ASSEMBLÉE NATIONALE

Compte rendu

17e LÉGISLATURE

Mercredi
17 décembre 2025
Séance de 10 heures 30

Compte rendu n° 24

SESSION ORDINAIRE DE 2025-2026

Commission des lois constitutionnelles, de la législation et de l'administration générale de la République

Présidence de M. Florent Boudié, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 10 heures 30.

Présidence de M. Florent Boudié, président.

La Commission auditionne Mme Marie-Laure Denis, présidente de la commission nationale de l'informatique et des libertés (CNIL).

M. le président Florent Boudié. Madame la présidente, j'ai souhaité que la commission des lois puisse vous recevoir aujourd'hui afin d'évoquer les grands enjeux de votre activité, qui concernent au premier chef les compétences de notre commission. Les sujets ne manquent pas, tant l'organe de contrôle que vous présidez apporte une contribution fondamentale à la protection des libertés publiques. Je pense en premier lieu à la protection des données dans un monde numérique qui a pris une place considérable, mais aussi au développement de la vidéoprotection algorithmique. Hier soir dans l'hémicycle, nous avons débattu de l'article 35 du projet de loi relatif à l'organisation des Jeux olympiques et paralympiques de 2030, sujet sur lequel vous êtes autorité d'accompagnement et de contrôle. Plus globalement, la question des outils de lutte contre la criminalité fondée sur les nouvelles technologies est centrale.

La Cnil a publié en janvier dernier son plan stratégique 2025-2028 pour les années à venir, qui comporte trois axes : l'intelligence artificielle (IA), avec la nécessité d'articuler le règlement général sur la protection des données (RGPD) avec le règlement européen sur l'IA; la protection des plus jeunes face aux risques liés à la surexposition aux écrans ; et enfin, la cybersécurité. Tous ces sujets concernent notre commission.

S'agissant des enjeux liés à l'accès et à la sécurité des messages échangés sur les messageries chiffrées, je souhaite vous interroger. Nous avons eu un débat sur ce point dans le cadre de l'examen de la proposition de loi visant à sortir la France du piège du narcotrafic, avec l'insertion de l'article 8 *ter* par le Sénat, que nous avons supprimé ici. Plus récemment, l'article 16 *bis* du projet de loi dit « résilience » a été adopté par la commission spéciale de l'Assemblée nationale. Ce sujet du déchiffrement intéresse particulièrement notre commission, qui a créé un groupe de réflexion dédié qui doit se réunir prochainement. Quelle est votre interprétation du champ d'application potentiel et des effets de cet article 16 *bis* ?

Par ailleurs, l'Assemblée examinera en janvier prochain une proposition de loi visant à interdire l'accès aux réseaux sociaux pour les moins de 15 ans, ce qui va au-delà des recommandations formulées par la Cnil. Quel regard portez-vous sur cette initiative législative ?

Enfin, quel bilan faites-vous de la mise en œuvre du règlement européen sur l'IAengagée il y a dix-huit mois ?

Le ministre de l'Intérieur a annoncé ce matin avoir saisi votre institution concernant la cyberattaque qui a frappé son ministère et, notamment, l'accès au fichier de traitement des antécédents judiciaires. Peut-être pourrez-vous nous éclairer sur cette situation et la mission qui vous a été confiée.

Mme Marie-Laure Denis, présidente de la commission nationale de l'informatique et des libertés (Cnil). Monsieur le président, mesdames et messieurs les députés, je suis honorée d'échanger à nouveau avec la commission des Lois. Je suis

accompagnée de M. Vincent Villette, secrétaire général de la Cnil, et de Mme Chirine Berrichi, notre conseillère pour les affaires parlementaires et institutionnelles.

Il y a presque deux ans, je partageais avec vous le bilan de cinq années de la Cnil et je vous présentais mes ambitions en vue d'un second mandat. Aujourd'hui, je reviendrai sur les accomplissements de la Cnil depuis 2024 dans ses missions traditionnelles, mais aussi sur les défis auxquels elle fait face, notamment concernant la régulation de l'IA. Je remercie les membres du collège de la Cnil, qui compte quatre parlementaires, ainsi que ses agents pour leur implication quotidienne.

Quelques éléments de contexte. La Cnil est une autorité administrative indépendante dont le champ d'intervention couvre tous les secteurs d'activité. C'est un régulateur transversal de la donnée. Son budget est resté stable entre 2024 et 2025, et le nombre de ses agents a peu varié.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 (Digital Services Act ou DSA) qui concerne la transparence des algorithmes, le ciblage publicitaire et le profilage des mineurs, le règlement sur la gouvernance des données (Data Governance Act ou DGA), celui sur l'espace européen des données de santé, ou encore le règlement relatif à la transparence et au ciblage de la publicité à caractère politique. Le plus important en termes d'impact est sans doute le règlement sur l'IA.

Si ces évolutions renforcent le rôle de la Cnil en tant que régulateur central du numérique, elles augmentent aussi considérablement sa charge de travail ainsi que les attentes des entrepreneurs, des administrations et des citoyens. Soyez convaincus que la Cnil fait tout son possible pour y répondre, même si je me dois de partager avec vous ma préoccupation de ne pas pouvoir les satisfaire pleinement en l'absence de moyens supplémentaires.

L'ambition de la Cnil est de mener une régulation équilibrée, entre accompagnement des acteurs et contrôle de leurs pratiques. Son action repose sur quatre piliers.

Le premier pilier est d'accompagner et de conseiller les acteurs privés et publics. Sur la période 2024-2025, la Cnil a été auditionnée 36 fois par le Parlement – 18 fois par l'Assemblée nationale, 16 fois par le Sénat et 2 fois par l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), a répondu à 42 questionnaires parlementaires et a rendu 217 délibérations, dont 145 avis sur des projets de texte. Nous avons également répondu à 2 679 demandes de conseil et traité 1 040 dossiers en santé. Parallèlement, nous avons produit de nombreux guides et recommandations – 13 en tout, notamment sur l'IA, la sécurité informatique et la prospection commerciale. Nous avons poursuivi notre programme d'accompagnement sur mesure concernant des projets innovants via notre « bac à sable », dont le thème pour 2024-2025 est l'économie du grand âge. Nous avons enfin accompagné des entreprises innovantes comme Docaposte ou la Française des Jeux sur le traitement de leurs données personnelles.

Le deuxième pilier concerne les contrôles et les sanctions. Notre philosophie est d'abord d'obtenir la mise en conformité. Au cours des deux dernières années, la Cnil a conduit 628 contrôles, qui ont justifié 550 mesures correctrices, dont 305 mises en demeure et 148 sanctions. Le montant cumulé des amendes prononcées en 2024 et 2025 s'élève à plus de 535 millions d'euros. Depuis l'entrée en vigueur du RGPD en 2018, le montant total des sanctions s'élève à 1,1 milliard d'euros. La réforme législative votée en 2022 nous a permis de mettre en place une procédure de sanction simplifiée, dont la Cnil s'est pleinement emparée : 119 sanctions ont été prononcées depuis son entrée en vigueur.

Le troisième pilier consiste à informer et à protéger le public, en particulier les jeunes. Nous produisons des contenus pédagogiques pour promouvoir auprès des personnes ciblées une meilleure hygiène numérique et l'exercice de leurs droits en matière de données personnelles. Malgré l'absence d'antenne locale, la Cnil a développé depuis quatre ans environ une stratégie pour aller à la rencontre de ces publics en région. En 2025, nous aurons sensibilisé 20 000 personnes directement, dont un quart de mineurs. Sur ces deux années, nous avons mené 414 actions sur tout le territoire et organisé des journées RGPD à Caen, Lille, Nancy, Nantes ou Montpellier. Nous avons également répondu à plus de 33 000 demandes d'information et 37 000 appels téléphoniques. La protection des individus se traduit aussi par l'instruction des plaintes. Nous avons reçu près de 18 000 plaintes en 2024, soit une augmentation de 8 % par rapport à l'année précédente, et ce chiffre a encore augmenté de 28 % en 2025. Avant l'entrée en vigueur du RGPD, c'était plutôt 7 000 plaintes par an. Nous faisons face à des volumes très conséquents de demandes d'exercice du droit d'accès indirect, qui consiste à nous demander de vérifier le contenu d'un fichier dont la consultation directe n'est pas autorisée par la loi, comme les fichiers de police ou de renseignement. En 2024 et 2025, nous avons reçu 31 655 de ces demandes.

Enfin, le quatrième pilier est notre capacité à anticiper les évolutions du numérique. Notre laboratoire d'innovation numérique, le Linc, s'est par exemple associé au pôle d'expertise de la régulation numérique de l'État (Peren) pour travailler sur les hypertrucages et alerter sur les risques d'usurpation d'identité, d'escroquerie ou de désinformation. Depuis 2023, une équipe de trois économistes analyse les modèles d'affaires liés à l'utilisation des données personnelles et mesure l'impact économique de nos choix de régulation.

Je souhaite maintenant faire un point d'étape sur les trois priorités de mon mandat : l'IA, les applications mobiles et la protection des mineurs en ligne.

Sur la première, la Cnil a publié plusieurs fiches pratiques pour aider les organismes à appliquer le RGPD et à anticiper l'application du règlement sur l'intelligence artificielle. Si le Parlement nous désigne comme autorité de surveillance de plusieurs marchés au titre de ce règlement, nous devrons réguler des secteurs d'activité. Nous veillerons à ce que les pratiques interdites, comme la notation sociale ou l'identification biométrique à distance en temps réel, ne soient pas mises en œuvre via des systèmes d'IA. Nous superviserons aussi les systèmes d'IA dits « à haut risque » dans des domaines stratégiques comme la biométrie, l'éducation, l'emploi ou la gestion des contrôles aux frontières. Il sera nécessaire de développer une doctrine du bon usage de l'IA dans tous ces domaines. Il nous reviendra également de contrôler et de sanctionner, le cas échéant, les mauvaises pratiques.

Concernant la régulation des applications mobiles, nous avons mis en œuvre un plan d'envergure comparable à celui sur les *cookies*. Après une phase de concertation avec les parties prenantes et une consultation publique, nous avons publié en avril une mise à jour de nos recommandations pour offrir aux utilisateurs une meilleure maîtrise de leurs données personnelles, mais aussi en vue d'accompagner les professionnels du secteur pour qu'ils puissent intégrer ces exigences dans leur processus de développement de leurs applications mobiles. Nous avons ensuite lancé un programme de contrôle et mené une dizaine d'investigations, dont trois devraient aboutir prochainement à des mesures correctrices.

Enfin, s'agissant de la protection des plus jeunes, nous produisons de nombreux contenus pédagogiques. Après une première campagne destinée aux 8-10 ans, nous avons souhaité nous adresser à des adolescents, particulièrement exposés. Nous avons notamment créé un manga, dont le deuxième tome sortira en 2026, qui aborde de manière ludique la protection

de la vie privée, la cybersécurité et le cyberharcèlement. Grâce à des fonds européens, nous avons développé une application mobile, FantomApp, disponible en ligne depuis hier. Elle permet aux adolescents de générer des mots de passe robustes, de flouter leurs photos de profil ou d'être accompagnés en cas de harcèlement.

Je souhaite également évoquer la menace cyber, qui s'est très fortement intensifiée. Près de 6 000 violations de données nous ont été notifiées en 2024, soit 20 % de plus qu'en 2023, et ce chiffre devrait au moins doubler en 2025. L'intensification de cette menace se reflète aussi dans l'ampleur des violations, qui touche désormais des secteurs de taille importante, dont certains interviennent dans la vie quotidienne des Français – France Travail, certaines fédérations sportives, ou encore des opérateurs de téléphonie. La Cnil conseille les acteurs, sensibilise aux risques et conduit de nombreux contrôles. Ce sujet illustre l'enjeu de la protection des données au quotidien et le rôle de la Cnil pour préserver la confiance des Français dans le numérique, condition du développement de l'innovation.

S'agissant de la violation de données subie par le ministère de l'Intérieur, celui-ci nous a notifié cette violation en indiquant qu'il poursuivait ses investigations pour en déterminer le périmètre précis. Nous attendons une notification complémentaire, ce qui est fréquent, les violations devant être notifiées dans un délai de 72 heures. En attendant, nous échangeons avec le ministère et l'Agence nationale de la sécurité des systèmes d'information (Anssi) pour déterminer les conséquences à en tirer, notamment sur l'information des personnes concernées.

Sur le chiffrement, cette question fait l'objet de débats clivants au niveau national comme européen. Elle nécessite une expertise technique forte. Nous nous efforçons de l'appréhender de façon posée, en mettant en balance les bénéfices attendus et les inconvénients des dispositifs qui fragiliseraient le chiffrement. Il nous semble que le plateau des inconvénients pèse beaucoup plus lourd que celui des bénéfices. Les services régaliens eux-mêmes semblent partagés sur les gains opérationnels tangibles d'une telle mesure, dans la mesure où la population cible, les délinquants aguerris, pourrait aisément la contourner. Il ne s'agirait pas d'une solution miracle. Du côté des inconvénients, force est de constater que les objections sont nombreuses : une atteinte au chiffrement des réseaux de communications électroniques fragiliserait la confidentialité des communications de tous les usagers et pourrait être exploitée par des acteurs malveillants ou des États tiers. Il existe aussi des considérations de faisabilité pratique importantes. Au début de l'année, Apple a par exemple abaissé la sécurité des données sur son *cloud* au Royaume-Uni, en supprimant l'option qui permettait de chiffrer les sauvegardes sur iCloud, suite à des demandes de portes dérobées. Un travail d'analyse approfondi me paraît donc indispensable, et la Cnil se tiendra à votre disposition pour y apporter son expertise.

Concernant l'accès des mineurs de moins de 15 ans aux réseaux sociaux, il n'est pas évident que le RGPD permette de fonder une interdiction systématique, même si l'esprit de ce règlement prévoit déjà qu'en dessous de cet âge, le mineur ne peut consentir seul. Il serait donc logique qu'une telle interdiction soit posée, d'autant que près des deux tiers des 8-10 ans sont aujourd'hui sur les réseaux sociaux. Nous serons à la disposition du Parlement pour apporter notre éclairage. Notre philosophie est de veiller à ce que les enjeux de vie privée soient pris en compte dans le cadre de la vérification de l'âge. C'est d'ailleurs ce à quoi nous avons travaillé avec l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) sur le contrôle de l'âge pour l'accès aux sites pornographiques, et notre laboratoire a apporté son expertise pour l'établissement d'un référentiel de double anonymat : le site pornographique connaît votre âge via un tiers de confiance, mais pas votre identité, et le tiers de confiance connaît votre identité mais pas le site sur lequel vous vous êtes connectés. Nous sommes

convaincus que si les solutions déployées ne sont pas respectueuses de la vie privée, les internautes les contourneront. Nous menons par ailleurs des initiatives de sensibilisation des jeunes, comme l'application FantomApp. Nous avons aussi diffusé une vidéo, en lien avec notre homologue irlandais, sur le « *sharenting* », c'est-à-dire le partage par les parents de photos de leurs enfants sur les réseaux sociaux, sans qu'ils aient en tête les conséquences que cela implique. Il faut savoir que cette pratique nourrit très largement les réseaux de pédocriminalité. C'est aussi faire peser sur les enfants concernés une charge importante en termes de non-droit à l'oubli. Enfin, j'ai signé hier le renouvellement de notre partenariat avec le ministère de l'éducation nationale pour la sensibilisation de la communauté éducative et l'accompagnement du ministère sur les enjeux innovants, notamment les usages de l'intelligence artificielle, puisque 80 % des élèves et 20 % des professeurs utilisent déjà l'IA.

Sur l'intelligence artificielle, l'actualité confirme que nous avons besoin d'une régulation. Cette technologie recèle de nombreuses opportunités, mais elle est aussi porteuse de dérives et d'abus : décisions automatisées sans explicabilité malgré leurs effets considérables, développement de biais, risques pour la santé mentale, en particulier des plus jeunes et des plus vulnérables, ou encore manipulation de l'information. Le règlement européen propose une approche graduée par les risques, en modulant les exigences en fonction de l'importance de ces risques, ce qui nous paraît cohérent pour éviter de faire peser des contraintes excessives sur les usages qui ne posent pas de problèmes. Je m'inscris en faux contre l'idée que la régulation serait la cause du retard européen en matière d'IA. D'une part, cette régulation, dans sa grande majorité, n'est pas encore entrée en application. D'autre part, si l'Europe ne représente que 5 % du capital-risque mondial contre 50 % aux États-Unis ou 40 % en Chine, la régulation n'est sans doute pas le seul facteur à interroger. La défiance d'une partie de nos concitoyens envers ces innovations technologiques est réelle. Certains l'utilisent dans le cadre de leur activité professionnelle mais demeurent inquiets des conséquences de l'IA sur leur emploi ou en matière de vie privée. La meilleure façon de permettre leur déploiement est de lever ces appréhensions par une régulation adaptée, et la Cnil est prête à jouer un rôle de tiers de confiance.

M. le président Florent Boudié. Je donne immédiatement la parole aux différents orateurs inscrits. La parole est à M. Julien Rancoule.

M. Julien Rancoule (RN). Madame la présidente, lors des Jeux olympiques et paralympiques de Paris 2024, une expérimentation de la vidéoprotection augmentée a été mise en œuvre. Le comité d'évaluation a dressé un bilan contrasté, relevant des performances techniques inégales et un nombre parfois élevé de fausses alertes. Si ces constats ne remettent pas en cause le principe de cette technologie, ils soulignent la nécessité d'un perfectionnement technique, d'un encadrement clair et de vérifications humaines systématiques. Le comité n'a relevé aucune atteinte aux exigences constitutionnelles européennes ou légales, mais a appelé à une vigilance particulière.

Par ailleurs, la sécurisation de ces événements repose sur le recours massif à des agents de sécurité privée, qui pourraient être dotés de caméras-piétons.

Dès lors, quels enseignements la Cnil tire-t-elle de l'expérimentation de la vidéoprotection augmentée ? Avez-vous relevé d'éventuelles atteintes ? À quelles conditions une pérennisation de cette technologie pourrait-elle être envisagée ? Enfin, comment la Cnil appréhenderait-elle l'extension du port de caméras-piétons aux agents de sécurité privée ?

M. Guillaume Kasbarian (EPR). Madame la présidente, je souhaite vous interroger sur l'intelligence artificielle. Un projet de désignation des autorités nationales en charge de la

mise en œuvre du règlement européen impliquerait une vingtaine d'entités. Qui fera quoi dans ce dispositif de régulation ?

Dans ce projet, la Cnil devrait veiller au respect des interdictions prévues par le règlement européen sur l'IA, surveiller les usages des systèmes d'IA à haut risque dans l'accès aux services publics et réguler les exceptions à l'interdiction de l'identification biométrique à distance en temps réel. Comment comptez-vous assurer opérationnellement ce rôle si ces missions vous étaient confirmées ?

Enfin, l'IA est un formidable levier de croissance. Comment nous assurer collectivement que la régulation permettra au secteur de se développer en France tout autant, si ce n'est plus, que chez nos voisins, afin de concilier les exigences de régulation et le développement de cette filière essentielle ?

Mme Élisa Martin (LFI-NFP). Madame la présidente, nous avons échangé par courrier à l'automne 2024 au sujet du suivi de l'expérimentation des traitements algorithmiques des images issues de la vidéosurveillance, autorisée par la loi relative aux Jeux olympiques et paralympiques de 2024. Cette question est cruciale alors que le gouvernement cherche à prolonger cette expérimentation jusqu'au 31 décembre 2027.

Vous deviez être destinataire de rapports trimestriels. Est-ce que cela a bien été le cas, et avez-vous jugé ces rapports fiables ? Vous évoquiez la nécessité d'une évaluation rigoureuse, contradictoire et pluridisciplinaire du traitement automatisé des images enregistrées par les dispositifs de vidéosurveillance. Considérez-vous que le rapport Vigouroux correspond à ces caractéristiques ?

Enfin, l'information du public est un élément clé. Or, des manquements ont été constatés, notamment sur les délais. Quel est votre point de vue sur ce sujet ?

Mme Marietta Karamanli (SOC). Madame la présidente, la stratégie 2025-2028 de la Cnil est axée sur l'IA, la protection des mineurs et la cybersécurité.

En matière d'IA, l'un des enjeux est d'éviter que les infrastructures et les connaissances ne soient concentrées entre les mains de quelques géants privés. Quelles sont les orientations de la Cnil, en lien avec le Comité européen de la protection des données (CEPD), sur le sujet de la souveraineté numérique ?

Dans le domaine de la protection des mineurs, notre Assemblée a appelé à une régulation européenne renforcée, en s'appuyant notamment sur le *Digital Services Act*. Comment la Cnil se positionne-t-elle et quelle évolution de la législation soutient-elle ?

Enfin, concernant le projet de simplification dit « omnibus numérique », comment s'assurer que la simplification ne devienne pas une dérégulation ? Je trouve dommageable que l'on veuille réformer un cadre dont on n'a pas encore mesuré toute l'opérationnalité. Comment préserver les principes actuels tout en procédant à des aménagements raisonnables ?

M. Philippe Gosselin (DR). Madame la présidente, je me réjouis de vous retrouver, moi qui ai siégé à la Cnil, qui joue un rôle majeur dans la construction européenne des opérateurs de contrôle.

Mes questions porteront sur trois points.

Premièrement, une part importante des maires et de la population souhaite un positionnement des candidats aux élections municipales sur l'usage de l'IA en matière de sécurité publique. Comment la Cnil entend-elle contribuer à l'élaboration d'un cadre législatif permettant un déploiement sécurisé de ces technologies ?

Deuxièmement, la proposition de règlement européen établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants remet en débat le chiffrement de bout en bout, nécessaire à la sécurité numérique mais parfois perçu comme un obstacle aux enquêtes. Quelle ligne rouge ne devrait pas être franchie sur ce point ?

Enfin, concernant les mineurs et les réseaux sociaux, quelles recommandations la Cnil pourrait-elle formuler pour concilier la protection des mineurs avec le respect des libertés publiques ?

M. Pouria Amirshahi (EcoS). Madame la présidente, au-delà du risque de cyberattaque, un danger plus silencieux mérite notre attention : celui des usages abusifs des fichiers par des personnes pourtant légalement autorisées à y accéder. Plusieurs travaux parlementaires, notamment ceux de la commission d'enquête sénatoriale sur le narcotrafic, ont mis en lumière des détournements de fichiers de police ou judiciaires au profit de réseaux criminels, révélant des failles dans le suivi des habilitations. L'actualité récente, avec la mise en examen de personnels du tribunal judiciaire de Marseille, illustre ce phénomène de corruption de basse intensité aux effets dramatiques.

La Cnil a un rôle déterminant à jouer en tant qu'autorité chargée d'apprécier les conditions d'accès aux données et l'effectivité des mécanismes de contrôle. Lors de l'examen de la proposition de loi visant à sortir la France du piège du narcotrafic, notre groupe avait évoqué plusieurs pistes : un encadrement plus strict des habilitations, un meilleur suivi des consultations et un renforcement des contrôles. Ces leviers vous paraissent-ils pertinents ? Quel renforcement vous semblerait aujourd'hui prioritaire pour garantir un usage loyal et conforme des fichiers sensibles ?

M. Éric Martineau (Dem). Dans un contexte d'augmentation continue des violations de données personnelles, des interrogations subsistent quant à l'effectivité du régime de sanctions. Bien que le RGPD prévoie des sanctions potentiellement dissuasives, celles-ci apparaissent dans les faits relativement peu nombreuses. Pourquoi ces sanctions ne sont-elles pas plus systématiquement prononcées ou renforcées ? Estimez-vous que les moyens juridiques et opérationnels de la Cnil sont adaptés à l'ampleur du phénomène ?

Je souhaite ensuite revenir sur la fuite de données du ministère de l'intérieur, et en particulier sur le fichier des traitements d'antécédents judiciaires. Plusieurs parlementaires, dont mes collègues Philippe Gosselin et Philippe Latombe, ont mis en lumière des problèmes de conformité de ce fichier : manquements à la loi Informatique et Libertés, données insuffisamment mises à jour, base juridique fragile. Quelles mesures prévoyez-vous pour sécuriser ce traitement, garantir sa conformité juridique et prévenir de nouvelles fuites ?

M. Xavier Albertini (HOR). Madame la présidente, la vidéosurveillance algorithmique, expérimentée à l'occasion des Jeux olympiques, repose sur l'analyse automatisée d'images pour détecter des situations prédéfinies, sans recours à la reconnaissance faciale. Cette expérimentation, strictement encadrée, va être prolongée jusqu'en 2027 et on peut se demander légitimement comment concilier durablement l'exigence de sécurité et de préservation de la confiance démocratique face à cette technologie.

Nous avons pu prendre connaissance d'un précédent rapport du 19 juillet 2022 de la Cnil traitant de ce sujet, mais mes questions porteront plus particulièrement sur le bilan, les perspectives et le positionnement de la France par rapport aux stratégies et aux pratiques étrangères. Ma première question porte sur le bilan. Avec le recul dont vous disposez, pouvez-vous nous dire si ces dispositifs ont démontré une utilité réelle et objectivable en matière de prévention des risques et de sécurisation des événements, et si les alertes générées ont été suffisamment pertinentes ?

Ma deuxième question concerne les perspectives. La prolongation de l'expérimentation pose la question des garanties juridiques. Identifiez-vous des points de vigilance qui devraient conditionner toute évolution future de ces dispositifs ?

Enfin, sur la comparaison internationale, comment situez-vous la France par rapport à d'autres démocraties dans l'usage de la vidéosurveillance algorithmique ? Sommes-nous sur une ligne d'équilibre entre efficacité opérationnelle et protection des libertés ?

M. Paul Molac (LIOT). Notre groupe est très attaché aux libertés publiques. Dans un contexte où les technologies numériques deviennent très intrusives, la question du contrôle est essentielle, notamment face aux masses financières phénoménales qui sont en jeu. Les technologies de surveillance progressent souvent plus vite que le cadre démocratique. C'est particulièrement vrai pour les caméras dites augmentées, qui analysent en continu les comportements dans l'espace public, lieu d'exercice des libertés fondamentales. Or, le droit d'opposition consacré par le RGPD ne peut s'exercer dans ce cadre.

Au regard du bilan de l'expérimentation autorisée pour les Jeux de 2024, avez-vous identifié des risques particuliers ou des défaillances de la vidéosurveillance algorithmique ? Quelles garanties effectives existent concernant la suppression rapide des données collectées, et ces garanties sont-elles réellement contrôlables et contrôlées ?

Mme Sophie Ricourt Vaginay (UDR). Madame la présidente, nous avons examiné cette année plusieurs textes importants sur les nouvelles technologies en matière pénale et de sécurité : fichiers de police interconnectés, outils numériques d'enquête, algorithmes de vidéoprotection. Ces outils sont indispensables à l'efficacité des forces de l'ordre, mais les libertés doivent être pleinement garanties.

Comment la Cnil entend-elle faire évoluer ses doctrines pour accompagner ces transformations, afin que la protection des droits fondamentaux ne freine pas l'innovation et l'efficacité opérationnelle ? Concrètement, où placez-vous le curseur entre la protection des libertés individuelles et le besoin pour les forces de l'ordre de disposer de fichiers fiables et rapidement utilisables ?

Un deuxième sujet concerne l'impact territorial de la régulation numérique. Les règles du RGPD sont souvent pensées pour les grandes structures. Leur application dans les petites communes rurales peut être compliquée. Comment la Cnil prend-elle en compte ces réalités locales ? La régulation n'est efficace que si elle est proportionnée, adaptable et connectée aux réalités du terrain.

Mme Monique Griseti (RN). Le nombre de fraudes qui entachent la distribution des prestations sociales demeure effarant. M. Nicolas Grivel, directeur de la Caisse nationale des allocations familiales, a révélé en mai 2025 avoir identifié un montant de 450 millions d'euros de fraude pour l'année 2024, soit une augmentation de 20 % par rapport à 2023. À cela s'ajoute

la problématique des cartes Vitale surnuméraires, à laquelle le gouvernement tente d'apporter des solutions, notamment par le recours à des contrôles biométriques, comme l'indique la réponse à une question écrite de mon collègue Patrice Martin.

Le gouvernement explore donc une première piste pour endiguer les abus que connaît notre système de solidarité. Cependant, une autre technique reste encore trop peu utilisée : le recoupement de données. Les procédures de demande de prestations, leur actualisation ou la déclaration d'une situation nouvelle se font désormais en ligne, générant une masse d'informations administratives qui, bien que liées, ne se recoupent pas ou pas suffisamment. C'est le cas pour le versement des retraites à l'étranger, où le manque de liaison entre nos caisses d'assurance retraite et les administrations étrangères porte préjudice au budget de la Sécurité sociale, et donc à l'argent des Français.

Dans son rapport de 2025 relatif à l'application des lois de financement de la Sécurité sociale, la Cour des comptes s'est intéressée à la fraude aux retraites. Bien que la Caisse nationale d'assurance vieillesse (Cnav) n'avance aucune estimation, la Cour évalue la fraude entre 50 et 90 millions d'euros pour trois pays seulement : l'Algérie, le Maroc et l'Espagne. Elle notait également que l'échange de données entre les administrations étrangères et françaises ne couvrait que la moitié des assurés vivant à l'étranger en 2024.

Dans ce contexte, madame la présidente, si vous étiez saisie de demandes de recoupement de données afin de lutter contre la fraude, la Cnil serait-elle encline à donner son accord pour que les deniers publics ne soient plus versés indûment à des individus qui profitent des failles du système ?

M. Jean-François Coulomme (LFI-NFP). En 2024, la Cnil a été notifiée de près de 6 000 violations de données personnelles, ce qui représente une augmentation de plus de 20 % par rapport à 2023. Vous constatez un changement de nature dans ces violations, avec une recrudescence des atteintes de grande ampleur qui touchent des dizaines de millions de personnes, comme ce fut le cas pour France Travail, les services de plusieurs mairies et, récemment, des bases judiciaires ou administratives. Vous identifiez à ce titre plusieurs failles principales : la compromission des informations de connexion, les défauts de mise à jour laissant perdurer les failles de sécurité, et une part importante de fuites impliquant des sous-traitants.

Face à un constat aussi alarmant, nous proposons plusieurs solutions structurelles qui diminueraient drastiquement les risques de fuite de données massives : instaurer un principe de décentralisation qui limite le stockage des données au même endroit, renforcer le chiffrement des données, accroître les moyens humains en charge du numérique dans les administrations, et recourir à des logiciels libres et en source ouverte permettant une *auditabilité* constante et ne soumettant pas les données personnelles aux Gafam.

Face à ces phénomènes massifs, l'enjeu n'est plus seulement celui du contrôle et des recommandations, par ailleurs nécessaires, mais bien celui des modifications structurelles dans l'usage des outils numériques. En effet, le RGPD est un outil essentiel, mais il doit s'inscrire dans un projet de sobriété numérique qui questionne l'idée même de la collecte des données. Il faut revenir à un principe de non-collecte des données personnelles, limiter les durées de conservation et favoriser le chiffrement.

Votre commission n'a pas la capacité d'absorber une telle charge de contrôle. Il faut donc remettre à plat la manière dont on collecte ces données, en la limitant au strict nécessaire pour le fonctionnement d'un service ou d'une entreprise.

Madame la présidente, que pensez-vous de ces propositions concrètes ? Et n'est-il pas nécessaire, selon vous, d'aborder aujourd'hui la protection des données non plus seulement par le biais de la régulation, mais par celui de la sobriété ?

M. Éric Pauget (LR). J'aborderai avec vous le sujet des polices municipales. Le Parlement sera saisi au début de l'année 2026 d'un projet de loi, dont un certain nombre d'articles vous concernent. Je pense notamment aux caméras-piétons pour les policiers municipaux et les gardes champêtres, à l'utilisation de la vidéosurveillance embarquée sur des drones, et surtout à un article très spécifique sur lequel la Cnil s'est toujours opposée par le passé : la mise à disposition du dispositif de lecture automatisée des plaques d'immatriculation (Lapi) pour les polices municipales.

Un article y est dédié, et je souhaitais connaître votre appréciation sur ces différents points. Nous sommes aujourd'hui dans une situation très paradoxale où l'État finance et encourage les communes à se doter de ce type d'équipements, mais où la Cnil en empêche l'utilisation.

Mme Sandra Regol (EcoS). Vous le releviez dans votre bilan 2024, les violations de données sont non seulement plus fréquentes, mais aussi d'une ampleur inédite. Je souhaite attirer votre attention sur les données d'une mission régalienne particulière : celles contenues dans les fichiers de police et de justice. Vous avez déjà partiellement répondu, mais certains aspects méritent d'être approfondis.

Ces fichiers, comme le traitement des antécédents judiciaires (TAJ) ou le fichier des personnes recherchées (FPR), sont aujourd'hui au cœur du fonctionnement de la police et de la justice. Ils accompagnent les décisions prises à chaque étape de la chaîne pénale et concentrent des informations particulièrement sensibles. Or, un risque de plus en plus préoccupant concerne les atteintes extérieures à la sécurité de ces fichiers. Le ministère de l'Intérieur a confirmé avoir été la cible d'une cyberattaque qualifiée d'« acte très grave », ayant permis l'accès à des données issues de fichiers sensibles. Bien que l'on peine à évaluer l'importance de ce piratage, il constitue une alerte majeure.

Ces attaques informatiques interrogent la capacité de l'État à protéger ces systèmes face à des intrusions relevant de la cybercriminalité ou d'ingérences plus structurées. Les premiers éléments rendus publics indiquent que cette intrusion serait passée par les messageries professionnelles des agents, mettant en lumière non seulement des vulnérabilités techniques, mais aussi des défaillances humaines.

Dans ce contexte, la Cnil joue un rôle central. Vous avez été saisie de cette affaire, en plus des deux enquêtes judiciaire et administrative ouvertes. Le groupe Écologiste et Social se demande donc si, de votre point de vue, le cadre juridique et les pratiques actuelles sont suffisants pour prévenir ce type d'atteintes, ou si vous identifiez au contraire des fragilités appelant à un renforcement des exigences, notamment en matière de sécurisation des systèmes et de prévention des intrusions.

M. Antoine Léaument (LFI-NFP). Ma question, peut-être un peu en décalage avec les précédentes, concerne le répertoire électoral unique (REU). Ce répertoire, qui regroupe les

inscrits sur les listes électorales, a été mis en œuvre avec la loi du 1er août 2016 et a globalement fait ses preuves, sous la forme d'un unique fichier national bien qu'il reste décrit par commune.

Une question se pose avec ce fichier : la possibilité de passer à une inscription automatique sur les listes électorales. C'était la recommandation numéro 9 du rapport que j'ai produit dans le cadre de la commission d'enquête sur l'inscription sur les listes électorales. Les acteurs que nous avons auditionnés nous ont indiqué que c'était possible, mais que cela nécessiterait des croisements de fichiers, notamment via le dispositif FranceConnect.

Par ailleurs, il faudrait pouvoir enrichir le répertoire électoral unique des adresses électroniques et des numéros de téléphone afin de mieux informer les électeurs de l'évolution de leur situation. Je pense notamment aux électeurs qui se trouvent parfois radiés des listes électorales sans en être dûment informés. On a l'impression que la Caf ou les impôts sont tout à fait capables de nous retrouver au fin fond d'un village pour un trop-perçu de 200 euros, mais que l'inscription sur les listes électorales demeure compliquée.

Que pensez-vous d'un tel croisement de fichiers pour permettre à terme une inscription automatique, et de l'alimentation du répertoire électoral unique avec les adresses électroniques et les numéros de téléphone ?

M. le président Florent Boudié. Je vous propose de répondre aux questions de ces différents orateurs, qui ont porté sur des points très divers. Madame la présidente, vous avez la parole.

Mme Marie-Laure Denis. Je m'efforcerai de vous apporter des réponses, en regroupant certaines d'entre elles.

Sur la vidéosurveillance algorithmique, de nombreuses questions ont été posées par MM. Rancoule, Gosselin, Albertini et Molac, dans la perspective des débats que vous avez actuellement pour prolonger l'expérimentation menée lors des Jeux olympiques de 2024. Il faut distinguer la consultation d'images en différé, notamment dans le cadre d'enquêtes judiciaires, de la couche algorithmique en temps réel, conçue pour identifier certains comportements et aider à la décision des forces de l'ordre.

Sur ce sujet, j'ai plusieurs convictions. La première est qu'il ne s'agit pas d'une technologie anodine, même sans reconnaissance faciale. La caméra augmentée, qu'elle soit sur des pylônes ou des drones, amène un changement de degré dans la surveillance, car celle-ci devient permanente, vingt-quatre heures sur vingt-quatre et en temps réel. De plus, sa fiabilité varie grandement selon les cas d'usage : on observe des taux de faux positifs de 50 à 70 % pour des cas d'usage de détection d'armes ou de repérer une personne qui tombe, alors que la technologie s'est montrée plus fiable pour détecter des franchissements de zones interdites ou des véhicules à contresens.

Concernant le bilan de l'expérimentation, je salue le fait qu'une véritable évaluation ait été menée par un comité indépendant, dans lequel la Cnil a désigné deux personnes. C'est assez rare pour être souligné. Ce bilan permet d'affiner la réflexion, tout en gardant à l'esprit le contexte particulier des Jeux olympiques, où la forte présence des forces de l'ordre a pu atténuer l'intérêt de cette technologie.

Ce changement de degré dans la surveillance s'apparente à un changement de nature, car il n'y a plus de limite humaine : elle ne dépend plus du nombre de paires d'yeux qui regardent les écrans.

Ma deuxième conviction est qu'il faut se garder du *solutionnisme* technologique : la caméra augmentée ne résout pas par elle-même les difficultés qu'elle identifie. Il faut examiner de façon posée les cas où elle fonctionne et ceux où elle est moins performante. En tant que garante de la protection de la vie privée, la Cnil cherche toujours à concilier des objectifs légitimes : la sécurité publique et la protection de la vie privée. Il s'agit de trouver le bon curseur. Je constate que certains traitements de données pour les Jeux olympiques étaient moins intrusifs que d'autres. Mesurer la densité ou les mouvements de foule, par exemple, vise une aide à la décision collective et pose moins de problèmes que l'identification d'individus. Il faut sortir d'un débat binaire et s'appuyer sur cette évaluation sérieuse pour concilier ces deux objectifs.

Dès 2019 et à nouveau en 2022, la Cnil a appelé à un débat et rappelé qu'il revenait au législateur de fixer le cadre de cette technologie, avec les garanties appropriées. L'expérimentation des Jeux olympiques en contenait plusieurs : le fait même que ce soit une expérimentation, un bilan obligatoire, l'absence de reconnaissance faciale, l'interdiction de la prise de décision automatisée et de la captation sonore. Cette position de la Cnil est d'ailleurs adossée à la jurisprudence constitutionnelle et à l'analyse du Conseil d'État. Nous serons attentifs, dans le futur texte sur la sécurité du quotidien, à l'enjeu d'une éventuelle généralisation de la vidéosurveillance algorithmique dans les centres de supervision urbains, en examinant sa nécessité et sa proportionnalité.

M. Rancoule a posé une question sur les caméras-piétons. Celles-ci sont déjà largement déployées par la police, la gendarmerie, les gardes champêtres, ainsi que les agents de sécurité de la SNCF et de la RATP. La Cnil ne remet pas en cause leurs finalités – prévention des infractions, collecte de preuves –, mais ses exigences portent sur la doctrine d'emploi, l'information des personnes via un signal visuel, et les droits en aval, notamment un accès limité aux données et une durée de conservation restreinte. Toute extension de leur usage devra être examinée au cas par cas pour éviter une banalisation de cette forme de surveillance.

Mme Élisa Martin (LFI-NFP). Concernant la VSA, avez-vous été destinataire des rapports trimestriels ?

Mme Marie-Laure Denis. Sur la réception des rapports que vous mentionnez, il me semble que nous en avons reçu, mais je ne saurais vous donner le nombre avec certitude. Je m'engage à vous répondre par écrit sur ce point. Quelle était votre deuxième question, madame la députée ?

Mme Élisa Martin (LFI-NFP). Ma question portait sur le caractère rigoureux de l'évaluation : avez-vous considéré que le rapport correspondait aux attentes en matière de rigueur, de procédure contradictoire et de pluridisciplinarité ? Il y avait aussi le fait que vous deviez être informée tous les trois mois, ce dont vous n'étiez plus certaine, et le fait que l'information du public n'a pas fonctionné.

Mme Marie-Laure Denis. L'évaluation a été rigoureuse et pluridisciplinaire, avec des représentants scientifiques et des juristes experts. Concernant l'information du public, j'ai lu dans certains rapports qu'elle était perfectible, car pas toujours compréhensible ou visible. La Cnil, au-delà de ses avis en amont, a reçu une vingtaine de plaintes et a réalisé une dizaine de

contrôles durant les Jeux olympiques, notamment sur les QR codes d'accès aux sites et sur la vidéosurveillance algorithmique elle-même, à la fois sur les traitements de données mis en œuvre par le ministère de l'Intérieur mais aussi auprès des opérateurs de transports publics. Nous avons également réalisé des contrôles *ex-post*. Nous n'avons pas constaté de manquement : les traitements de données étaient conformes à la loi, sans détournement des cas d'usage prévus et avec une suppression des données récoltées.

Concernant l'IA, et pour répondre aux questions sur la répartition des compétences, la complexité du paysage réglementaire n'est pas étonnante pour les régulateurs du marché. En matière de surveillance des marchés, comme c'est une forme de régulation par produits, de même qu'il y a un régulateur pour la mise sur le marché des médicaments ou des jouets. C'est la même logique ici. La Cnil veillera à l'interdiction des systèmes proscrits par le règlement européen, comme la notation sociale ou l'analyse des émotions (sauf dans certains cas précis pour les médicaments notamment). Pour les systèmes à haut risque, la Cnil devrait être l'autorité de surveillance de marché pour la plupart des secteurs, soit seule, soit en lien avec, par exemple, la Direction générale de la consommation et de la répression des fraudes (DGCCRF) sur des sujets qui peuvent être liés au secteur du travail ou avec l'Arcom sur la surveillance des processus démocratiques, par exemple. Et puis, il y a des instances de coordination aussi qui sont prévues.

Notre philosophie n'est pas de freiner l'innovation, mais de l'accompagner avec les garanties nécessaires. J'ai parlé de l'IA de l'ombre, le fait qu'une entreprise, une administration peut voir ces données divulguées parce qu'un de ses salariés a utilisé un agent d'IA dont il ne s'est pas assuré de la sécurité.

Nous disposons d'une expertise, notamment grâce à notre service dédié à l'IA : la preuve en est, nous avons accompagné, à la demande du Parlement, les fournisseurs d'algorithmes pour les Jeux olympiques. A ce stade, avec une approche graduée par les risques, je ne vois pas de risque de surtransposition, et je ne crois pas que la réglementation européenne soit la cause d'un retard de l'Europe en matière d'IA.

La question de la souveraineté numérique est essentielle. Nous devons analyser nos dépendances technologiques, il y en a nécessairement, et il faut identifier celles que nous sommes prêts à accepter, auprès de quels acteurs et dans quelles proportions. Le contexte géopolitique aide maintenant davantage à valoriser le discours de la Cnil sur ces enjeux. Les entreprises deviennent très facilement captives de ces acteurs étrangers, et il est difficile de sortir de certains contrats. C'est vraiment une réflexion générale qui nous inspire sur tous les pans de notre activité. La Cnil a joué son rôle en rappelant que les données de santé des Français, par exemple, ne devaient pas hébergées, via la plateforme nationale des données de santé, par un hébergeur extra-européen et auquel ont accès les services de renseignement d'un État étranger.

Sur les projets européens de textes de simplification dits « Omnibus », nous ne sommes pas hostiles par principe à l'idée d'ajuster le RGPD, notamment vu la multiplication des textes européens dans le domaine du numérique. Le comité européen de protection des données rendra un avis au début de l'année prochaine sur ces textes, et c'est à ce moment-là que la Cnil fera valoir ses points d'alerte et ses lignes rouges. Mais il faut se garder de trois écueils dans l'adoption de ces textes : ne pas céder aux critiques étrangères parfois véhémentes en détricotant notre régulation, comme si ça allait faire apparaître magiquement des champions européens. Au contraire, les actions des régulateurs sont souvent conçues pour préserver les choix des utilisateurs, comme pour les *cookies* par exemple, et tout ce qui atténue ces actions limite les

capacités qu'ont les individus de contrôler leurs données et renforce *de facto* les très grands acteurs du numérique. Donc les véritables leviers sont à mon sens ailleurs. Pour vous donner une idée, le montant des sanctions prononcées par l'ensemble des Cnil européennes s'élève à 5,6 milliards d'euros sur les sept dernières années sur le seul fondement du RGPD et des injonctions. L'objectif n'est pas uniquement de délivrer des amendes mais bien que les traitements changent. A titre d'exemple, lorsque Meta utilise les données sur certains de ses services pour entraîner son IA, elle propose un formulaire d'opposition et en informe ses utilisateurs : si c'est le cas, c'est bien suite à un bras de fer avec l'entreprise en mettant en avant le marché de 450 millions de consommateurs dont elle se priverait si elle ne respectait pas le RGPD. Le marché européen constitue 25 % des revenus des Gafam, et je pense donc qu'il ne faut pas se priver de dire les règles auxquelles nous tenons.

Il faut aussi veiller à préserver la prévisibilité du cadre juridique, et ne pas restreindre les notions cardinales du RGPD comme la définition des données personnelles ou le droit d'accès. Je vous renvoie d'ailleurs à un article récent publié par la professeure américaine Anu Bradford sur « l'effet Bruxelles », autrement dit comment l'Union européenne influence les normes applicables au-delà de ses frontières.

S'agissant de la mise en œuvre du règlement sur les services numériques, la Cnil n'est pas la principale autorité compétence mais elle intervient dans le cadre d'une convention tripartite aux côtés de l'Arcom et de la DGCCRF.

Sur la question de l'accès des mineurs aux réseaux sociaux, je fonde des espoirs dans le *wallet* européen qui devrait, à partir de la fin de l'année 2026, permettre d'identifier plus facilement l'âge des mineurs.

Concernant l'accès abusif à des fichiers régaliens, c'est l'une de nos préoccupations majeures, systématiquement abordée dans nos avis et contrôles. Nous avons adopté une recommandation sur la journalisation pour repérer les extractions de données anormales. Nous menons des contrôles réguliers, par exemple sur une vingtaine de traitements du ministère de l'Intérieur l'an dernier ou actuellement au sein de l'administration pénitentiaire.

Indépendamment de l'augmentation du nombre de violations de données – + 20 % – nous sommes préoccupés par l'augmentation du nombre de personnes concernées. La plupart d'entre nous ont des données personnelles susceptibles d'être croisées par des cybercriminels, et c'est la voie à des tentatives d'hameçonnage et d'usurpation d'identité. Pour les entreprises, c'est aussi le risque de devoir cesser leur activité. On l'a vu avec Jaguar en Angleterre, avec Air France, France Travail, des fédérations françaises de sport, des logiciels concernant des laboratoires médicaux, des médecins, etc. Il en résulte des répercussions concrètes fortes, on l'a constaté pour la Fédération française de tir, victime de cambriolages à la suite de la violation de ses données. Il ne faut vraiment pas minimiser les conséquences de ces sujets. D'ailleurs, le sujet de la cybersécurité représente l'un des axes stratégiques de la Cnil pour la période 2025-2028.

Nous agissons en amont, en imposant par exemple l'authentification multifacteur pour les accès à distance aux grandes bases de données dès le 1er janvier 2026. Nous estimons que 80 % des grandes violations de 2024 auraient pu être évitées avec cette mesure. Nous agissons aussi pendant les violations, en apportant des conseils de premier niveau aux personnes, aux sociétés, aux administrations qui nous notifient une violation de données, en tout cas pour celles qui ne sont pas en lien avec l'Anssi. Nous transmettons, le cas échéant, ces informations au parquet compétent. Enfin, nous sanctionnons : 15 % des sanctions prononcées par la Cnil qui

comportent au moins un manquement à des obligations de sécurité et six dossiers importants de manquement à la sécurité ont été transmis à notre formation restreinte pour des décisions attendues au premier semestre 2026.

Pour la lutte contre la fraude sociale ou fiscale, nous cherchons à concilier cet objectif de valeur constitutionnelle avec la protection de la vie privée. Notre principal point de vigilance est d'éviter toute décision purement automatisée, qui pourrait entraîner des discriminations, comme l'a montré un scandale aux Pays-Bas sur des fraudes supposées aux prestations sociales, alors que les algorithmes étaient biaisés.

Nous accompagnons les collectivités territoriales dans leur mise en conformité, notamment sur la cybersécurité, via des contenus dédiés et des partenariats. La Cnil participe par exemple, chaque année, au salon des maires et elle dispose d'un service dédié à l'accompagnement des délégués à la protection des données qui sont naturellement tournés vers les collectivités.

Concernant les dispositifs Lapi, notre site détaille les conditions dans lesquelles les collectivités peuvent financer ces dispositifs, pour la répression ou la prévention d'infractions, via des conventions de prestations de matériel passées avec le ministère de l'Intérieur Aucune opération de traitement de données au bénéfice de la collectivité ne doit être réalisée et aucun accès aux données du dispositif Lapi par la police municipale ne doit être permis. Les collectivités peuvent également utiliser ces dispositifs pour le contrôle du stationnement payant.

S'agissant du fichier du TAJ, notre formation restreinte a prononcé il y a un an un rappel à l'ordre avec une injonction de mise à jour, notamment sur l'exactitude des données. Ce rappel a été adressé à la fois aux ministères de l'Intérieur et de la Justice. Nous contrôlerons à nouveau le respect de ces injonctions à l'issue du délai imparti.

Enfin, sur le répertoire électoral unique, la Cnil n'est pas opposée par principe à l'interconnexion de fichiers. Nous examinons chaque projet au cas par cas. Je n'ai pas d'éléments précis sur ce dossier, mais je m'engage à revenir vers vous. Nous sommes très attentifs au sujet des élections et avons récemment rappelé aux partis politiques leurs obligations en matière de transparence de la publicité politique, et notamment le règlement européen sur la transparence de la vie publique qui exclut la collecte indirecte des données des personnes auxquelles est adressée cette publicité.

M. le président Florent Boudié. Je vous remercie, madame la présidente, pour la précision de vos réponses. Nous avons une réunion de commission au titre de l'article 88 immédiatement après votre audition.

*

* *

Puis, la Commission examine, en application de l'article 88 du Règlement, des amendements à la proposition de loi, adoptée avec modifications par le Sénat en deuxième lecture, portant reconnaissance par la Nation et réparation des préjudices subis par les personnes condamnées pour homosexualité entre 1942 et 1982 (n° 2243) (M. Hervé Saulignac, rapporteur).

Les amendements qui n'ont pas été examinés lors de la réunion tenue en application de l'article 86 du Règlement ont été repoussés.

*

* *

Puis, la Commission examine, en application de l'article 88 du Règlement, des amendements à la proposition de loi, adoptée par le Sénat, visant à reconnaître le préjudice subi par les personnes condamnées sur le fondement de la législation pénalisant l'avortement, et par toutes les femmes, avant la loi n° 75-17 du 17 janvier 1975 relative à l'interruption volontaire de grossesse (n° 2244) (M. Guillaume Gouffier Valente et Mme Marietta Karamanli, rapporteurs).

Les amendements qui n'ont pas été examinés lors de la réunion tenue en application de l'article 86 du Règlement ont été repoussés.

*

* *

La séance est levée à 12 heures 40.

Informations relatives à la Commission

La Commission a *désigné :*

- *M. Vincent Caure,* rapporteur sur la recevabilité de la proposition de résolution de Mme Elsa Faucillon tendant à la création d'une commission d'enquête relative aux conséquences des accords du Touquet sur l'action publique et le respect des libertés et droits fondamentaux des personnes migrantes (n° 2150) ;

- *Mme Caroline Yadan,* rapporteure sur la proposition de loi de Mme Caroline Yadan et plusieurs de ses collègues visant à lutter contre les formes renouvelées de l'antisémitisme (n° 575) ;

- *M. Christian Baptiste,* rapporteur sur la proposition de résolution de M. Christian Baptiste et plusieurs de ses collègues tendant à la création d'une commission d'enquête sur le traitement judiciaire des violences sexuelles incestueuses parentales commises contre les enfants et la situation des parents protecteurs, notamment des mères protectrices (n° 1977 rect.) ;

- *M. Paul Christophe et Mme Marie-Charlotte Garin,* rapporteurs sur la proposition de loi de M. Paul Christophe et plusieurs de ses collègues visant à mettre fin au devoir conjugal (n° 2175).

La Commission a *créé* :

- une mission d'information sur l'utilisation des financements publics par les associations impliquées dans l'accompagnement et la défense des personnes migrantes, composée de *M. Éric Martineau (Dem) et Mme Sophie Ricourt Vaginay (UDR), rapporteurs* ;

- une mission d'information sur l'évaluation de la mise en œuvre de la loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, composée de 22 membres (5 RN, 3 EPR, 3 LFI, 3 Soc, 2 DR, 1 EcoS, 1 Dem, 1 Hor, 1 LIOT, 1 GDR et 1 UDR). Elle a *désigné* comme rapporteurs *MM. Vincent Caure (EPR), Éric Pauget (DR) et Roger Vicot (Soc).*

Membres présents ou excusés

Présents. - M. Xavier Albertini, Mme Marie-José Allemand, M. Pouria Amirshahi, Mme Léa Balage El Mariky, M. Christian Baptiste, M. Ugo Bernalicis, M. Philippe Bonnecarrère, M. Florent Boudié, Mme Blandine Brocard, M. Vincent Caure, M. Paul Christophe, M. Paul Christophle, M. Jean-François Coulomme, M. Olivier Falorni, Mme Elsa Faucillon, Mme Agnès Firmin Le Bodo, Mme Marie-Charlotte Garin, M. Jonathan Gery, M. Yoann Gillet, M. Philippe Gosselin, M. Guillaume Gouffier Valente, Mme Monique Griseti, Mme Justine Gruet, M. Jordan Guitton, M. Harold Huwart, M. Sébastien Huyghe, Mme Sylvie Josserand, Mme Marietta Karamanli, M. Guillaume Kasbarian, M. Antoine Léaument, Mme Élisabeth de Maistre, M. Éric Martineau, Mme Élisa Martin, M. Ludovic Mendes, M. Paul Molac, M. Jean Moulliere, Mme Danièle Obono, M. Éric Pauget, Mme Lisette Pollet, M. Thomas Portes, M. Julien Rancoule, Mme Sandra Regol, Mme Sophie Ricourt Vaginay, Mme Andrée Taurinya, M. Michaël Taverne, Mme Céline Thiébault-Martinez, M. Roger Vicot, Mme Caroline Yadan

Excusés. - M. Gabriel Attal, Mme Émilie Bonnivard, M. Ian Boucard, Mme Colette Capdevielle, M. Thomas Cazenave, Mme Émeline K/Bidi, M. Philippe Latombe, Mme Marie- France Lorho, M. Stéphane Mazars, Mme Véronique Riotton, M. Hervé Saulignac, M. Philippe Schreck, M. Antoine Villedieu