146 454* *157 662*	**4 187 888** *146 454* *120 000*
Total budget Consommé *Budget T2* *Budget Hors Titre 2*	**29 481 814** *25 292 233* *4 189 581*	**29 304 917** *25 292 233* *4 012 684*
% de consommation/budget ouvert *% de consommation/budget ouvert T2* *% de consommation/budget ouvert HT2*	*98 %* *97 %* *99 %*	*97 %* *97 %* *96 %*

Les ressources humaines

En 2025, la CNIL a bénéficié de 6 créations de postes, portant son effectif à 303 équivalents temps plein travaillé (ETPT).

Renforcement des effectifs

Les nouvelles créations de postes ont notamment permis :

- de renforcer la chaîne répressive (2 postes à la direction de l'exercice des droits et des plaintes et 1 à la direction des contrôles et des sanctions) ;
- de renforcer le filtre cyber (ou anti-arnaque), l'accessibilité et la communication (2 postes au SG) ;
- de renforcer l'information et la sensibilisation du public (1 poste à la direction des relations avec les publics).

Rémunérations et gestion budgétaire

Dans la continuité des actions engagées depuis 2023, la CNIL a confirmé en 2025 son engagement en faveur de l'attractivité des métiers et de la reconnaissance des compétences.

Cette dynamique s'est traduite par une revalorisation des compléments individuels de rémunération (CIR), permettant de reconnaître l'expertise, l'investissement et la performance des agents méritants, en particulier des profils les plus engagés et spécialisés.

Optimisation du plafond d'emplois

Malgré le ralentissement des postes alloués observé depuis 2024, la CNIL a su tirer pleinement parti des marges dégagées par les vacances de postes, liées aux délais de recrutement et au renouvellement naturel des effectifs.

Cette gestion rigoureuse et agile des ressources humaines a permis :

- de renforcer le soutien apporté aux directions métiers, notamment par l'attribution de mois supplémentaires de contrats non permanents ;
- d'atteindre, une fois de plus, le schéma d'emplois prévu et un taux de consommation du plafond d'emplois de 97 %, dans un contexte de fortes tensions sur le marché du travail.

Données sociales

303
postes à fin 2025

Âge moyen
40 ans

59 %
des agents travaillant à la CNIL sont arrivés entre 2020 et 2025

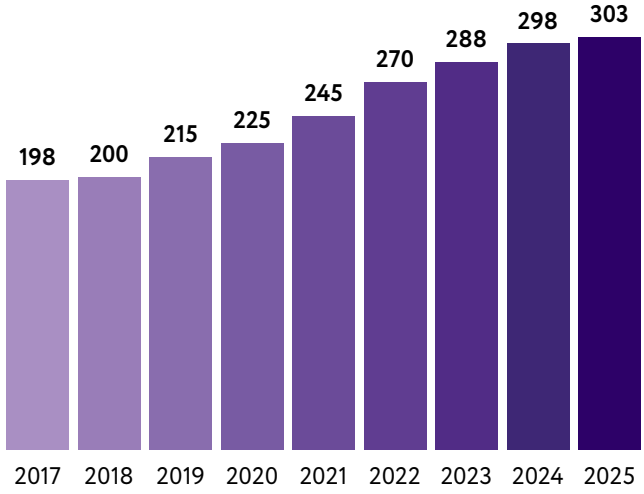
84 %
des agents occupent un poste de catégorie A

62 %
de femmes

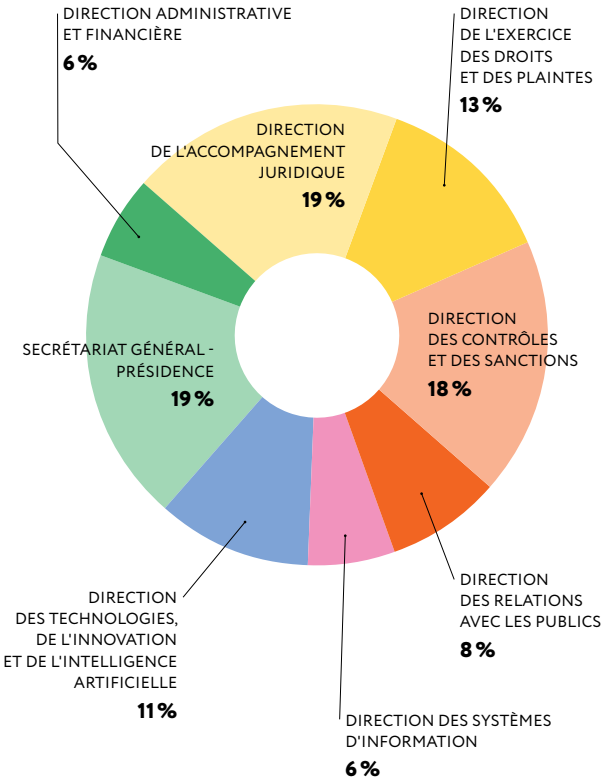
38 %
d'hommes

L'ancienneté moyenne à la CNIL est de
7 ans et 3 mois

ÉVOLUTION DU NOMBRE D'EMPLOIS EN ÉQUIVALENTS TEMPS PLEIN TRAVAILLÉ (ETPT)



RÉPARTITION DES EFFECTIFS AU 31/12/2025



COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS
–
3, PLACE DE FONTENOY
75007 PARIS
TÉL. 01 53 73 22 22

cnil.fr

CNIL
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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