

Rapport annuel : le bilan et les actions marquantes de la CNIL en 2025

18.5.2026 - | Commission Nationale de l'Informatique et des Libertés

Accompagnement des professionnels, contrôle de leurs pratiques, sensibilisation du public, mais aussi régulation de l'IA, cybersécurité et coopération européenne... la CNIL fait le bilan d'une année 2025 intense, au service de la protection des données personnelles et de la vie privée de tous.

Chaque année, la CNIL publie son rapport d'activité pour faire le point sur ses actions autour de ses quatre grandes missions : **informer et protéger** le grand public, **accompagner et conseiller** les professionnels et les pouvoirs publics, **anticiper et innover** pour construire le numérique de demain et, enfin, **contrôler et sanctionner** les manquements aux exigences en matière de protection des données, qui découlent notamment du règlement général sur la protection des données (RGPD).

2025 a notamment été marquée par une **hausse très importante des plaintes reçues**, un **montant total d'amendes inédit**, mais aussi un record de **notifications de violations de données**. En dépit de moyens contraints au regard de l'accroissement de sa charge, la CNIL s'organise et se transforme, notamment pour accompagner l'entrée en application progressive du **règlement sur l'intelligence artificielle (RIA)**.

Elle innove aussi dans les outils qu'elle propose, comme ceux à destination des jeunes et des familles, parmi lesquels l'application FantomApp, dédiée aux adolescents et financée par la Commission européenne.

Accompagnement : une palette d'outils pour tous les professionnels

Pour produire des recommandations proches des pratiques et des attentes des professionnels, 7 consultations publiques ont été lancées en 2025, sur des thématiques variées : véhicules connectés, dossiers médicaux, octroi de crédit, traceurs sur Internet ou encore sur le logement social.

Par ailleurs, la CNIL a publié des fiches pratiques rappelant les règles et bons usages pour de nombreuses situations, par exemple sur l'affichage des [listes scolaires](#) ou l'utilisation de [caméras « augmentées »](#), la [réutilisation de bases de données](#) ainsi que pour [les candidats et partis politiques](#) lors des élections. Elle a aussi accompagné [six projets innovants](#) pour la *silver* économie (économie des seniors) dans le cadre de son « bac à sable ».

En outre, la CNIL a traité **539** demandes d'autorisations en santé (pour des recherches, études ou évaluations qui n'entrent pas dans le cadre d'un de ses référentiels) dont **406** dossiers en recherche en santé.

Enfin, la CNIL a traité **1 351 demandes de conseil** de professionnels et rendu 90 avis sur des projets de loi ou de textes réglementaires, essentiellement à la demande du gouvernement.

Plaintes : une hausse record des sollicitations

2025 a été marquée par un nouveau record de plaintes reçues par la CNIL, qui atteint **20 150**, soit **10 % de plus** qu'en 2024. En cause, notamment, un non-respect de la protection des données et de la vie privée dans le cadre du travail, du commerce, de l'immobilier ou encore sur les réseaux sociaux. Environ 1 900 plaintes concernent aussi directement les violations de données.

La CNIL collabore au quotidien avec les autres autorités de protection des données européennes. Elle a ainsi transmis plus de **230 plaintes transfrontalières** et répondu à **600 sollicitations de ses homologues**.

Contrôles et sanctions : un montant inédit d'amendes

Comme chaque année, la CNIL a conduit des contrôles auprès d'organismes publics et privés, à la suite de plaintes, de signalements, en fonction de l'actualité ou dans le cadre de [ses thématiques de contrôle prioritaires](#). Les sujets sont variés : respect des droits fondamentaux, cybersécurité, dispositifs vidéo, ou encore utilisation de traceurs en ligne.

Au total, la CNIL a mené **323 contrôles** et a rendu 259 décisions, dont **83 sanctions** pour un montant total de près de **487 M€** (perçus par le Trésor public). Si deux sanctions importantes expliquent ce montant total d'un niveau inédit pour l'institution, la CNIL a également prononcé de **nombreuses amendes concernant des entreprises de toutes tailles et de tous secteurs d'activité**, notamment grâce à sa procédure simplifiée mise en place en 2022, qui lui permet d'agir plus vite dans certains cas moins complexes.

En outre, la CNIL participe activement à la régulation au niveau européen grâce à un dialogue soutenu avec ses homologues dans le cadre du [guichet unique](#). Ainsi, en 2025, près de 80 décisions de la CNIL ont été soumises à d'autres autorités européennes, 4 sanctions ont été adoptées en coopération et, en parallèle, la CNIL a examiné 9 projets de décision de ses homologues.

Sensibilisation : une stratégie multicanal pour dialoguer avec tous les publics

Afin d'échanger avec les publics, particulièrement les mineurs, plus vulnérables, la CNIL s'appuie sur de nombreux partenariats avec : Radio France (chronique « Vie numérique, vie privée » sur Radio ICI), France Télévision (clip « Réfléchissez avant de publier »), ou le magazine Geek Junior.

Parallèlement, la CNIL est présente dans de nombreuses manifestations : salon des seniors en mars, festival Hauts-de-Seine Digital Games en avril ou Paris Plage durant l'été... À cela s'ajoutent de nombreuses interventions dans des établissements scolaires. Au total, les **266 actions** menées sur le terrain ont permis de sensibiliser plus de **20 000 personnes** à la protection des données.

2025 a aussi été marquée par le lancement de [l'application FantomApp](#), conçue pour aider les adolescents à se protéger sur les réseaux sociaux.

Enfin, sur l'ensemble de l'année, la CNIL a répondu à **35 403 appels** et à **14 654 demandes d'information écrites**.

La cybersécurité au cœur des préoccupations de la CNIL

Tous les organismes publics ou privés sont concernés par les enjeux de cybersécurité : associations comme entreprises, PME comme multinationales, collectivités comme ministères.

Parmi les **6 167 violations de données** notifiées à la CNIL, **1 incident sur 2** déclaré en 2025 relève d'un piratage, qui demeure la nature d'incident la plus fréquente. Les violations de données peuvent aussi provenir de l'envoi de données personnelles à un mauvais destinataire ou de la perte de matériel.

Face aux menaces, la CNIL agit : les manquements en matière de cybersécurité, en partie responsables de l'augmentation du nombre de plaintes, **constituent un tiers des contrôles** et près de **30 % des sanctions**. Elle travaille également avec l'Agence nationale de la sécurité des systèmes d'information, ainsi qu'avec le parquet « cyber » de Paris pour les suites pénales, notamment dans les cas les plus graves.

"Trois enseignements peuvent être tirés des notifications de violations de données faites à la CNIL en 2025 : personne n'est épargné ; les violations sont de plus en plus massives ; elles impliquent souvent des prestataires."

Marie-Laure Denis, présidente de la CNIL

En 2026, la CNIL consacrera 50 % de ses contrôles et actions répressives aux manquements en matière de cybersécurité

Les deux dernières années ont été marquées par de nombreuses violations de données d'ampleur significative, affectant un nombre considérable de personnes. La CNIL s'est emparée de ce sujet dès les premières alertes, [en tirant des enseignements](#) des violations, en mettant en avant des [préconisations pour sécuriser les grandes bases de données](#) au printemps 2025, mais aussi en faisant de la cybersécurité des collectivités territoriales l'une de ses thématiques prioritaires de contrôle.

Par ailleurs, lorsque cela était justifié, elle a sanctionné les acteurs, [publics](#) et [privés](#), responsables de traitements de données comme [sous-traitants](#), dont les pratiques en matière de sécurité étaient insuffisantes.

Malgré une forte implication, la situation reste très préoccupante et nécessite que la CNIL renforce ses actions.

C'est pourquoi, en 2026, elle consacrera la moitié de ses contrôles et de ses actions répressives à la sécurité des données.

La CNIL vérifiera ainsi le strict respect des exigences en matière de sécurité, tout en continuant à diffuser des messages de sensibilisation et des conseils aux particuliers et aux professionnels, car la sécurité de nos données est l'affaire de tous.

Les contrôles pourront porter sur des organismes concernés par une violation, faisant l'objet de plaintes ou appartenant à des secteurs propices à traiter massivement des données, y compris [sensibles](#) ou [hautement personnelles](#) (données de localisation, données bancaires, fichiers de l'État, etc.).

Ces contrôles s'articuleront avec les autres [thématiques prioritaires définies pour 2026](#).

Pour rappel : La sécurité des données personnelles est une obligation prévue notamment par l'article 32 du RGPD (en complément d'autres textes, comme la directive NIS2 pour certains secteurs critiques). Toutes les mesures adaptées doivent être prises pour limiter les risques : la CNIL met à disposition [un guide dédié](#), [des recommandations officielles et des conseils sur le sujet](#).

De nombreuses actions pour une IA innovante et responsable

Au titre du règlement sur l'intelligence artificielle, la CNIL est déjà désignée comme autorité de contrôle des usages interdits et devrait prochainement être désignée en tant qu'autorité de surveillance du marché pour certains systèmes d'IA à haut risque (par exemple concernant la biométrie, la migration, les usages répressifs, l'emploi ou l'éducation).

Tout en se préparant à ces nouvelles attributions, la CNIL accompagne depuis des années les usages de l'intelligence artificielle dans le respect du RGPD. Ainsi, en 2025, elle a publié [une série de ressources pour concepteurs et développeurs](#), à la suite de consultations publiques, désormais [traduites en anglais](#). Elle a également participé au [Sommet pour l'action sur l'IA du 6 au 11 février](#).

Dans une démarche plus prospective, elle a publié [un outil de traçabilité des modèles d'IA en source ouverte](#) et participe, en coopération avec l'ANSSI, Inria et le PEReN, au projet PANAME : une bibliothèque logicielle permettant de vérifier si un modèle d'IA traite des données personnelles.

Document reference

<https://www.cnil.fr/fr/rapport-annuel-2025>