CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

2025-2028

PLAN STRATÉGIQUE

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

www.cnil.fr

AVANT-PROPOS DE LA PRÉSIDENTE

L'essor fulgurant des nouvelles technologies et des services numériques (biométrie, intelligence artificielle, Internet des objets, réalité virtuelle et augmentée, identité numérique, *cloud*, réseaux sociaux) a transformé nos sociétés, ouvrant la voie à une ère dominée par le numérique.

Cette évolution constitue une opportunité considérable pour l'innovation et la croissance, mais repose sur un équilibre délicat entre exploitation des données et respect de la vie privée. Elle soulève également des préoccupations majeures en termes d'éthique.

À cet égard, la CNIL porte la responsabilité particulière de concilier respect des droits fondamentaux et innovation technologique. C'est à cette condition que pourra émerger un cadre de confiance favorisant le développement des usages du numérique.

Dans ce contexte, le Collège de la CNIL a identifié trois sujets au cœur des enjeux numériques et justifiant une attention particulière pour que l'innovation reste au service du citoyen. Ils constituent l'ossature du plan stratégique 2025-2028 de la CNIL.

Le premier concerne l'intelligence artificielle et l'avènement de l'IA générative qui marque une nouvelle révolution numérique. Le second se rapporte à la cybersécurité dans un contexte de multiplication des violations à grande échelle qui renforce l'inquiétude des personnes sur l'usage de leurs données. Le troisième porte sur la protection des plus jeunes face aux risques liés à la surexposition aux écrans.

En complément de son action sur ces trois axes, la CNIL se mobilisera sur deux thématiques prioritaires au centre des usages numériques du quotidien : d'une part, les applications mobiles pour lesquelles un plan d'action a été initié en 2024, et d'autre part, les systèmes d'identité numérique.

La mise en œuvre de ce plan stratégique s'inscrit dans la continuité d'actions entreprises depuis 2019. Il doit permettre, en ce début de mon second mandat, de maintenir une forte dynamique d'adaptation de la CNIL face aux défis posés, pour la protection de la vie privée, par un contexte technologique en très rapide évolution. Le renouvellement de l'action de la CNIL se décline ainsi de trois façons.

Premièrement, dans son organisation. La création d'un service de l'IA et d'une équipe dédiée à l'analyse économique en sont les manifestations les plus évidentes. Le premier devant permettre à la CNIL de mieux appréhender les évolutions de cette technologie, la seconde de mesurer l'impact économique de ses décisions.

Ensuite, dans sa méthode de régulation. La production de droit souple s'effectue en dialogue avec les parties prenantes (concertation, consultations publiques). L'accompagnement des acteurs publics et privés s'inscrit dans une logique de co-construction (accompagnement de projets numériques innovants autour d'une même thématique annuelle, accompagnement semestriel d'organismes). La proximité avec les publics est renforcée par de nombreux déplacements sur le terrain. L'accroissement du nombre et de la variété des mesures répressives favorise les démarches de mise en conformité.

Enfin, dans ses interactions avec les régulateurs d'autres secteurs et d'autres pays. L'application cohérente des nouvelles règlementations européennes (« paquet numérique européen », règlement sur l'IA, directive NIS2) implique de renforcer la coopération. La CNIL se coordonne ainsi avec les autres autorités compétentes à l'échelle nationale (ARCOM, DGCCRF, ANSSI) et européenne, comme elle a déjà l'habitude de le faire au quotidien, en tant que régulateur des données personnelles, avec ses homologues européens et au sein de la communauté internationale de la protection des données.

Je suis convaincue que, forte d'un cap et d'une méthode pour les quatre années à venir, la CNIL contribuera à protéger les données de chacun, pour sécuriser l'avenir numérique de tous.

Marie-Laure DENIS
Présidente de la CNIL

LA CNIL EN BREF

SON RÔLE

Créée par la loi Informatique et Libertés du 6 janvier 1978, le rôle de la Commission nationale de l'informatique et des libertés est de préserver les libertés des citoyens à l'ère du tout-numérique en accompagnant et en contrôlant l'usage des données personnelles contenues dans les fichiers et traitements informatiques ou papier, aussi bien publics que privés.

SES MISSIONS

Informer et protéger les droits
La CNIL répond aux demandes des particuliers et des professionnels et mène différentes actions de communication, que ce soit à travers ses réseaux, les médias, son site web ou en mettant à disposition des outils pédagogiques. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

Accompagner la conformité et conseiller
Afin d'aider les organismes privés et publics à se conformer au RGPD, la CNIL propose une boîte à outils adaptée à leurs tailles et à leurs besoins. La CNIL veille à la recherche de solutions leur permettant de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens.

Anticiper et innover
Pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée, la CNIL assure une veille dédiée. Elle contribue au développement de solutions 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.

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

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »

Article 1er de la loi Informatique et Libertés

SON FONCTIONNEMENT

La CNIL est composée d'un Collège de 18 membres élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent, par le Premier ministre et les présidents du Sénat et de l'Assemblée nationale. Le président de la CNIL est désigné par le président de la République.

Qui compose le Collège de la CNIL ?

- 6 représentants de 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

Ses ressources humaines et financières

298 **agents** en 2024
28M€ de budget en 2024

SES VALEURS

Indépendance : autonomie décisionnelle et pouvoir d'action
Conviction : engagement, dialogue, sens de l'intérêt général
Expertise : compétence, qualité, exigence
Collégialité : collectif, compromis, pluridisciplinarité

CHIFFRES CLÉS

BILAN 2022-2024

377
délibérations

dont 264 avis sur des projets de texte (lois, décrets, etc.)

64
auditions parlementaires

168 283
réponses par téléphone et par écrit

44 977
plaintes traitées

30 035
demandes d'exercice de droits indirect traitées

4 414
demandes de conseils aux professionnels traitées

39
nouveaux guides, référentiels et recommandations

14 385
notifications de violations de données reçues

1 006
contrôles

495
mises en demeure

126
rappels aux obligations légales par la présidente

150
sanctions prononcées pour un montant cumulé de
245 669 800 euros

34M **de visites sur cnil.fr**

CONTEXTE ET ENJEUX

INTELLIGENCE ARTIFICIELLE : ENTRE OPPORTUNITÉS ET DÉFIS

79 % des Français de 18 ans et plus déclarent être inquiets vis-à-vis de l'émergence des IA génératives

62 % considèrent qu'elles constituent un risque important pour la sécurité des données

(source IFOP - 2024)

L'IA s'impose aujourd'hui comme une technologie clé dans de nombreux secteurs (santé, transport, finance, éducation) et les bénéfices qu'elle offre sont incontestables. Cependant, elle présente également des risques significatifs qui touchent à la vie privée (modalités de collecte des données personnelles), à la sécurité (vulnérabilité aux cyberattaques) et à l'éthique (biais algorithmiques).

Certains risques se sont accrus avec l'IA générative qui tend à se généraliser (faux contenus avec les hypertrucages – voix, images, vidéos – risque de manipulation et désinformation sur les réseaux sociaux).

L'intégration de l'IA dans le plan stratégique 2025-2028 s'inscrit dans le prolongement de travaux de fond de la CNIL (fiches pratiques, webinaires, colloques) destinés à clarifier le cadre légal, dialoguer avec l'écosystème et développer des capacités d'audit des systèmes. Elle doit permettre de favoriser une intelligence artificielle respectueuse des droits des personnes et de préparer l'entrée en application du règlement européen sur l'IA.

« Elle doit permettre de favoriser une intelligence artificielle respectueuse des droits des personnes et de préparer l'entrée en application du règlement européen sur l'IA. »

MINEURS ET NUMÉRIQUE : COMPRENDRE LES RISQUES POUR MIEUX PROTÉGER LEURS DONNÉES ET LEUR AVENIR

L'accès généralisé aux smartphones et tablettes, associé à l'essor des réseaux sociaux, des plateformes éducatives et des jeux en ligne font que le numérique est omniprésent dans la vie quotidienne des mineurs. Cette hyperconnectivité, à un âge de plus en plus précoce, s'accompagne de risques majeurs notamment en matière de protection de la vie privée, de sécurité en ligne, de cyberharcèlement et d'exposition à des contenus inadaptés. Les mineurs sont également l'objet de ciblage publicitaire et de profilage ; ils partagent souvent leurs données personnelles sans mesurer les conséquences de leurs choix.

La protection de la vie privée des enfants constitue une priorité absolue justifiant la mobilisation de moyens importants. Pour mettre en œuvre cet axe de son plan stratégique 2025-2028, la CNIL collaborera activement avec tous les acteurs concernés (parents, éducateurs, acteurs publics, entreprises, régulateurs et organisations internationales) pour promouvoir un environnement numérique plus sûr et favorable à leur développement.

67 % des 8-10 ans sont présents sur les réseaux sociaux et 1 famille sur 4 déclare avoir été confrontée au cyberharcèlement

(source Caisse d'Epargne / e-enfance - 2023)

Les jeunes âgés de 7 à 19 ans passent 3h11 sur les écrans chaque jour en moyenne

(source IFOP - CNIL 2024)

CYBERSÉCURITÉ: UNE PRIORITÉ STRATÉGIQUE DANS UN MONDE HYPERCONNECTÉ

« Tous les acteurs, privés ou publics, petits ou grands, et les individus eux-mêmes, sont des cibles. »

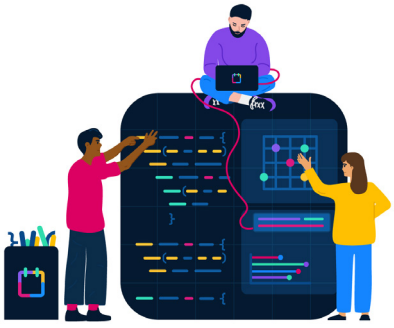
La multiplication des cyberattaques conduisant à des violations massives de données confirme un peu plus chaque mois que la cybersécurité est un enjeu de société. Le paysage de la cybercriminalité évolue avec l'évolution des nouvelles technologies (Internet des objets - IoT, *cloud*, IA, applications mobiles) et les interconnexions entre ces dispositifs augmentent les points de vulnérabilité. De plus, la sophistication croissante des cybermenaces rend les attaques plus difficiles à détecter et à contrer. Tous les acteurs, privés ou publics, petits ou grands, et les individus eux-mêmes, sont des cibles.

Au travers de son nouveau plan stratégique, la CNIL souhaite aider les professionnels et les particuliers à prendre la mesure des risques et à recourir à des solutions et des outils adaptés. Son action se fera en coordination avec les autorités compétentes chargées d'appliquer les réglementations nationales et européennes (NIS2, paquet « cyber ») imposant de nouvelles obligations, notamment pour déceler les attaques et renforcer la résilience face aux cybermenaces.

61 % des français interrogés ont déclaré avoir été victimes d'au moins une attaque durant l'année écoulée : virus informatique, fraude, ordinateur bloqué, piratage de comptes, menaces de diffusion de contenus intimes

67 % des vols de données sont restés indétectés pendant plus de 100 jours

(source IFOP - CNIL 2024)



LES APPLICATIONS MOBILES ET L'IDENTITÉ NUMÉRIQUE AU CŒUR DES USAGES DU QUOTIDIEN

Le service FranceConnect recense plus de 43 millions d'usagers. Plus de 200 000 personnes seraient victimes d'usurpation d'identité en ligne chaque année.

(source ministère de l'Intérieur masecurite.interieur.gouv.fr – 2024)

Compte tenu de l'usage croissant des applications mobiles et des informations particulièrement sensibles auxquelles elles peuvent avoir accès (contacts, géolocalisation, santé), la CNIL a publié des recommandations pour aider les professionnels à concevoir des applications respectueuses de la vie privée. La plan stratégique 2025-2028 sera l'occasion de contrôler la conformité des acteurs et de renforcer la sensibilisation des utilisateurs.

Face à l'augmentation préoccupante des cas d'usurpation d'identité, de cyberattaques et d'hameçonnage, l'usage d'identités numériques est une opportunité pour les entreprises et les pouvoirs publics de favoriser la sécurité de l'identification et de l'authentification en ligne des usagers et d'accroître la confiance dans l'économie numérique. Dans le cadre du plan stratégique 2025-2028, la CNIL veillera à ce que les nouvelles technologies relatives aux identités numériques soient intégrées de manière sécurisée et conformes aux règles de protection des données personnelles.

93,7 % des internautes dans le monde accèdent au web par l'intermédiaire de leur smartphone

(source GWI - 2024).

En 2023, les Français ont téléchargé en moyenne 30 applications par an et utilisé leur téléphone 3h30 par jour

(source Data.ai - 2023)

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

2025-2028

AXE 1

Promouvoir une intelligence artificielle éthique et respectueuse des droits

OBJECTIFS

1. Contribuer au partage de connaissances et d'expertise au sein de l'écosystème de l'IA
2. Clarifier le cadre juridique applicable à l'IA et mettre en œuvre une régulation effective et équilibrée
3. Sensibiliser le grand public aux enjeux de l'IA et le former à l'exercice de ses droits
4. Contrôler la conformité des systèmes d'IA

AXE 2

Protéger les mineurs et leurs données dans l'univers numérique

OBJECTIFS

1. Accroître la présence de la CNIL sur le terrain auprès des enfants, des parents et des prescripteurs
2. Permettre aux mineurs un exercice effectif de leurs droits
3. Promouvoir un usage responsable du numérique au plan national et international
4. Contrôler les opérateurs qui proposent des services en ligne au public mineur

AXE 3

Faire de chacun un acteur de la cybersécurité pour renforcer la confiance dans le numérique

OBJECTIFS

1. Consolider la coopération et la coordination avec l'écosystème de la cybersécurité
2. Accompagner les individus et les organismes face aux violations de données
3. Contribuer au développement de solutions techniques protectrices de la vie privée
4. Renforcer le respect des règles en matière de sécurité par le contrôle et la sanction

AXE 4

Mettre en oeuvre des actions ciblées sur des usages numériques du quotidien

OBJECTIFS

1. Poursuivre la mise en œuvre du plan d'action relatif aux applications mobiles et protéger les utilisateurs
2. Veiller au développement de systèmes d'identité numérique respectueux de la vie privée

AXE 1

PROMOUVOIR UNE INTELLIGENCE ARTIFICIELLE ÉTHIQUE ET RESPECTUEUSE DES DROITS

OBJECTIF 1

Contribuer au partage de connaissances et d'expertise au sein de l'écosystème de l'IA

- Renforcer la capacité de la CNIL à comprendre les avancées technologiques, les usages et les enjeux économiques liés aux systèmes d'IA en s'appuyant sur des partenariats stratégiques (chercheurs, startups, fournisseurs, utilisateurs, institutions et régulateurs) à l'échelle nationale et européenne.
- Promouvoir, au sein d'instances européennes et internationales, l'usage de solutions et de bonnes pratiques en matière de protection de la vie privée dans le domaine de l'IA.
- Participer au processus d'interrégulation avec les autres autorités compétentes pour mettre en œuvre le règlement européen sur l'IA, tant au niveau national qu'européen.

OBJECTIF 2

Clarifier le cadre juridique applicable et mettre en œuvre une régulation effective et équilibrée

- Renforcer la sécurité juridique des acteurs (concepteurs, fournisseurs, utilisateurs) en poursuivant la clarification du cadre légal, notamment par la production d'outils pédagogiques éclairant l'articulation entre le règlement européen sur l'IA et le RGPD.
- Contribuer à l'élaboration de la doctrine en promouvant les positions françaises auprès des instances européennes (CEPD, Bureau européen de l'IA).
- Poursuivre l'accompagnement des projets innovants, tout au long de leur cycle de vie, en encourageant le recours à des technologies émergentes de protection de la vie privée (*Privacy Enhancing Technologies* ou PETs en anglais).

OBJECTIF 3

Sensibiliser le grand public aux enjeux de l'IA et les former à l'exercice de ses droits

- Proposer aux personnes des outils pédagogiques leur permettant de comprendre le fonctionnement des systèmes d'IA, les enjeux dans leur quotidien (vie personnelle / vie professionnelle) et connaître leurs droits.
- Accompagner les personnes dans l'exercice de leurs droits, notamment pour qu'elles obtiennent des explications claires et accessibles sur les décisions prises grâce à des systèmes d'IA.
- Promouvoir les systèmes d'IA vertueux et ayant le recours à des technologies émergentes de protection de la vie privée (*PETs*), notamment par des incitations réputationnelles (*sunshine regulation*).

OBJECTIF 4

Contrôler la conformité des systèmes d'IA

- Concevoir une méthodologie et des outils permettant de contrôler la conformité des systèmes d'IA au cours des différentes étapes de leur cycle de vie.
- Participer à des opérations de contrôles conjointes avec les autorités de protection des données européennes, notamment des solutions de grands modèles de langage.
- Poursuivre les contrôles des dispositifs d'IA utilisés par l'Etat et les collectivités territoriales, en particulier dans le cadre de caméras augmentées.

AXE 2

PROTÉGER LES MINEURS ET LEURS DONNÉES DANS L'UNIVERS NUMÉRIQUE

OBJECTIF 1

Accroître la présence de la CNIL sur le terrain auprès des enfants, parents et prescripteurs

- Renforcer la présence de la CNIL sur l'ensemble du territoire national pour sensibiliser le plus grand nombre aux questions de protection des données personnelles et recenser sur le terrain les besoins.
- Développer les partenariats avec la communauté éducative, les associations, les collectivités locales et les médias dans les territoires.
- Évaluer l'impact des actions d'éducation au numérique mise en œuvre en vue d'orienter les décisions et les productions de la CNIL.

OBJECTIF 2

Permettre aux mineurs un réel exercice de leurs droits

- Informer les mineurs sur leurs droits et les modalités de leur exercice afin d'accroître leur maîtrise de leurs données.
- Accompagner les organismes dans le développement d'interfaces adaptées aux mineurs, contribuant à la transparence du traitement de données personnelles et facilitant l'exercice de leurs droits.
- Adapter le parcours usagers du site web de la CNIL pour faciliter le dépôt de plainte par des mineurs.

OBJECTIF 3

Promouvoir un usage responsable du numérique au plan national et international

- Informer les utilisateurs sur le fonctionnement des services numériques (réseaux sociaux, applications, IA), les risques liés à l'utilisation et les conséquences de leurs choix.
- Élaborer des outils pédagogiques de sensibilisation à la protection des données personnelles coconstruits avec les jeunes pour tenir compte de leurs usages et de leurs besoins.
- Mobiliser les réseaux et partenariats institutionnels nationaux, européens et internationaux, autour d'un projet commun de politique d'éducation au numérique.

OBJECTIF 4

Contrôler les opérateurs qui proposent des services en ligne au public mineur

- Renforcer les contrôles des plateformes utilisées par les mineurs (réseaux sociaux, applications éducatives, jeux vidéos, *EdTech*), notamment sur les modalités de recueil du consentement et le respect des règles en matière de publicité.
- Participer à des actions coordonnées avec d'autres régulateurs concernant ces plateformes afin de mutualiser les informations et les compétences.
- Organiser des contrôles conjoints avec les autorités de protection des données.

AXE 3

FAIRE DE CHACUN UN ACTEUR DE LA CYBERSÉCURITÉ POUR RENFORCER LA CONFIANCE DANS LE NUMÉRIQUE

OBJECTIF 1

Consolider la coopération et la coordination avec l'écosystème de la cybersécurité

- Assurer une application cohérente et harmonisée des nouveaux textes européens (NIS2, DORA, RIA) en matière de cybersécurité, en lien avec les autres régulateurs.
- Collaborer avec les principaux acteurs de l'écosystème afin de concevoir des outils permettant d'augmenter le niveau général de maturité et de protection des organismes.
- Assurer l'intégration d'exigences sur la protection des données personnelles dans les normes et certifications européennes et internationales.

OBJECTIF 2

Accompagner les individus et les organismes face aux violations de données

- Poursuivre la formation et l'accompagnement des organismes pour les aider à se prémunir contre les nouvelles menaces et savoir réagir en cas d'incident.
- Promouvoir, sur le terrain, une culture de la sécurité auprès des personnes pour qu'elles identifient les principaux risques et adoptent les réflexes essentiels.
- Élaborer des ressources pédagogiques adaptées aux besoins et aux moyens des publics cibles (TPE/PME, grandes entreprises, collectivités locales, individus).

OBJECTIF 3

Contribuer au développement de solutions techniques protectrices de la vie privée

- Participer au niveau national, européen et international à l'élaboration de procédés et de solutions technologiques innovants de sécurité.
- Encourager les démarches technologiques favorisant la protection de la vie privée par conception dans tous les usages, notamment les *PETs*.
- Promouvoir les solutions de cybersécurité vertueuses du point de vue de la protection de la vie privée.

OBJECTIF 4

Renforcer le respect des règles applicables en matière de sécurité par le contrôle et la sanction

- Accroître les opérations de contrôle à l'issue de violations de données pour vérifier la mise en œuvre de mesures correctives adaptées.
- Assurer une coordination de l'action répressive (contrôle et sanction) avec les autres autorités compétentes.
- Réévaluer les recommandations de la CNIL en matière de sécurité en s'appuyant sur le bilan des contrôles réalisés et des notifications de violations de données.

AXE 4

METTRE EN ŒUVRE DES ACTIONS CIBLÉES SUR DES USAGES NUMÉRIQUES DU QUOTIDIEN

OBJECTIF 1

Poursuivre la mise en œuvre du plan d'action « applications mobiles » pour protéger la vie privée des personnes

- Sensibiliser le grand public sur les enjeux pour la vie privée liés à l'utilisation des applications mobiles et les informer sur les bonnes pratiques à adopter.
- Contrôler la conformité des applications mobiles et les pratiques des différents acteurs impliqués dans leur déploiement.
- Actualiser les recommandations destinées aux professionnels en s'appuyant sur les enseignements issus des échanges avec l'écosystème, l'analyse des modèles économiques et les contrôles réalisés.

OBJECTIF 2

Veiller au développement de systèmes d'identité numérique respectueux de la vie privée

- Coopérer avec les autorités de contrôle et les homologues européens chargés de l'application du règlement eIDAS et de la mise en œuvre du portefeuille européen d'identité numérique (PEIN).
- Contribuer au développement et à l'usage de solutions de vérification d'identité et de vérification d'âge en ligne protectrices de la vie privée.
- Contrôler les modalités de mise en œuvre des services d'identité numérique auprès des acteurs publics et privés.

Crédit photographique : John Nguyen page 2
Date de publication : janvier 2025

Commission nationale
de l'informatique
et des libertés
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

www.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS