ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

– Audition, ouverte à la presse, de Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (Cnil), M. Thomas Dautieu, directeur de l'accompagnement juridique, et M. Florent Della Valle, chef du service de l'expertise technologique..... 2

– Présences en réunion..... 21

Mercredi
15 avril 2026
Séance de 17 heures

Compte rendu n° 27

SESSION ORDINAIRE DE 2025-2026

Présidence de
Mme Sophie-Laurence Roy, vice-présidente

ASSEMBLÉE NATIONALE

La séance est ouverte à dix sept heures cinq.

Mme Sophie-Laurence Roy, présidente. Je souhaite la bienvenue à Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (Cnil), accompagnée de M. Thomas Dautieu, directeur de l'accompagnement juridique, de M. Florent Della Valle, chef du service de l'expertise technologique, ainsi que de Mme Chirine Berrechi, conseillère pour les questions parlementaires et institutionnelles. Je précise que je remplace Philippe Latombe, qui a préféré ne pas exercer ses fonctions de président pendant cette audition, car il est lui-même membre de la Cnil.

Je vous remercie de nous déclarer au préalable tout autre intérêt public ou privé de nature à influencer vos déclarations.

L'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter serment de dire la vérité, toute la vérité, rien que la vérité.

(Mme Marie-Laure Denis, M. Thomas Dautieu, M. Florent Della Valle et Mme Chirine Berrechi prêtent successivement serment.)

Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (Cnil). Je vous remercie de votre intérêt pour les travaux de la Commission nationale de l'informatique et des libertés, qui pourront, je l'espère, éclairer cette commission d'enquête.

Permettez-moi tout d'abord de souligner que les questions liées aux dépendances structurelles et aux vulnérabilités systémiques dans le secteur du numérique reviennent de plus en plus dans les sollicitations adressées à la Cnil. Elles émanent des médias, des entreprises, des administrations et renvoient souvent à la sécurité des données ou à l'encadrement contractuel des relations avec un prestataire. Cette tendance s'explique notamment par certaines déclarations et positions de l'administration américaine qui remettent en question les équilibres dans les relations avec l'Union européenne, en particulier dans la régulation du secteur numérique. Ce n'est pas une nouveauté : ces inquiétudes s'expriment régulièrement sans pour autant entraîner un changement significatif des pratiques des administrations et des acteurs économiques.

Une première prise de conscience a eu lieu avec les révélations d'Edward Snowden en 2013 et l'affaire Cambridge Analytica en 2018. A été alors mis en lumière le fait que les géants du numérique disposaient de pans entiers de notre vie privée, mais également que nos données étaient massivement exploitées à notre insu, au détriment de nos intérêts et de nos droits.

Un autre moment important a été l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 16 juillet 2020, dit Schrems II, qui a invalidé la décision d'adéquation de la Commission européenne à l'égard des États-Unis. En considérant que la législation américaine portait une atteinte disproportionnée à la vie privée des Européens, la Cour a remis en question l'ensemble des transferts de données vers ce pays et *de facto* vers les fournisseurs de services numériques soumis au droit états-unien. Les conséquences opérationnelles de cette décision ont mis en lumière l'extrême dépendance de nos administrations et des entreprises à l'égard de ces acteurs à tous les niveaux – hébergement, services d'informatique en nuage, outils de cybersécurité, outils bureautiques ou d'analyse de données. Au-delà de ce constat, il est vite

apparu que soit il n'existait pas – ou pas assez – d'alternatives françaises ou européennes aux services en question, soit qu'elles étaient moins performantes et parfois plus onéreuses.

Je relève qu'il y a encore quelques années, le simple fait d'évoquer les enjeux de dépendance ou de souveraineté numérique était parfois associé à du protectionnisme. Le contexte actuel rappelle pourtant combien il est essentiel d'anticiper les risques liés à ces dépendances, la maîtrise des données étant devenue une nouvelle arme géopolitique.

Cette préoccupation n'est d'ailleurs pas propre à l'Europe. Les États-Unis, bien qu'ils concentrent une part majeure des infrastructures et des logiciels, cherchent eux aussi à limiter certaines dépendances stratégiques. L'actualité récente l'illustre : les nouveaux routeurs fabriqués à l'étranger seront désormais placés sur liste noire et interdits à la vente sur le sol américain, sauf rares dérogations.

Après ce bref rappel chronologique, je dirai en quoi la protection des données personnelles appelle une prise en compte des enjeux en matière de dépendances numériques.

Le règlement général sur la protection des données, le RGPD, constitue un outil de souveraineté normative par lui-même. Son champ d'application ne se limite pas aux sociétés européennes, mais couvre tous les acteurs dès lors qu'ils proposent des biens ou des services à des personnes dans l'Union européenne. En exigeant un haut niveau de protection des données, notamment en matière de sécurité ou d'encadrement des transferts, le RGPD constitue un levier favorable à l'affirmation d'une souveraineté européenne.

À cet égard, dans un contexte où les notifications de violation sont de plus en plus fréquentes, je suis convaincue que la sécurité des données, et j'entends par là aussi le contrôle que nous avons sur elles, ne passe pas uniquement par une bonne gestion des aspects cyber mais également par la prise en compte des enjeux de souveraineté numérique. En effet, on pourra toujours élever le niveau de maturité de tous les acteurs, sensibiliser les particuliers, accompagner les professionnels, tenter d'éviter les accès illégaux aux données, cela ne résoudra pas les difficultés liées aux cas où un accès est prévu par les législations extra-européennes auxquelles les fournisseurs de services peuvent être soumis. Cet angle mort est un risque objectif pour les données personnelles des citoyens.

C'est pourquoi il m'apparaît que ces sujets ne doivent pas être abordés seulement sous l'angle purement technique de l'efficacité à circonscrire une menace mais aussi, de plus en plus dans le contexte géopolitique actuel, sous l'angle de la dépendance. C'est particulièrement vrai pour nos données les plus sensibles, comme les données relatives à la santé ou biométriques. La Cnil préconise que celles-ci soient hébergées par des systèmes qui ne soient pas soumis à des lois extra-européennes et a œuvré, avec d'autres, pour l'émergence d'une certification européenne renforçant notre contrôle sur les données et leur sécurité. Elle soutient aux côtés du gouvernement et de l'Anssi (Agence nationale de la sécurité des systèmes d'information) l'initiative visant à développer une offre de cloud de confiance autour du label SecNumCloud.

Dans le cadre de la mise en œuvre du règlement sur la cybersécurité, l'Agence européenne de cybersécurité, l'Enisa (European Union Agency for Cybersecurity), s'est vu confier l'élaboration de schémas européens de certification de cybersécurité. Parmi ses travaux figure le projet de schéma de certification des services cloud, dit EUCS (*European Union Cybersecurity Certification Scheme on Cloud Services*). Nous ne pouvons que déplorer que, s'agissant des données les plus sensibles, il ne prévoie pas la possibilité d'intégrer, de façon optionnelle, des exigences de protection contre les lois extra-européennes.

À ce sujet, il me semble important de rappeler que la problématique du cloud ne se résume pas à la seule question de l'emplacement physique des données. L'accès à des données hébergées dans le cloud dépend également du prestataire qui fournit l'interface ou le service permettant d'y accéder. Dès lors, si ce prestataire interrompt ses services ou les dégrade, la question du lieu du stockage effectif des données perd de son importance. C'est notamment pour cette raison que, concernant la plateforme des données de santé, le collège de la Cnil a eu une position constante : elle a toujours considéré que cette base de données sensibles avait vocation à être hébergée par un opérateur européen. Or, à ce jour, l'hébergement s'effectue toujours sur le cloud de Microsoft, Microsoft Azure. Toutefois, nous accueillons très favorablement l'annonce faite au début de l'année de la mise en place dans les prochains mois d'un hébergement de l'ensemble des données sur une plateforme souveraine répondant aux plus hautes exigences en matière de sécurité.

J'ajoute que le cas de la plateforme des données de santé illustre, au-delà des aspects réglementaires, la nécessité de prôner l'exemplarité de la puissance publique. C'est d'ailleurs tout le sens de la logique de la doctrine dite du cloud au centre, appelée à devenir la solution de référence. La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, la loi Sren, relaie cette exigence au niveau légal, son article 31 imposant l'hébergement souverain pour les projets les plus sensibles des administrations de l'État.

Cette exemplarité ne devrait pas s'arrêter aux questions liées à l'hébergement des données. Il importe aussi de prendre en compte les outils de travail les plus courants. Je pense notamment aux messageries, aux solutions de traitement de texte, aux suites collaboratives, parce que ce sont ces outils qui façonnent les usages, qui créent les habitudes et qui installent parfois très durablement des dépendances. La Cnil a, par exemple, été interrogée à plusieurs reprises sur le recours à des outils collaboratifs et d'intelligence artificielle offerts à l'éducation nationale par des acteurs américains. Le RGPD en soi ne peut pas l'interdire, mais un tel choix pose question : il accroît de fait notre dépendance et il est susceptible d'exposer les données des élèves et des professeurs à des risques difficiles à maîtriser.

Pour conclure, j'aimerais partager avec votre commission plusieurs constats issus de nos échanges avec des acteurs privés et publics européens. Dans le cadre de nos activités, nous avons eu l'occasion d'interroger plusieurs d'entre eux pour savoir si la dépendance à des solutions étrangères était une inquiétude exprimée par leurs clients. Nous avons pu constater que c'était bien le cas, mais il faut relever que c'est par crainte de voir ces services disparaître du jour au lendemain. Le fait que le sort des données, personnelles ou non, soit laissé aux mains d'acteurs extra-européens apparaît secondaire dans leurs préoccupations, ce qui est regrettable.

Tout en nous réjouissant d'une prise de conscience des questions d'autonomie numérique, nous nous devons de continuer à appeler à la vigilance et à prôner une approche globale des enjeux intégrant non seulement la protection des données, mais aussi l'intelligence économique et la compétitivité. À ce stade, une préoccupation demeure : le regain d'attractivité pour les solutions souveraines persistera-t-il de façon décorrélée de l'évolution du contexte géopolitique ? À cela s'ajoute le fait qu'une fois qu'une grande organisation a structuré ses données, ses usages, ses contrats, ses équipes et ses processus autour d'un prestataire, revenir en arrière devient souvent complexe tant techniquement que juridiquement. Cela soulève la question de l'irréversibilité numérique. Une fois habitué à une solution ou un écosystème numérique particulier, il est compliqué et coûteux de faire marche arrière.

La souveraineté ne doit donc pas se penser dans l'urgence, en temps de crise : elle suppose une stratégie prévisible, inscrite dans le temps long et conçue avec volontarisme au plus haut niveau de la gouvernance des administrations et des entreprises.

Mme Sophie-Laurence Roy, présidente. Madame la présidente, je vous remercie pour la clarté de votre exposé, qui est à la fois rassurant et inquiétant : rassurant parce que vous décrivez très bien la conscience qu'a la Cnil du problème de la souveraineté ; inquiétant parce que vous vous demandez vous-même si la force de l'habitude ancrée dans l'usage de produits américains que font tous les Français, des mails à l'intelligence artificielle, ne va pas générer une sorte de soumission permanente.

Au sujet de la protection de nos données hébergées dans les clouds, il est absolument évident qu'une politique de souveraineté numérique ne se crée pas en quelques mois : elle réclame un travail de long terme et une immense détermination. Intuitivement, on a tendance à penser que l'informatique est impalpable, ce qui n'est absolument pas vrai. Tout cloud suppose des *data centers*, des logiciels pour gérer les données qu'ils hébergent et même des techniques pour abaisser leur température, car leurs serveurs chauffent.

Il faut absolument que la France puisse former du personnel à la gestion matérielle de tels centres. Or je viens d'apprendre qu'une école de la chambre de commerce et d'industrie d'Île-de-France qui formait plus de 2 000 chauffagistes par an serait contrainte de fermer en juillet prochain, compte tenu du coût de la formation et de l'insuffisance de l'aide apportée par France Compétences.

Ma deuxième question porte sur les labels et les normes. La qualification SecNumCloud, supposée certifier des solutions assurant une réelle souveraineté française, a été accordée à S3NS pour son produit Premi3ns ; or celui-ci fonctionne avec la technologie Google Cloud et le capital de cette société est détenu à hauteur de 5 % par Google. Vous l'avez souligné, les législations étrangères peuvent s'appliquer à nos données et je me demande si, compte tenu des particularités de la législation américaine, cette petite part qu'a Google dans la société S3NS ne permettrait pas au gouvernement américain d'exiger d'avoir connaissance de la totalité des données hébergées dans le cadre de l'offre Premi3ns. Cela ne me paraît pas rassurant : comment asseoir notre souveraineté si un label censé la garantir est accordé à une société appartenant pour une part à une société américaine et recourant à des plateformes et à des logiciels américains ?

Mme Marie-Laure Denis. Selon une récente étude du Cigref, 80 % des dépenses faites en France en matière de logiciels et services cloud vont à des acteurs américains, dépendance qui a bien sûr des effets indirects sur la croissance et l'emploi dans notre pays. À cet égard, on peut se réjouir que des sociétés françaises reçoivent la qualification SecNumCloud, même si tout n'est pas parfait puisque leur offre repose sur des sortes de joint-ventures avec des sociétés fournissant des services numériques américains. Cette qualification proposée par l'Anssi présente quand même des avantages : elle a été conçue pour se prémunir contre les accès de gouvernements étrangers à des données hébergées en France ou en Europe pour lesquelles les clés de chiffrement, et je parle sous le contrôle des experts techniques à mes côtés, sont dans des mains françaises. Fin décembre 2025, l'entreprise S3NS a rejoint six autres fournisseurs français ayant obtenu cette qualification. Cette offre, qui repose sur l'infrastructure de Thales, est la première à être issue d'un partenariat entre un *hyperscaler* américain, Google Cloud, et une entreprise française. Le directeur de l'Anssi a, je crois, pris soin de préciser que cela ne signifiait pas qu'il n'y avait pas de dépendance. Par ailleurs, Bleu, offre issue du partenariat entre Orange, Capgemini et Microsoft, est toujours en cours de qualification. Reste

que cela représente une amélioration puisque cela permet de prendre en compte les risques d'accès étrangers aux données des Français et des Européens.

S'ajoute à cela un élément technique, sur lequel nous pourrons vous apporter des précisions : les coupures ou dégradations de services imputables aux acteurs américains ne peuvent pas, semble-t-il, intervenir du jour au lendemain. Ce décalage dans le temps implique que, durant cette phase transitoire, l'irréversibilité peut en quelque sorte être maîtrisée.

M. Florent Della Valle, chef du service de l'expertise technologique. La Cnil n'a pas été amenée à étudier en détail ce projet. L'Anssi pourrait vous répondre plus précisément, madame la présidente, sur la question de savoir si le risque de dépendance est susceptible de subsister. Ledit risque ne saurait être pleinement couvert par quelque qualification que ce soit, d'autant qu'il ruisselle sur tous les composants d'un cloud, en particulier ses volets logiciels et matériels. SecNumCloud, s'il ne prémunit pas nécessairement contre l'ensemble des dépendances, constitue néanmoins une solution respectant certaines exigences. La Cnil a toujours considéré qu'il représentait une garantie dans la mesure où le risque d'accès est rendu suffisamment minime pour être acceptable compte tenu de la sensibilité des données.

Mme Sophie-Laurence Roy, présidente. Vu la nature de la plateforme à laquelle s'est liée S3NS et la composition de son capital, je peux dire que l'Anssi a ouvert si ce n'est un portail, du moins un portillon.

Mme Marie-Laure Denis. Je ne dis pas que la situation est parfaite, loin de là, mais elle est meilleure que celle qui prévalait avant que la qualification ne soit mise en place et que ces partenariats entre entreprises françaises et services américains ne soient établis. La dépendance demeure, mais il faut tout faire pour qu'émergent des alternatives françaises et européennes. Évitons tout fatalisme.

Mme Cyrielle Chatelain, rapporteure. Je rejoins certaines des réserves émises sur les offres Bleu et S3NS : qu'elles tentent de répondre à des besoins de services dans le cadre de joint-ventures montre une certaine incapacité à dépasser notre dépendance.

Dix ans après la création du RGPD, quel bilan en dressez-vous ? Quelles améliorations seraient souhaitables ? Identifiez-vous des freins à sa mise en œuvre ?

S'agissant des *dark patterns*, des réglementations plus précises sont-elles envisagées ? Les modifications des règles relatives aux cookies relèvent-elles de la législation française ?

Mme Marie-Laure Denis. Le RGPD, adopté il y a dix ans, entré en application il y a huit ans, a permis plusieurs avancées majeures. D'abord, il a contribué à exporter le modèle européen au-delà de nos frontières – c'est même, je crois, l'un des règlements européens les plus connus dans le monde.

Ensuite, il a mis à disposition de la Cnil et de ses homologues européens des outils de régulation des plus gros acteurs ayant les plus forts impacts, même s'il ne fait pas de distinction selon la taille des acteurs, sa régulation n'étant pas asymétrique comme d'autres réglementations européennes telles le DSA (Digital Services Act) ou le DMA (Digital Markets Act). Pour les cookies ou traceurs, la Cnil, se fondant sur un autre règlement européen, la directive « e-privacy », a prononcé depuis 2019 des sanctions portant sur un total de 953 millions d'euros d'amendes, dont 903 millions à l'encontre des plus grandes plateformes

étrangères, non parce qu'elles sont étrangères mais en raison de leur impact sur la protection des droits de nos concitoyens.

Le RGPD a consolidé les droits des usagers en matière de données et renforcé la conscience qu'ils ont de ces droits. Nous le voyons bien : le nombre annuel de plaintes adressées à la Cnil atteint 20 000, contre 7 000 avant son entrée en vigueur. Ce règlement a aussi imposé aux organismes d'avoir une hygiène pour leurs systèmes d'information : c'est le premier texte européen qui, à ma connaissance, pose des obligations en matière de sécurité des données, laquelle est devenue un enjeu de gouvernance.

De plus, comme le RGPD est neutre technologiquement, il permet une adaptation aux différentes évolutions technologiques.

Reposant sur la transparence et la confiance, il redonne aux utilisateurs des possibilités de contrôle sur les données et a considérablement renforcé le pouvoir de sanction de la Cnil et de ses homologues : les sanctions pécuniaires peuvent aller jusqu'à 20 millions d'euros et, pour les entreprises, jusqu'à 4 % de leur chiffre d'affaires mondial. Les organismes n'ont plus à demander d'autorisations préalables, sauf dans le domaine de la recherche en santé, mais sont investis de responsabilités, ce qui est une évolution heureuse compte tenu de l'importance prise par le numérique.

Le RGPD a également favorisé une application plus harmonisée des règles de protection des données au sein des vingt-sept pays de l'Union européenne, avec une exigence de coopération au quotidien. Depuis l'entrée en application du règlement, le Comité européen de la protection des données, le CEPD, a élaboré soixante-huit lignes directrices et émis sept recommandations afin de bâtir pour l'ensemble des pays de l'Union européenne une doctrine commune sur certains sujets. Il a également prononcé 10 000 sanctions, d'un montant total de 6,5 milliards d'euros, souvent assorties d'injonctions, ce qui force les acteurs à changer réellement leurs pratiques au lieu de se contenter d'acheter leur non-conformité.

S'agissant des axes d'amélioration, nous devons rester en permanence à l'écoute. Cela a été le sens de la réunion du CEPD qui s'est tenue en juillet dernier à Helsinki : la Cnil et ses homologues européens ont insisté sur la particulière vigilance, dont font aussi preuve les pouvoirs publics européens, à l'égard des contraintes propres aux PME et aux TPE, les petites et moyennes entreprises ayant moins de facilités pour implémenter les enjeux relatifs à la protection des données, même si c'est une nécessité. Par ailleurs, nous avons décidé d'avoir un dialogue plus proactif avec les parties prenantes, d'organiser davantage de consultations et de délivrer plus d'outils clés en main.

J'en viens aux *dark patterns*, les interfaces trompeuses, sur lesquelles nous avons beaucoup travaillé. Je me permets de vous suggérer de vous rendre sur le site du laboratoire d'innovation numérique de la Cnil, le Linc, pour faire le test sur les apparences trompeuses qu'il a mis en ligne depuis janvier. À travers diverses situations de la vie quotidienne, il s'agit de sensibiliser aux pratiques, parfois très au point, visant à manipuler l'utilisateur dans sa navigation et à influencer ses comportements et ses choix. D'une façon plus structurelle, nous avons mené en 2023 une étude avec la direction interministérielle de la transformation publique (DITP) sur les *dark patterns*.

Nous affinons notre politique relative aux cookies et aux traceurs publicitaires ainsi qu'aux sanctions à appliquer. L'objectif premier de la régulation de la Cnil a été d'offrir la possibilité à l'utilisateur de refuser les cookies dès le premier écran. Cela a réclamé un travail

de régulation méthodique mené durant trois ans en concertation avec les acteurs : publication de lignes directrices, puis, après avoir laissé un temps d'adaptation, lancement des contrôles et application des sanctions. Désormais, la plupart des sites se conforment aux règles : il est possible de refuser dès le premier écran – sur le téléphone portable, c'est l'option « continuer sans accepter », en général en haut à droite de l'écran. Nos contrôles se tournent désormais vers les interfaces trompeuses qui visent par exemple à noyer le « continuer sans accepter » dans d'autres informations. J'ajoute que les Cnil européennes, dans le cadre du Comité européen de la protection des données, ont édicté en 2022 des lignes directrices qui confirment que certaines pratiques sont incompatibles avec le consentement, défini par le RGPD comme devant être libre, éclairé et univoque – je pense aux cases précochées, aux parcours asymétriques, au design trompeur. Par ailleurs, le DSA interdit explicitement les interfaces trompeuses dans son article 25.

J'ajoute que la Cnil coopère avec l'Arcom (Autorité de régulation de la communication audiovisuelle et numérique) et la DGCCRF (direction générale de la concurrence, de la consommation et de la répression des fraudes), avec lesquelles elle a signé une convention tripartite visant une application cohérente du RGPD et du DSA, notamment sur cette question.

Mme Cyrielle Chatelain, rapporteure. Pour les *dark patterns*, considérez-vous que les bases juridiques actuelles sont suffisamment solides ? Estimez-vous des ajouts nécessaires ?

Ma deuxième question porte sur les contrôles. Quels sont les délais moyens d'instruction ? Pour ce qui est de la conformité au RGPD, quelles sont vos relations avec vos homologues irlandais ? Quel est le niveau d'information des personnes dont la plainte déposée en France est transmise à la Commission de protection des données irlandaise ? Quelles limites trouve ce travail de coopération ? Nous avons eu plusieurs témoignages au sujet de procédures longues et complexes et de problèmes d'accès à l'information, notamment du côté irlandais.

Mme Marie-Laure Denis. Je vais essayer d'illustrer mes réponses par des chiffres : en 2025, la Cnil a effectué 323 contrôles, dont la moitié était des contrôles sur place, le reste étant fait en ligne, sur pièces ou par audition. L'ensemble a donné lieu à 260 mesures correctrices, dont 84 sanctions. Les mesures correctrices qui ne sont pas des sanctions peuvent par exemple être des mises en demeure. La moitié des contrôles faisaient suite à des plaintes, le reste étant lié à l'actualité, à des thèmes prioritaires de contrôle définis par le collège de la Cnil ou à la volonté de nous assurer que nos précédentes sanctions ou mesures répressives ont bien été suivies d'effet.

S'agissant du délai, il est assez variable. Nous essayons d'être les plus rapides possible. Cela dépend naturellement de la complexité des sujets.

Des contrôles sur les applications mobiles peuvent par exemple prendre davantage de temps, car c'est un écosystème complexe, avec beaucoup d'intervenants. Nous en avons mené treize l'année dernière à la suite des recommandations que nous avions faites s'agissant des applications mobiles pour s'assurer que les personnes soient informées. Vous avez toute votre vie dans votre téléphone portable et, souvent, sur les applications. Les Français en téléchargent trente par an. On ne fait pas très attention à la question de savoir si on accepte d'être géolocalisé ou pas, alors que la géolocalisation dit beaucoup de choses sur la vie privée.

D'autres contrôles sont plus faciles à réaliser, par exemple lorsqu'il s'agit d'accéder à certaines données. Il est alors assez aisé de constater si l'organisme a donné ou non cet accès.

Mais nous sommes très conscients de la nécessité d'être très proactifs, notamment en matière de gestion des plaintes. Nous avons fait au cours des dernières années un gros travail de productivité, de mise en place d'indicateurs, etc., ce qui n'existait pas auparavant, pour essayer de traiter autant de plaintes que nous en recevons dans l'année. Les ratios peuvent cependant se dégrader. En effet, lors des trois premiers mois de l'année, nous avons reçu 75 % de plaintes en plus par rapport aux trois premiers mois de l'année dernière, sans que je puisse en expliquer les raisons.

Sur la coopération européenne en matière répressive, comme vous l'avez très bien rappelé, l'un des intérêts et des avantages du règlement général sur la protection des données est en effet qu'une autorité de protection des données prend le *lead* en Europe lorsque des traitements de données concernent plusieurs États membres. Les très grandes plateformes ayant installé à Dublin leur établissement principal en Europe, c'est l'autorité irlandaise qui est très largement compétente sur ces sujets – mais pas toute seule, parce que nous transmettons parfois des plaintes qui ont donné lieu à des sanctions. Il arrive même que nous coopérions en menant des enquêtes conjointes. Cela avait notamment été le cas avec l'autorité de protection des données luxembourgeoise, qui a prononcé une amende de 746 millions d'euros contre Amazon en 2021, me semble-t-il. Nous avions aussi coopéré avec l'autorité néerlandaise, qui a prononcé en 2024 une amende de 290 millions d'euros contre Uber, dont le siège principal est aux Pays-Bas. De façon moins spectaculaire mais très intéressante, car il s'agissait d'un acteur très connu en Europe, nous avons coopéré avec l'autorité lituanienne, qui a prononcé une amende de 2,3 millions d'euros contre Vinted en 2024. Cette coopération a une vraie consistance et est effective.

Pour revenir plus précisément à votre question sur l'Irlande, il est vrai qu'au début de la mise en œuvre du RGPD, l'autorité irlandaise a mis un peu de temps à se mettre en route et à décider des sanctions, pour des raisons qu'il lui reviendrait d'expliquer et aussi parce qu'il y avait certainement une montée en charge très importante des plaintes et des contrôles.

Mais le RGPD est bien fait – au moins de ce point de vue-là –, puisqu'un mécanisme permet que les homologues d'une autorité *lead* lui imposent en quelque sorte de prendre une décision ou lui disent qu'ils ne sont pas d'accord avec celle-ci. Si une autorité décide de n'imposer aucune amende et estime qu'il faut circuler car il n'y a rien à voir, les autres autorités peuvent manifester leur désaccord, sous réserve d'atteindre une certaine majorité. C'est ce qui s'est passé à neuf reprises à ma connaissance, la *lead supervisory authority* compétente ayant été contrainte de modifier sa copie. Cette procédure de résolution des litiges, qui permet d'imposer une décision contraignante pour l'autorité chef de file, est actuellement tout à fait active.

Comme nous parlons de souveraineté et de dépendance, je crois que l'Irlande a prononcé l'année dernière une amende à l'encontre de TikTok qui s'élève de mémoire à 530 millions d'euros, notamment en raison de transferts de données vers la Chine. La coopération en matière répressive entre les autorités de protection des données européennes est donc désormais une réalité.

Mme Sophie-Laurence Roy, présidente. La répression, c'est bien. Ne pas avoir à réprimer, ce serait mieux.

Je reviens aux sujets de souveraineté et de cloud souverain. L'État a développé deux clouds souverains, Nubo pour le ministère des finances et Pi pour celui de l'intérieur, pour un

coût total de 55 millions d'euros à ma connaissance. Or ils restent sous-utilisés, y compris par les ministères qui les ont financés.

Selon vous, comment pourrait-on faire, comment l'État peut-il faire ou que pouvons-nous faire en tant que parlementaires pour que les données de ces ministères – qui sont sensibles et importantes – soient transférées réellement et rapidement sur des clouds français, avec des systèmes français, et qu'elles soient souverainement protégées ?

Mme Marie-Laure Denis. Si vous le permettez, je vais profiter de votre première observation pour dire que, contrairement à une idée reçue, la Cnil n'est pas uniquement un gendarme de la protection des données. Même si nous ne communiquons peut-être pas assez sur le sujet, nous faisons beaucoup d'accompagnement – d'ailleurs, le directeur de l'accompagnement juridique est présent à mes côtés, alors qu'il n'y a personne de la direction des contrôles et des sanctions. Notre but n'est pas de réprimer, mais vraiment de s'assurer de la mise en conformité.

Le rôle du collège de la Cnil est de rendre des avis sur les projets de loi et les projets de décret en Conseil d'État. Je crois que 150 de ces avis ont été émis au cours des deux dernières années. Ils sont publics et peuvent nourrir le débat, notamment parlementaire. Mais nous répondons aussi à 1 500 demandes par an émanant d'entreprises. Nous avons créé des bacs à sable, qui ne sont pas réglementaires, pour accompagner les projets innovants.

Nous menons beaucoup d'actions de sensibilisation auprès des mineurs. Avec votre consentement éclairé, libre et univoque, je me permets de faire la publicité de l'application FantomApp. À ma connaissance, c'est la première fois qu'une autorité administrative indépendante, grâce d'ailleurs à des fonds européens que nous sommes allés chercher, publie une application à destination des mineurs – mais pas seulement, car elle pourrait être utile à tous s'agissant de la navigation sur les réseaux sociaux. Cette application est téléchargeable gratuitement et elle permet à chacun de vérifier si son mot de passe est robuste. Elle permet de savoir comment déposer une plainte et à quelle plateforme s'adresser si l'on est harcelé. Quid du rôle de la Cnil ? Quid de celui de e-Enfance ? L'application aborde des situations très concrètes : comment flouter ses profils sur les réseaux sociaux ? Quels sont nos droits à l'effacement de nos données ?

Tout cela pour vous dire que, par-delà nos missions répressives et d'anticipation technologique, nous faisons beaucoup de sensibilisation de tous les publics.

Sur la question des clouds souverains, je dirais quelques mots avant que Florent Della Valle complète éventuellement mes propos, sachant que j'ai vu que vous aviez auditionné la Dinum (direction interministérielle du numérique) hier. Votre question est davantage de son ressort que de celui de la Cnil, même si celle-ci ne peut que se féliciter de l'existence de clouds souverains pour héberger les données les plus sensibles des administrations.

Je souhaite insister sur un point : on comprend bien qu'il faut faire un saut important pour réduire les dépendances que vous traquez, et qui sont illustrées dans le cadre de vos auditions. Il faut beaucoup de volontarisme, parce que cela demande des efforts au plus haut niveau de la gouvernance des ministères. Mais je pense qu'il est également nécessaire de bien cartographier ces données pour savoir lesquelles sont sensibles et lesquelles le sont moins, pour faire les choses progressivement.

Je ne sais pas si Florent a davantage d'éléments à vous fournir, car je ne vous cache pas que ce n'est pas directement du ressort de notre autorité.

M. Florent Della Valle, chef du service de l'expertise technologique. Nous aurons du mal à dire que nous préférerions que l'on utilise un cloud opéré par un ministère plutôt que par un acteur privé qui répondrait aux mêmes critères de souveraineté. Je ne crois pas qu'il y ait eu un avis de la Cnil allant dans ce sens.

En revanche, nous pourrions attirer l'attention sur ce qui compte *in fine*, c'est-à-dire la maîtrise de la donnée. Si un acteur responsable d'une infrastructure ne maîtrise pas celle-ci, le risque est au fond le même que pour un ministère. Par-delà le fait de posséder l'infrastructure, nous pourrions donc être amenés à insister sur la compétence nécessaire pour maîtriser des données. Elles peuvent être aussi bien aux mains d'acteurs privés souverains qu'aux mains d'acteurs publics. Le critère de possession n'est pas celui auquel la Cnil serait sensible dans le cadre de ses propres missions.

Mme Cyrielle Chatelain, rapporteure. Avant de revenir à la question des contrôles, je note que vous aviez déjà parlé du développement de l'application FantomApp lors de votre audition par la commission des affaires économiques ou par la commission des lois.

Mme Marie-Laure Denis. C'était à la commission des lois.

Mme Cyrielle Chatelain, rapporteure. Je l'ai téléchargée et je la trouve extrêmement simple d'accès et intéressante. Le test du mot de passe est un moment que je recommande !

Même si l'on a cet outil, on a parfois l'impression qu'il s'agit de David contre Goliath : quelle est la capacité de diffuser des applications utiles face à des applications qui s'appuient sur un certain nombre d'algorithmes extrêmement néfastes ?

L'impact de ces algorithmes est avéré, notamment en matière de santé. La question des *dark patterns* ne concerne pas seulement les cookies, puisqu'ils sont utilisés de manière très générale par les plateformes. Serait-il intéressant de renforcer le délit de plateforme ? Il concerne déjà le type de produits proposés, notamment. L'utilisation de *dark patterns* ou d'algorithmes qui entraînent des problèmes de santé devrait-elle être mieux encadrée ou constituer un délit ? Quels sont les points sur lesquels il serait nécessaire de légiférer ? Une réflexion est en cours à ce sujet et votre avis m'intéresse.

S'agissant des contrôles, comment déterminez-vous le montant des sanctions ? A-t-il un lien avec ce que les violations des textes ont rapporté aux acteurs numériques, ou bien les sanctions sont-elles calculées en fonction de la gravité ou du type de méfait ?

Pourriez-vous nous faire parvenir par écrit le montant total des amendes perçues ces dernières années pour les procédures closes et nous indiquer ce qu'il en est du recouvrement pour les autres sanctions prononcées ?

Je me trompe peut-être, mais il me semble que la décision prise au Luxembourg contre Amazon a fait l'objet d'un recours. Pourriez-vous nous indiquer sur quel fondement ?

Enfin, de nombreuses dispositions concernant la question des cookies et la « fatigue des cookies » figurent dans le projet « omnibus numérique ». En effet, comme vous l'avez indiqué, les acteurs ont travaillé à rendre les choses très compliquées pour les usagers. Que

pensez-vous de la proposition qui consiste à tenir compte de la fatigue des cookies en recueillant le consentement directement dans le navigateur, et non plus lors de la consultation de chaque site ? Est-ce que cela favorisera les pratiques des grandes plateformes ou, au contraire, renforcera les droits des usagers ?

Mme Marie-Laure Denis. Nous savons tous que les algorithmes de recommandation ont un impact sur la santé et parfois même sur la santé mentale des utilisateurs, notamment pour les populations les plus vulnérables et les jeunes – et les parlementaires le savent tout particulièrement pour avoir organisé un certain nombre d'auditions sur le sujet. La Cnil a d'ailleurs été entendue dans le cadre de plusieurs commissions d'enquête, notamment celle sur TikTok.

Cette question relève davantage de l'Arcom, avec laquelle je ne voudrais pas me fâcher car nous nous concertons et coopérons beaucoup entre régulateurs. Cependant, nous sommes bien entendu susceptibles de nous intéresser au sujet des biais des algorithmes, notamment dans le cas de l'intelligence artificielle.

S'agissant des contrôles, il existe deux procédures de sanction au sein de la Cnil.

La procédure dite ordinaire concerne les manquements les plus importants. Les sanctions sont alors prononcées par la commission des sanctions, c'est-à-dire par une formation restreinte que je saisis et à laquelle je ne participe pas. Elles peuvent aller jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise, ou 20 millions d'euros s'il s'agit d'un organisme qui n'a pas de chiffre d'affaires.

Il y a deux ou trois ans, nous avons demandé et obtenu du gouvernement et du Parlement la création d'une procédure dite simplifiée, qui nous a permis de passer d'une dizaine de sanctions par an à quatre-vingt-cinq. Dans ce cas, elles sont plafonnées à 20 000 euros et ne sont pas publiques – même si nous pouvons communiquer à leur sujet de façon anonymisée afin qu'elles aient un rôle d'exemple. Cette procédure dite simplifiée est destinée à traiter les dossiers plus vite, avec une procédure contradictoire moins étoffée. Elle concerne les manquements les moins importants, afin de réduire les trous dans la raquette.

La question que vous posez sur la détermination des sanctions dans le cadre de la procédure dite ordinaire est extrêmement pertinente et les membres de la commission des sanctions de la Cnil se la posent également. Il est plus compliqué de définir des critères très précis lorsque l'on défend un droit fondamental tel que la protection de la vie privée. Combien rapporte un biais de consentement ? Combien rapporte le refus d'accès à des données ? Ce n'est pas tout à fait la même chose que dans le domaine de la concurrence, l'Autorité de la concurrence ayant publié une grille indiquant des critères de sanction précis en fonction du préjudice causé et des sommes rapportées.

Cela dit, les autorités de protection des données, réunies au sein du CEPD, ont élaboré un document fournissant des critères indicatifs sur les grilles de sanction. Tout le problème est d'arriver à concilier la proportionnalité – il est heureux que cette exigence s'applique dans un État de droit, où les décisions de la Cnil peuvent faire l'objet d'un recours devant le Conseil d'État – et le rôle dissuasif de la sanction.

J'en profite pour dire que, jusqu'à présent – je touche du bois –, nos décisions ont été très largement suivies par le juge administratif. Toutefois, même si ce n'était pas le cas et que tel ou tel montant de sanction était revu – encore une fois, ce n'est pas moi qui prononce les

sanctions –, je considère que, dans un droit en construction et qui est souvent à l'intersection avec d'autres droits – par exemple le droit à la vie privée ou le droit du travail –, affirmer une position qui cherche à concilier la proportionnalité et la fonction dissuasive de la sanction fait partie du rôle d'une autorité de protection des données. Il ne faut pas que les très gros acteurs puissent en quelque sorte acheter leur non-conformité. Si l'amende était une proportion négligeable de leur chiffre d'affaires, peut-être auraient-ils intérêt à ne pas être conformes, car cela leur rapporterait plus que le coût de l'amende.

Il faut donc trouver le bon équilibre entre dissuasion et proportionnalité, quitte à ce que, *in fine*, le juge nous aide en quelque sorte à affiner les critères de sanction. Encore une fois, je me réjouis que la Cnil ait pour l'instant été très largement suivie par son juge s'agissant des sanctions qu'elle a infligées en mettant en œuvre le RGPD. Mais, même si elle n'était pas suivie ou si ses décisions ont pu être modifiées de manière marginale, je ne considère pas que c'est inutile : au contraire, cela nous permet à tous de progresser.

Compte tenu du montant des sanctions que j'ai évoquées, vous imaginez bien que les décisions contentieuses de la Cnil, quand elles ont une forte portée, sont systématiquement attaquées par les meilleurs avocats de la place spécialistes du droit de la protection des données. Nous sommes donc particulièrement vigilants sur ce sujet.

Vous avez évoqué le recouvrement. Nos amendes sont très largement recouvrées. D'ailleurs, les grandes plateformes qui ont fait l'objet de sanctions de la Cnil sur le fondement non pas du RGPD mais de la directive « e-privacy », notamment s'agissant des cookies, payent de façon tout à fait normale leurs amendes. En gros, 98 % du montant de nos amendes sont recouvrés. Il ne vous aura pas échappé que nous ne les recouvrons pas nous-mêmes. En tout cas, je peux vous certifier qu'elles n'alimentent pas le budget de la Cnil et que ce n'est pas un élément pris en compte pour déterminer le montant des sanctions que nous prononçons – et c'est bien normal.

Selon les informations transmises par la direction générale des finances publiques, dans les quelques cas où le recouvrement est difficile, il s'agit notamment d'un opérateur étranger que les pouvoirs publics français ont du mal à identifier ou, inversement, d'une société défaillante ou d'un individu qui n'est pas en mesure de payer – même si nous cherchons vraiment à prendre en compte la capacité financière des entreprises ou des organismes en question.

Vous avez évoqué les sanctions européennes. Le cas de l'Irlande est particulier puisque, à ma connaissance, les amendes que prononce son autorité de protection de données peuvent faire l'objet d'un appel qui est suspensif. Le recouvrement de l'amende ne peut donc avoir lieu qu'à l'issue de tous les contentieux consécutifs à la sanction, ce qui fait qu'un certain nombre d'amendes dont le montant est élevé n'ont pas encore été recouvrées – mais je ne vais pas être catégorique et je ne saurais pas vous dire desquelles il s'agit dans le détail.

En ce qui concerne la sanction de 743 millions d'euros prononcée par l'autorité de protection des données luxembourgeoise contre Amazon en 2021, je crois que la Cour administrative n'a pas annulé la décision mais l'a renvoyée à l'autorité de protection des données elle-même – cela ne veut pas dire que l'autorité de protection ne va pas pouvoir reprendre la même décision en modifiant certains éléments de son analyse.

M. Thomas Dautieu, directeur de l'accompagnement. La Cour a validé les manquements relevés par l'autorité luxembourgeoise, mais elle a annulé la décision car le

montant de la sanction n'était pas justifié par les manquements. L'autorité de protection des données luxembourgeoise doit donc reprendre le travail pour justifier le montant initial en fonction des manquements.

Mme Marie-Laure Denis. Donc, pour résumer, mais sans être une spécialiste de la justice luxembourgeoise, cette décision s'explique davantage par des questions de procédure et de motivation que par des questions de fond – mais peut-être a-t-elle aussi un lien avec celles-ci.

Je vais laisser la parole à Thomas Dautieu pour répondre à votre question sur les navigateurs et le projet omnibus.

M. Thomas Dautieu. Ce projet prévoit la possibilité d'utiliser le navigateur pour consentir aux cookies ou les refuser. Il est vrai que cela résout le problème de la fatigue du consentement, puisqu'il suffit d'une seule action. Par contre, cela pose le problème de la granularité du consentement. Si vous dites non à tout, ça marche. Mais si vous souhaitez par exemple accepter les cookies seulement pour les sites culturels et non pour les sites marchands, ça marche moins bien : c'est tout ou rien.

Nous discutons avec des entreprises qui proposent des solutions techniques pour une approche plus fine via le navigateur, afin d'éviter ce tout ou rien qui poserait des problèmes aux sites concernés.

Mme Marie-Laure Denis. S'agissant du projet « omnibus digital », dit de simplification, les discussions portent notamment sur l'intégration partielle dans le RGPD de la réglementation sur les traceurs, qui relève actuellement de la directive « e-privacy ».

Sur le papier, cette proposition peut paraître cohérente, d'autant que les autorités compétentes sont les équivalents, selon les pays, soit de la Cnil, soit de l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). Le texte conduirait en pratique à soumettre la régulation des traceurs au mécanisme européen dit du guichet unique, donc, très concrètement, à la confier à deux ou trois autorités au sein de l'Union européenne – les autorités irlandaise et luxembourgeoise, par exemple.

Je ne sais pas comment cela peut se traduire en pratique : la Cnil a reçu 2 000 plaintes concernant les traceurs ces trois dernières années ; comment une ou deux autorités vont-elles pouvoir absorber toutes les plaintes actuellement déposées dans vingt-sept pays ? Si cette réforme aboutit, n'y a-t-il pas un risque que cela se traduise par une diminution des droits des personnes et de l'effectivité de la régulation ? Or, en France, nous avons particulièrement investi ce champ de la régulation depuis six ans. Nous avons été à l'avant-garde pour construire une régulation équilibrée, validée par le Conseil d'État, qui a donné lieu à quarante-huit sanctions et à 953 millions d'euros d'amende. En tout cas, c'est une préoccupation pour nous.

Mme Cyrielle Chatelain, rapporteure. De plus en plus de sites conditionnent l'accès aux contenus soit à un paiement, soit à l'acceptation des cookies. C'est compréhensible du point de vue des modèles économiques, car on sait que la vente des données en fait malheureusement désormais partie intégrante. En revanche, cela biaise le consentement. Quel est votre avis à ce sujet ?

Ma deuxième question porte sur la manière de monétiser les données. Martin Untersinger, journaliste au *Monde*, y a révélé comment des données, notamment de

géolocalisation, sont captées via des applications qui utilisent généralement des listes de consentement très longues, biaisant d'une certaine manière le consentement, et sont revendues à des courtiers en données.

On peut se poser plusieurs questions sur la qualité du consentement, et notamment sur le fait qu'il n'est pas éclairé, puisque même l'application ne sait pas à quelles fins les données sont utilisées. Vous êtes-vous penchés sur ces acteurs économiques et sur ces circuits ? Quels sont les outils pour les réguler ou les sanctionner ?

Mme Marie-Laure Denis. Lors de l'élaboration de nos lignes directrices sur les traceurs, nous avons approfondi la question des *cookie walls* – c'est-à-dire des « murs de traceurs », qui permettent de subordonner l'accès à un service à l'acceptation de cookies. Avec nos homologues, nous avions adopté une position commune, selon laquelle un tel usage des cookies n'est pas acceptable en l'absence d'une solution alternative raisonnable, mais le Conseil d'État ne nous a pas suivis. Depuis, je crois que le CEPD a formulé un avis à ce sujet.

M. Thomas Dautieu. Oui, à la suite d'un arrêt de la CJUE concernant un grand acteur américain, le CEPD a estimé que le choix binaire n'était pas acceptable et que des alternatives devaient être proposées.

Après, quand un accès est payant, toute la question est celle de la bonne détermination du prix. Le CEPD travaille actuellement à des lignes directrices pour adapter ce principe aux sites de presse, notamment. Pour de tels sites, la question est plus compliquée que pour les grandes plateformes de publicité.

En tout cas, nous avons bien ce sujet en tête et nous en discutons avec l'écosystème, pour parvenir à une solution qui satisfasse les intérêts économiques tout à fait légitimes des sites tout en respectant le principe du consentement libre des internautes.

Mme Marie-Laure Denis. J'en viens aux courtiers en données, ou *data brokers*. Ces acteurs sont plus opaques que les grandes plateformes numériques, qui exploitent directement les données qu'elles collectent. Ils croisent les informations issues de multiples sources, par exemple les données concernant les achats en ligne ou en magasin avec les cartes de fidélité, celles issues des applications mobiles, notamment concernant la localisation, ou encore les historiques de navigation sur internet. À l'issue de ce travail d'agrégation, ils sont capables de constituer des profils extrêmement précis des individus, qu'ils vendent à des annonceurs – je pense que beaucoup de nos concitoyens ne se rendent pas compte de ces phénomènes.

Sur le plan juridique, la réutilisation et la revente de données, même si elles ne sont pas illégales, sont strictement encadrées. En effet, le RGPD et la loi « informatique et libertés » prévoient que les personnes doivent être informées de la collecte et des usages de leurs données, et donner leur consentement en cas de traitement de celles-ci à des fins publicitaires et de revente. En apparence, nous disposons donc d'un cadre juridique protecteur, celui relatif à l'information et au consentement, pour faire face à ces pratiques.

Toutefois, dans la pratique, de nombreux *data brokers* contournent ces obligations. En s'appuyant sur des chaînes de collecte et de revente complexes et peu transparentes, ils compliquent la traçabilité des données et l'identification des responsables par le régulateur. Par exemple, ces acteurs collectent souvent les informations dans le cadre d'enchères en temps réel. Parmi les dizaines voire les centaines de participants à ces enchères, certains conservent l'information pour la revendre, mais il est difficile d'identifier lesquels.

Quant aux acteurs qui revendent les données de géolocalisation sur les places marchandes, ce sont pour la plupart de petites structures, qui n'ont aucun établissement en Europe, ne sont pas pérennes, ou changent souvent de nom.

Certes, la formation restreinte de la Cnil a prononcé plusieurs sanctions à l'encontre de courtiers en données, par exemple le 31 janvier 2024, ou le 15 mai 2025. Dans cette dernière affaire, un courtier collectait les données par l'intermédiaire de formulaires de participation à des jeux-concours pour les revendre, mais sans avoir obtenu de consentement valide des joueurs – le design de ces formulaires était en effet trompeur. Toutefois, les moyens des autorités restent limités face à l'ampleur et à la complexité du marché mondial des données personnelles.

Nous attachons beaucoup d'importance à la donnée de géolocalisation, indépendamment, d'ailleurs, de son usage par les *data brokers*. Demain, le collège de la Cnil se prononcera sur les règles d'utilisation de la géolocalisation pour les voitures connectées ou autonomes, en émettant des recommandations.

Dans notre régulation sur les applications mobiles, nous essayons de faire beaucoup de pédagogie sur la donnée de géolocalisation. Encore une fois, alors que cette fonction est relativement facile à désactiver, nous ne le faisons pas assez – dans les cas où elle n'est pas nécessaire au service demandé, s'entend.

Mme Cyrielle Chatelain, rapporteure. Même si l'éditeur d'une application ne connaît pas forcément la chaîne d'intermédiaires par laquelle transitent les données qu'il collecte – de fait, celle-ci est complexe –, n'y aurait-il pas intérêt à faire porter sur lui la responsabilité de l'usage de ces données ? Cela pourrait favoriser la vigilance.

Il est vrai qu'en tant qu'utilisateurs, nous ne désactivons pas assez souvent la géolocalisation, de même que les fonctions de partage public des informations. Selon vous, serait-il intéressant de proposer leur désactivation par défaut, afin que les utilisateurs n'aient pas à prendre l'initiative de ce choix ? Si oui, une telle modification relèverait-elle du droit européen ou du droit français ?

Plus largement, les mesures concernant le RGPD de la proposition de paquet « omnibus numérique » sont justifiées par leurs défenseurs par le coût de la mise en conformité. Grâce à votre mission d'analyse économique, avez-vous une idée de son niveau ? À l'inverse, vous est-il possible de mesurer les bénéfices liés à cette réglementation européenne ?

Mme Marie-Laure Denis. Nous nous posons toujours la question de la responsabilité des différents acteurs, car elle est assez complexe – il faut d'abord déterminer qui est responsable du traitement, qui est sous-traitant et qui est responsable conjoint du traitement.

M. Florent Della Valle. Madame la rapporteure, en entendant vos propositions de faire porter la responsabilité sur les éditeurs d'application et de modifier le paramétrage par défaut, on croirait que vous avez lu les quatre-vingt-douze pages de notre recommandation relative aux applications mobiles !

Ces principes font partie de ceux que nous avons voulu réaffirmer, dans un écosystème où les chaînes de responsabilité sont complexes. Au titre du RGPD, le responsable de la collecte du consentement est en premier lieu l'éditeur de l'application, celui qui la met en place, même si nous avons conscience que les éditeurs peuvent être économiquement ou techniquement

dépendants d'autres acteurs, dont ils intègrent les composantes et qui réutilisent parfois eux-mêmes les données.

En tout cas, le principe est clair : c'est l'éditeur qui est responsable, et, en le rappelant, nous n'avons pas inventé de nouvelles normes juridiques. Il fallait toutefois signaler des points d'attention concernant la mise en œuvre concrète de cette responsabilité.

Pour prendre en compte la dépendance des éditeurs à d'autres acteurs, nous prévoyons, dans le cadre du plan de contrôle évoqué tout à l'heure par Mme la présidente, de contrôler les fournisseurs de SDK (kits de développement logiciel), des composantes qui sont utilisées dans les applications mobiles et constituent un maillon essentiel de la collecte de données.

Par ailleurs, l'article 25 du RGPD impose déjà que le paramétrage par défaut soit le plus protecteur de la vie privée. Ce principe est donc reconnu au niveau européen. Il doit toutefois être décliné dans différents contextes. Dans le secteur des applications mobiles, nous avons ainsi souhaité expliquer concrètement aux acteurs comment l'appliquer, pour mieux protéger la vie privée des personnes.

Mme Marie-Laure Denis. Madame la rapporteure, votre proposition de désactiver la géolocalisation par défaut me paraît intéressante – mais quand on dit cela, c'est parfois parce que l'on n'a pas la réponse…. Je pense, de fait, qu'elle relève du droit européen et non du droit français et qu'elle risque de poser question du point de vue du droit de la concurrence – mais ce n'est qu'une première réaction, qui demande à être approfondie. Nous devons réfléchir davantage, et nous vous enverrons le fruit de nos réflexions, si vous le permettez.

Quant à l'impact économique du RGPD, le service de la Cnil chargé de l'analyse économique a essayé de l'étudier. En mai 2025, nous avons organisé un événement académique à ce sujet, dont le compte rendu est disponible sur notre site. Il en résulte que, d'une manière générale, les études menées pointent davantage le coût du RGPD que ses bénéfices.

Ces coûts sont réels pour les entreprises ou les administrations ; il est probable qu'ils décroissent proportionnellement à la taille des entités concernées. Enfin, ils ne sont pas tous récurrents : une fois qu'une entité a fait l'effort de se mettre en conformité, elle n'a pas à le faire de nouveau, même s'il peut arriver, ponctuellement, qu'elle doive évoluer, sur des sujets tels que le cyber, ou qu'elle doive assumer des coûts liés à l'exercice par les utilisateurs de leur droit d'accès.

Plutôt que de gommer la question des coûts du RGPD, il est plus intéressant de mettre en avant ses différents bénéfices, car ils sont rarement perçus par les entreprises.

Dans une économie digitalisée, tellement fondée sur l'exploitation de la donnée, les règles du droit de la protection des données constituent un atout, car elles poussent les administrations et les entreprises à se doter d'une vision de leur patrimoine informationnel, à cartographier leurs traitements, à fixer des délais de conservation des données, à se débarrasser de celles qui ne sont pas liées à la finalité du traitement, et cetera. C'est dans l'intérêt des entreprises – elles s'évitent ainsi, par exemple, de solliciter quelqu'un qui n'aurait pas répondu à tous les mails qu'elles lui envoient depuis des années. En somme, le RGPD incite à une hygiène numérique du quotidien. C'est quelque chose de très positif.

En outre, le fait, pour une entreprise, de prendre en compte les enjeux de vie privée lui ouvre un meilleur accès aux appels d'offres. C'est également valorisé dans le cadre des *due diligence* (audits d'acquisition), en cas de cession.

Enfin, je crois nos concitoyens et les entreprises de plus en plus sensibles aux risques réputationnels. C'est tout le sens de notre coopération avec l'Autorité de la concurrence, que nous avons beaucoup développée. La capacité à protéger les données et la vie privée devient un avantage concurrentiel distinctif, au même titre que le prix, le coût ou la qualité de service. Certes, ce n'est pas le cas dans tous les domaines et dans tous les secteurs. Toutefois, je crois vraiment que le facteur confiance pèsera beaucoup dans la croissance de l'économie numérique ces prochaines années.

Ainsi, je suis un peu désolée de n'entendre parler que du coût du RGPD – même si je comprends que c'est une contrainte –, alors que ses bénéfices sont nombreux. Le premier, dans le contexte cyber actuel, est qu'il permet des mesures appropriées. Par exemple, la Cnil reçoit les notifications de violation de données – nous en avons reçu 6 200 l'année dernière. Nous nous sommes aperçus que leur nombre connaissait une forte augmentation pour les grandes bases de données, soit celles qui concernent plus de 1 million de personnes : il y en a eu quarante-cinq l'année dernière, contre trente-cinq l'année précédente et deux fois moins celle d'avant. C'est un peu contre-intuitif : on pourrait penser que les grandes organisations ont les moyens de parer les attaques – même si nous savons que ce n'est pas facile, raison pour laquelle nous prônons une obligation de moyens et non de résultat. Nous avons également constaté que 80 % de ces grosses violations de données auraient pu être évitées, si, entre autres mesures, les organisations concernées avaient mis en place une authentification multifonctionnelle.

Ainsi, les entités n'avaient tout simplement pas tiré toutes les conséquences de l'essor du télétravail : un salarié travaillant à distance pouvait accéder aux données d'une dizaine ou d'une vingtaine de millions de clients uniquement à partir de son identifiant et de son mot de passe, alors que ceux-ci pouvaient être compromis. Le collège de la Cnil a donc imposé en avril 2025 une authentification multifacteur, comme celles utilisées par les applications bancaires, pour l'accès à distance aux bases de données de plus d'un million de personnes. Notre rôle de régulateur est d'être pragmatique. Nous avons donc laissé aux acteurs jusqu'au 1er janvier 2026 pour s'adapter. Depuis, nous contrôlons qu'une authentification multifacteur a bien été instaurée.

De telles normes évitent beaucoup de problèmes aux entreprises et aux administrations. Vous noterez que, depuis le début de l'année – et cela va continuer –, la formation restreinte de la Cnil a prononcé des amendes significatives à l'encontre d'administrations ou d'entreprises pour des manquements cyber. En tout cas, il y a de vrais avantages pour elles à prendre en compte les risques liés à la protection des données.

Mme Cyrielle Chatelain, rapporteure. Dans un avis conjoint de février 2026, le Contrôleur européen de la protection des données et le Comité européen de la protection des données ont exprimé des préoccupations majeures concernant la proposition de règlement « omnibus numérique ». Quelle est votre analyse à ce sujet, en complément de ce qui a déjà été dit ?

Par ailleurs, jusqu'ici, la Cour de justice européenne n'a pas invalidé la décision d'adéquation du 10 juillet 2023 de la Commission, qui permet le transfert de données personnelles de citoyens européens vers les États-Unis. Outre qu'elle avait invalidé des décisions similaires dans le passé, depuis 2023, la réélection de Donald Trump a conduit à un

changement de politique assez radical aux États-Unis, faisant apparaître des risques nouveaux. Selon vous, ces risques rendent-ils obsolète la décision d'adéquation de 2023 ?

Enfin, quels outils législatifs le Parlement pourrait-il proposer pour faciliter ou renforcer l'action de la Cnil ?

Mme Marie-Laure Denis. Parmi les mesures de la proposition « omnibus numérique », j'appelle votre attention sur celle de modifier la définition des données à caractère personnel pour la rendre plus restrictive. Une telle proposition est très préoccupante, comme l'ont signalé le Contrôleur européen de la protection des données et le Comité européen de la protection des données dans leur avis conjoint.

La Commission européenne a souhaité transposer la jurisprudence « SRB », née de l'arrêt du 4 septembre 2025 de la Cour de justice de l'Union européenne. De notre point de vue, elle la surtranspose, sans prendre en compte tous les effets négatifs que cela emportera.

Actuellement, si une donnée permet d'identifier une personne, elle est définie comme donnée à caractère personnel, et elle est soumise au RGPD ; si une donnée est, au contraire, impossible à rattacher à une personne, elle est considérée comme donnée anonyme, et le RGPD ne s'applique pas. La proposition de la Commission tend à brouiller cette distinction, en introduisant une dose de relativisme, et sans en encadrer l'usage. Désormais, une donnée susceptible d'être rattachée à une personne pourrait être considérée comme anonyme, et donc être exclue du champ du RGPD, s'il apparaît que celui qui la détient « ne dispose pas de moyens pouvant raisonnablement être utilisés » pour établir le lien entre les données et la personne.

De mon point de vue, ce serait tout sauf de la simplification : ce qui serait une donnée à caractère personnel pour l'un serait une donnée anonyme pour l'autre. Des données identiques prendraient ainsi un double visage. Les responsables de traitement de données devraient porter une appréciation sur leur capacité à identifier ou non les personnes derrière les données qu'ils détiennent. Or une telle appréciation serait subjective : à partir de quel degré d'effort estime-t-on que l'identification n'est pas « raisonnablement » possible ? De plus, cette appréciation devrait évoluer avec les technologies.

Par opportunisme, ou, tout simplement, faute d'avoir compris des règles qui ne sont pas si simples, les responsables de traitement de données risquent de traiter des données à caractère personnel comme des données anonymes, donc de ne pas soumettre leur traitement au RGPD. Ils s'exposeront à des sanctions si nous ne partageons pas leur appréciation. Surtout, ils priveront les utilisateurs des garanties nécessaires, alors mêmes que leurs données sont susceptibles d'être transmises à des tiers, y compris des tiers étrangers. Ainsi, la proposition de la Commission me semble une source d'incohérence et de complexité, plutôt que de simplification. Il faut maintenir la responsabilisation des acteurs, en conservant les règles binaires actuelles – c'est le point qui nous paraît le plus essentiel, à propos de l'« omnibus numérique ».

Après que, en 2020, la Cour de justice de l'Union européenne a invalidé une première décision d'adéquation permettant le transfert des données de l'Union européenne vers les États-Unis, la Commission a négocié un nouvel accord, le DPF (Data Privacy Framework), afin de sécuriser ces transferts, et a pris la décision d'adéquation permettant son entrée en vigueur. La Cnil est particulièrement attentive à ces évolutions.

Tout comme le Comité européen de la protection des données, nous interrogeons régulièrement la Commission européenne sur son analyse de la situation et sur les mesures qu'elle entend prendre pour assurer la protection des données dans le cadre transatlantique – car c'est d'elle que dépendent ces questions.

Pour l'heure, l'administration américaine actuelle ne donne pas de signe qu'elle souhaite abroger l'e*xecutive order* (décret présidentiel) de 2022 sur lequel le DPF repose du côté américain.

En tout cas, le Comité européen de la protection des données est tenu informé. Il a adopté en novembre 2024 son premier rapport sur le cadre Union européenne-États-Unis de protection des données, où il salue les efforts déployés pour mettre en œuvre le DPF, note qu'un certain nombre de garanties ont été apportées, notamment un mécanisme de recours indépendant, mais souligne qu'il faudra s'assurer de son effectivité.

Par ailleurs, la question de la validité du Data Privacy Framework reste pendante devant la Cour de justice de l'Union européenne – au sein de cette commission, vous êtes bien placés pour savoir qu'un contentieux est en cours.

Enfin, je vous remercie pour votre dernière question et votre souci de favoriser la régulation de la Cnil. J'espère que vous ne m'en voudrez pas, mais ma réponse sera très prosaïque. Vous me voyez venir… Même si le contexte budgétaire est très contraint, la Cnil dépend fortement des moyens qui lui sont attribués. D'une manière générale, le Parlement est très sensible à la question – au moins une dizaine de rapports parlementaires soulignent l'intérêt de soutenir les ressources de la Cnil.

Nous comptons trois à quatre fois moins d'agents que nos homologues anglais et allemand, alors que notre périmètre est à peu près le même. Nous vivons dans un monde digitalisé et nous avons évoqué, ne serait-ce que partiellement, l'ampleur de nos missions. Quand la Cnil formule une recommandation sur l'authentification multifacteur, par exemple, je pense qu'elle agit dans l'intérêt général. Si j'ai répondu en évoquant nos moyens, c'est un peu par esprit de boutade, mais pas seulement, car la question est importante.

Je me réjouis beaucoup de nos multiples auditions à l'Assemblée nationale et au Sénat. Nous devons en avoir une vingtaine ou une trentaine par an. Ces deux dernières années, nous avons répondu, je crois, à quarante-cinq questionnaires parlementaires. Nous saurons vous trouver si nous avons des points d'attention à vous soumettre.

Mme Sophie-Laurence Roy, présidente. Je vous remercie pour votre disponibilité et la clarté de vos explications. Nous en avons pris bonne note, y compris de vos problèmes budgétaires.

La séance s'achève à dix-huit heures trente.

Membres présents ou excusés

Présents. - M. Éric Bothorel, M. Jérôme Buisson, Mme Cyrielle Chatelain, M. Philippe Latombe, M. Stéphane Rambaud, Mme Sophie-Laurence Roy, M. Hervé Saulignac, M. Vincent Thiébaut.