ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête concernant l'organisation des élections en France

– Audition, ouverte à la presse, de représentants de la Commission nationale de l'informatique et des libertés (CNIL) : Mme Laurence Franceschini, membre du collège, chargée de la vie politique et citoyenne, M. Mathias Moulin, secrétaire général adjoint, M. Antoine Gaume, ingénieur expert au service de l'expertise technologique, et Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles 2

– Présences en réunion..... 15

Mercredi
9 avril 2025
Séance de 16 heures

Compte rendu n° 29

SESSION ORDINAIRE DE 2024-2025

Présidence de
M. Thomas Cazenave,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures.

La commission entend des représentants de la Commission nationale de l'informatique et des libertés (CNIL) : Mme Laurence Franceschini, membre du collège, chargée de la vie politique et citoyenne, M. Mathias Moulin, secrétaire général adjoint, M. Antoine Gaume, ingénieur expert au service de l'expertise technologique, et Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles.

M. le président Thomas Cazenave. Depuis sa création par la loi du 6 janvier 1978, la CNIL veille à ce que l'informatique soit au service du citoyen et ne porte pas atteinte aux libertés individuelles ou publiques, garantissant ainsi les droits des citoyens. Au cours de nos auditions, nous avons constaté que, bien que l'acte de vote conserve généralement sa forme traditionnelle avec l'utilisation d'un bulletin, les procédures électorales et les campagnes s'appuient désormais sur des systèmes d'information nécessitant la collecte de données essentielles. Dans ce contexte, vous avez d'ailleurs mis en place un observatoire des élections.

Je vous rappelle que 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 le serment de dire la vérité, toute la vérité, rien que la vérité.

(Mme Laurence Franceschini, M. Mathias Moulin, M. Antoine Gaume et Mme Chirine Berrichi prêtent serment.)

Mme Laurence Franceschini, membre du collège, chargée de la vie politique et citoyenne (CNIL). Je vous prie tout d'abord de bien vouloir excuser l'absence de notre présidente, Mme Marie-Laure Denis, retenue par des engagements.

Permettez-moi d'ouvrir mon propos par quelques mots sur les missions générales de la CNIL. Comme vous l'avez rappelé, il s'agit d'une autorité administrative indépendante, instituée par la loi du 6 janvier 1978, modifiée en 2018 à la suite de l'adoption du règlement général sur la protection des données (RGPD). Elle est composée d'un collège de dix-huit membres, parmi lesquels figurent quatre parlementaires, six représentants de juridictions, cinq personnalités qualifiées (dont deux sont désignées par l'Assemblée nationale et le Sénat), deux membres du Conseil économique, social et environnemental (Cese), ainsi que le président de la Commission d'accès aux documents administratifs (Cada). La CNIL comprend par ailleurs une formation restreinte composée de cinq membres, présidée par une personnalité distincte de la présidente de la CNIL et chargée de prononcer des sanctions.

La CNIL se distingue d'autres autorités de régulation par sa compétence transversale en matière de protection des données à caractère personnel, compétence qui s'applique à l'ensemble des secteurs d'activité. Ses missions recouvrent l'information des particuliers, le conseil apporté aux pouvoirs publics, l'autorisation de certains traitements sensibles, l'accompagnement des organismes dans leur mise en conformité, l'élaboration de cadres juridiques tels que des référentiels ou des recommandations, le traitement des réclamations des citoyens, le contrôle des traitements de données ainsi que la faculté de prononcer des sanctions.

En résumé, la CNIL veille à ce que le développement du numérique serve le citoyen sans porter atteinte à l'identité humaine, aux droits de l'homme, à la vie privée, ni aux libertés individuelles ou publiques. Depuis l'entrée en vigueur du RGPD, elle s'attache tout particulièrement à favoriser un environnement de confiance dans le domaine numérique.

S’agissant du cadre juridique applicable à la protection des droits et libertés des citoyens dans le contexte électoral, celui-ci s’articule autour du code électoral, du RGPD et de la loi informatique et libertés. Ces deux derniers textes se caractérisent par leur neutralité technologique, en ce sens qu’ils privilégient l’effectivité de la protection des données personnelles indépendamment des technologies mobilisées.

Parmi les évolutions récentes, il convient de mentionner la réforme des modalités d’inscription sur les listes électorales, adoptée en 2016 et entrée en application en janvier 2019. Cette réforme vise à moderniser les procédures d’inscription, notamment en ce qui concerne les ressortissants de l’Union européenne et les Français établis hors de France, en permettant une mise à jour en continu des listes électorales, afin d'autoriser une inscription au plus près de la date du scrutin, et en instaurant le répertoire électoral unique (REU), qui rend possible la gestion de l’ensemble des informations nécessaires à la tenue et à la mise à jour des listes électorales.

Une autre évolution majeure réside dans l’adoption du règlement européen 2024/900 relatif à la transparence et au ciblage de la publicité à caractère politique, entré progressivement en vigueur depuis le 13 mars 2024. En vertu du premier alinéa de l'article 22 de ce règlement, la CNIL est compétente pour contrôler l'application des articles 18 et 19, qui entrent en application en octobre prochain. Ces derniers viennent renforcer des exigences déjà existantes en précisant que le recours aux techniques de ciblage ou de diffusion d’annonces publicitaires impliquant le traitement de données à caractère personnel n’est autorisé, dans le contexte de la publicité politique en ligne, qu’à certaines conditions strictement définies.

La première impose que la collecte des données s’effectue directement auprès de la personne concernée, laquelle doit avoir donné son consentement préalable. Ce point marque un véritable changement de paradigme en passant d’un système dans lequel l’usager devait se soustraire activement au traitement à un modèle fondé sur une démarche proactive de consentement, ce dernier devant être éclairé.

La seconde condition tient à l’interdiction du profilage fondé sur des données sensibles, parmi lesquelles figurent notamment les opinions politiques. Il convient de souligner que ce règlement ne crée pas un régime autonome applicable aux publicités à caractère politique mais vient plutôt en complément des acquis existants de l’Union européenne en matière de protection des données, et s’inscrit ainsi dans la continuité du RGPD.

Au cours des dernières années, la CNIL a observé un recours croissant des candidats et des partis politiques aux traitements de données à caractère personnel dans le cadre de leurs opérations de communication politique, qu’il s’agisse de démarchage téléphonique, de l’envoi de SMS ou de communications électroniques.

La CNIL a mené plusieurs actions significatives en matière de protection des données dans le contexte électoral. Parmi celles-ci, deux initiatives majeures méritent d’être particulièrement soulignées. D’une part, la délibération du 26 janvier 2012 portant recommandation relative à la mise en œuvre en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques. D’autre part, la création, la même année, de l’observatoire des élections de la CNIL, qui mobilise une douzaine de personnes à chaque élection.

Cet observatoire poursuit trois objectifs principaux. Il vise d’abord au respect de la réglementation relative à la protection des données dans le cadre des opérations de prospection politique, en sensibilisant les candidats et les partis, en recueillant également les signalements

des citoyens s'estimant contactés de manière indue et en assurant la coordination avec d'autres autorités nationales concernées en période électorale, telles que l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), le secrétariat général de la défense et de la sécurité nationale (SGDSN) ainsi que certains organismes européens, tels que l'Organisation pour la sécurité et la coopération en Europe (OSCE), qui joue un rôle important dans la supervision des scrutins.

À l'occasion des élections législatives anticipées organisées l'année dernière, le canal SMS s'est imposé comme le principal mode de prospection politique, représentant plus de la moitié des signalements adressés à la CNIL. Cette évolution marque une rupture notable par rapport aux pratiques observées lors des scrutins antérieurs.

Outre son rôle d'observation, la CNIL est amenée à se prononcer sur les traitements de données personnelles liés à l'organisation des élections. À titre d'exemple, une délibération adoptée en 2022 portait sur un projet de décret modifiant les dispositions du code électoral relatives au vote par correspondance électronique pour l'élection de députés par les Français établis hors de France.

La CNIL s'intéresse d'ailleurs à la question du vote par correspondance électronique depuis 2003. Plusieurs recommandations ont été formulées à ce sujet, notamment en 2003, 2010 et 2019, dans le but de renforcer la sécurité des systèmes de vote par correspondance électronique, c'est-à-dire le vote par internet. Je précise ici que les machines à voter ne font pas partie du périmètre d'action de la CNIL. Ces recommandations visaient d'une part à informer les responsables de traitement des risques réels associés à ces systèmes et, d'autre part, à inciter l'écosystème des fournisseurs de solutions de vote par correspondance électronique à adopter des pratiques plus vertueuses et exigeantes en matière de sécurité et de protection des données personnelles, notamment par l'intermédiaire d'audits indépendants de ces systèmes.

Au début de l'année 2025, la CNIL a proposé une actualisation de cette recommandation, soumise à consultation publique. Les contributions reçues sont en cours d'analyse. De ce travail, conduit en étroite collaboration avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), découlera une recommandation actualisée accompagnée d'un guide apportant des précisions complémentaires.

En ce qui concerne l'entrée en application du règlement européen relatif au ciblage politique, prévue pour le 10 octobre 2025, la CNIL met actuellement en œuvre un plan d'action destiné à clarifier les règles applicables aux partis politiques, aux candidats et aux sous-traitants et à accompagner leur mise en conformité. Ce plan repose sur une analyse juridique approfondie et sur des consultations avec les parties prenantes, en particulier les partis politiques, dans le but de les sensibiliser aux nouvelles obligations et de recueillir leurs observations.

Dans ce même cadre, la CNIL travaille en coordination avec l'Arcom et la direction générale des médias et des industries culturelles (DGMIC) du ministère de la culture pour définir la répartition des compétences prévue par le règlement. Si la CNIL exerce une compétence exclusive en matière de ciblage et de diffusion de publicités politiques reposant sur des données personnelles (articles 18 et 19), d'autres dispositions, notamment celles liées à la transparence, à l'information et à la documentation, relèvent en effet de la compétence d'autres autorités comme l'Arcom.

À l'issue de ces concertations, la CNIL prévoit de mettre à jour sa doctrine et de publier de nouvelles ressources sur son site avant l'entrée en application du règlement le 10 octobre 2025.

S'agissant enfin de l'intelligence artificielle, la CNIL a mené une série de travaux portant sur son impact sur les processus électoraux, en particulier dans le cadre des élections européennes organisées l'an dernier. Les premiers résultats de ces études, menées par le Laboratoire d'innovation numérique de la CNIL (LINC), ont mis en évidence, sans susrprise, le rôle croissant joué par l'intelligence artificielle dans le fonctionnement des réseaux sociaux, des moteurs de recherche et des plateformes, qui constituent désormais des vecteurs majeurs d'information pour les citoyens, de communication pour les formations politiques ou d'influence pour d'autres acteurs intéressés par le résultat des élections.

L'intelligence artificielle peut être mobilisée de plusieurs manières dans le contexte électoral. Elle peut servir à la génération de contenus réels dans le cadre d'une campagne politique, à la promotion directe ou indirecte d'idées mais également, de façon plus préoccupante, à la création de faux contenus pouvant paraître crédibles, contribuant ainsi à la désinformation et à la manipulation de l'opinion publique. Une troisième utilisation concerne la diffusion et la mise en visibilité des contenus, qu'ils soient véridiques ou non, à travers des systèmes automatisés. Enfin, l'intelligence artificielle est également utilisée à des fins de ciblage et de profilage des utilisateurs, notamment dans le cadre des publicités ciblées ou des moteurs de recommandation.

Pour chacune de ces formes d'usage, la CNIL a procédé à une analyse approfondie des dispositions applicables dans le droit en vigueur, qu'il s'agisse du RGPD, du règlement relatif au marché unique des services numériques (DMA) ou encore des textes en cours d'élaboration, tels que le règlement sur l'intelligence artificielle ou celui relatif à la transparence et au ciblage de la publicité à caractère politique. Cet important travail d'analyse doit nécessairement se poursuivre de manière continue.

Je tiens à souligner, pour conclure, l'importance du travail mené par votre commission d'enquête, qui rejoint pleinement les préoccupations de la CNIL, notamment autour de la notion de citoyenneté numérique. Cette notion implique des actions volontaristes en matière d'éducation au numérique, car la formation à la citoyenneté débute dès le plus jeune âge et doit irriguer l'ensemble de nos actions.

M. Antoine Léaument, rapporteur. Pouvez-vous préciser combien de personnes travaillent au sein de la CNIL ?

M. Mathias Moulin, secrétaire général adjoint (CNIL). Environ 300 personnes travaillent au sein de la CNIL. La commission s'articule autour de quatre directions métiers, directement rattachées à ses missions fondamentales. La direction de l'accompagnement, qui regroupe environ soixante agents, se consacre au conseil, à l'élaboration de droit souple, à la formulation d'avis sur les projets de textes législatifs et réglementaires, ainsi qu'à l'accompagnement du Parlement dans ses travaux.

La direction du répressif, forte d'une centaine de collaborateurs, prend en charge l'ensemble de la chaîne répressive, depuis l'instruction des plaintes jusqu'à la conduite des contrôles, en passant par la proposition de mesures correctrices.

La direction des technologies, de l'innovation et de l'intelligence artificielle, essentiellement composée d'ingénieurs, apporte son expertise technique en appui aux deux directions précédemment mentionnées. Elle analyse les dispositifs technologiques, évalue la sécurité des systèmes et intervient notamment sur des sujets tels que le vote électronique.

Enfin, la direction des relations avec le public, qui constitue notre interface directe avec les citoyens, gère le centre d'appels, assure une présence active sur le terrain à travers des actions de sensibilisation et d'information, avec des interventions dans les écoles, et pilote nos dispositifs d'éducation au numérique. Elle conçoit également des ressources pédagogiques à destination de publics variés, comme par exemple un manga destiné aux collégiens qui aborde les enjeux de cyberharcèlement, de cybersécurité et de citoyenneté numérique.

En termes d'effectifs, la direction de l'accompagnement compte environ soixante personnes, celle du répressif une centaine, la direction des technologies une cinquantaine, et la direction des relations avec le public une trentaine. À ces effectifs s'ajoutent les directions support, notamment celles en charge de l'informatique et des finances, qui garantissent le bon fonctionnement opérationnel de l'institution.

M. Antoine Léaument, rapporteur. Concernant le droit souple, votre approche semble privilégier la production de recommandations non contraignantes mais néanmoins largement suivies d'effets. Pourriez-vous clarifier ce que vous entendez exactement par cette notion de droit souple ?

Le domaine de la publicité politique, fortement encadré par le droit électoral, prévoit notamment l'interdiction de publicité dans les six mois précédant une élection sur les réseaux sociaux, règle à la fois peu respectée, notamment pour les élections locales, et mal connue des candidats. Quel est le rôle de la CNIL dans le respect de cette règle ? Cette responsabilité incombe-t-elle à d'autres instances telles que l'Arcom ?

Par ailleurs, les possibilités de ciblage offertes par les réseaux sociaux pour les publicités politiques, âge, genre, pages politiques suivies, sont extrêmement détaillées. Disposez-vous de moyens de contrôle pour vérifier le respect des règles de ciblage par les partis politiques ou les candidats ?

Concernant le REU, relativement récent, il nous a été rapporté qu'il incluait des adresses électroniques et des numéros de téléphone, bien que ces derniers soient encore peu nombreux. Quelle serait la position de la CNIL sur un enrichissement massif de ce répertoire avec ces moyens de contact, dans le but spécifique d'informer les citoyens sur les élections ? Considérez-vous cela comme une menace pour les données personnelles ou, au contraire, comme une utilisation bénéfique pour l'information des citoyens ?

Mme Laurence Franceschini. La CNIL a, à sa disposition, un ensemble d'outils lui permettant d'élaborer des cadres juridiques, parmi lesquels figurent les référentiels, les lignes directrices, les résolutions et les recommandations.

Le droit souple, bien qu'il ne revête pas un caractère contraignant au sens strict, est désormais pleinement pris en compte par le juge administratif. Il ne saurait, dès lors, être assimilé à une simple faculté laissée à l'appréciation des acteurs. Cette approche reflète une méthode d'élaboration normative particulièrement adaptée aux spécificités de l'environnement numérique. Nous constatons d'ailleurs que d'autres autorités ou agences publiques indépendantes se voient désormais dotées d'outils similaires. Cette démarche implique, par ailleurs, une concertation étroite avec les acteurs concernés qui seront appelés à appliquer les règles ainsi définies.

M. Mathias Moulin. En complément, il convient de rappeler que les textes imposent un certain nombre d'obligations, parmi lesquelles figurent des obligations de moyens, en particulier en matière de sécurité. Il ne s'agit nullement d'une obligation de résultat, ce qui serait irréaliste compte tenu de la diversité des situations, mais bien de la nécessité, pour les responsables de traitement, de démontrer qu'ils ont mis en place des moyens adaptés au niveau de risque propre à chaque contexte. Le droit souple intervient précisément pour apporter des clarifications quant aux moyens à mobiliser et aux niveaux d'exigence attendus dans le cadre de ces obligations de moyens. Il permet également d'éclairer les modalités concrètes de mise en œuvre d'une législation dense et parfois complexe.

S'agissant de notre approche en matière de régulation, notamment en ce qui concerne les cookies et, prochainement, les applications mobiles, nous avons adopté une démarche séquencée pour traiter les enjeux à caractère systémique. Celle-ci repose sur une phase de concertation et de consultation sur un projet, suivie de l'élaboration d'un projet de droit souple visant à expliciter la norme. Ce projet est ensuite soumis à consultation publique, puis consolidé et mis en œuvre, avant de faire l'objet de contrôles sur le terrain, destinés à en évaluer la compréhension et l'application effective.

En cas de manquement manifeste au droit, et non à la seule recommandation, des sanctions peuvent être prononcées.

Mme Laurence Franceschini. Cette approche s'inscrit pleinement dans l'esprit du RGPD, qui promeut une responsabilisation accrue des acteurs. La souplesse dont il est ici question relève avant tout d'une pédagogie des textes, visant à expliciter de manière concrète l'application des règles législatives ou réglementaires dans un environnement en perpétuelle évolution. Il s'agit d'un outil de régulation moderne, qui permet une intervention rapide, dans le respect du cadre légal, afin de mieux appréhender la diversité des situations rencontrées.

S'agissant de l'article L. 52-1 du code électoral, la CNIL demeure strictement dans le périmètre de ses compétences, à savoir la protection des données à caractère personnel. La sanction, quant à elle, relève du juge de l'élection, comme le confirme la jurisprudence établie en la matière.

M. Antoine Léaument, rapporteur. Disposez-vous de la capacité technique de vérifier le respect des règles en matière de ciblage dans les publicités à caractère politique ?

Certaines publicités politiques peuvent en outre être diffusées de manière déguisée, notamment lorsqu'elles émanent d'acteurs médiatiques qui, sous couvert de la liberté de la presse, peuvent promouvoir des contenus à forte orientation politique en utilisant leur puissance financière. Cette pratique peut s'étendre aux réseaux sociaux ainsi qu'à d'autres sites en ligne, recourant à des outils tels que Google AdSense, voire à des sites spécifiquement créés à cette fin. Dans ce contexte, quelle est votre capacité effective de contrôle face à ces formes dissimulées de publicité politique et aux mécanismes de ciblage qu'elles peuvent indirectement mettre en œuvre ?

Mme Laurence Franceschini. Votre observation est très juste et s'inscrit dans le prolongement de notre recommandation de 2012 relative aux fichiers constitués par les partis politiques.

Nous exerçons une vigilance renforcée durant les périodes pré-électorales et électorales, en nous appuyant notamment sur les signalements que nous recevons. Il s'agit néanmoins d'un phénomène pour lequel il nous faut encore renforcer notre capacité

d'anticipation et de préparation. L'exemple de la Roumanie, où la puissance algorithmique du ciblage, heureusement détectée, a conduit à l'annulation d'un scrutin, soulève en effet des interrogations majeures quant à l'intégrité des processus démocratiques dans un contexte de numérisation croissante.

M. Mathias Moulin. Jusqu'à présent, les observations fondées sur les signalements que nous recevons indiquent que la majorité des opérations de propagande et d'action politique s'effectue principalement par l'envoi de SMS, l'utilisation d'automates d'appel et de courriels. Nous nous trouvons assurément à un point de bascule mais, lors de la dernière séquence électorale en France, nous n'avons pas constaté d'actions massives menées via les réseaux sociaux, ni d'opérations de *deep fake* comme cela a pu être observé en Roumanie. Il est néanmoins manifeste que nous sommes passés dans une nouvelle ère, marquée par une évolution technologique particulièrement rapide.

S'agissant de notre capacité de contrôle, la CNIL est fondée à mener à la fois des contrôles sur pièces, des contrôles en ligne, des contrôles sur place ainsi que sur auditions. Nous avons la possibilité de demander la transmission de documents, de procéder à des extractions sur site, de réaliser des vérifications directement en ligne et même de créer des comptes fictifs à des fins d'observation, afin d'analyser les messages de prospection reçus en fonction des caractéristiques renseignées.

Concernant plus spécifiquement le contrôle des réseaux sociaux, la majorité de ces plateformes sont établies à l'étranger, principalement aux États-Unis, ce qui limite notre capacité d'investigation directe. Dans le cadre du RGPD, nous agissons selon le principe du guichet unique, l'autorité compétente pour instruire les dossiers étant celle du pays où l'entreprise a son établissement principal. Ainsi, pour des entités telles que Google ou Meta, c'est l'autorité irlandaise qui exerce le rôle de chef de file pour procéder aux investigations. Nous entretenons une coopération étroite avec cette autorité, à laquelle nous transmettons nos plaintes et que nous pouvons inciter à intervenir.

M. Antoine Léaument, rapporteur. Dans le cas spécifique des publicités à caractère politique, le dispositif actuellement en vigueur permet, sauf erreur, d'identifier l'annonceur. Cette exigence de transparence devrait, en théorie, vous autoriser à exercer un contrôle directement auprès de l'annonceur, y compris sur les critères de ciblage employés.

Votre compétence en matière de contrôle devrait vous permettre d'examiner les modalités de ciblage mises en œuvre, non pas en sollicitant des informations auprès des autorités irlandaises, mais en demandant un accès direct aux éléments commandés par l'annonceur.

M. Mathias Moulin. Il convient de prendre en considération les limites inhérentes aux systèmes distants, les informations détaillées n'étant pas nécessairement stockées sur le terminal de l'utilisateur. Si nous avons la faculté d'interroger l'annonceur et de solliciter la documentation afférente, l'accès aux configurations techniques précises au sein des systèmes utilisés peut s'avérer sensiblement plus complexe.

Notre capacité de vérification se trouve ainsi restreinte lorsqu'il s'agit de services mis en œuvre par des réseaux sociaux établis à l'étranger, recourant à des infrastructures de type cloud. Dans ces configurations, notre accès direct aux machines, aux systèmes et aux paramètres spécifiques est considérablement limité.

Mme Laurence Franceschini. S’agissant du REU et de la possibilité d’y adjoindre des numéros de téléphone en complément des adresses électroniques, la CNIL a exprimé sa position lors de l’examen des textes fondateurs en 2021. Nous faisons preuve, à cet égard, d’une vigilance particulière à la fois sur la proportionnalité des coordonnées collectées au regard de l’objectif poursuivi et sur la durée de conservation des données enregistrées. Notre recommandation était, en ce sens, de limiter cette durée de conservation à six mois.

M. Mathias Moulin. Il est en effet essentiel que les catégories de données collectées soient strictement alignées sur les finalités définies pour le REU, telles que l’inscription sur les listes électorales ou la mise à jour des informations afférentes.

L’introduction d’une nouvelle finalité, telle que la communication, nécessiterait une modification du cadre juridique existant car les durées de conservation sont déterminées en fonction des finalités poursuivies. Le décret en vigueur prévoit ainsi environ cinq régimes de conservation distincts, dont la durée varie selon l’usage envisagé.

Le principe fondamental reste l’adéquation entre la durée de conservation et la finalité poursuivie. Dès lors, l’ajout d’une nouvelle finalité supposerait de définir, de manière cohérente, les catégories de données nécessaires ainsi qu’une durée de conservation adaptée.

M. Antoine Léaument, rapporteur. La question des radiations électorales, en particulier lorsqu’elles sont motivées par une perte d’attache communale, suscite des préoccupations légitimes au sein de notre commission. La procédure actuellement en vigueur, qui repose sur l’envoi d’un courrier suivi d’une relance peut conduire, dans certains cas, à des radiations injustifiées.

L’idée de recourir à des moyens de communication plus directs, tels que les SMS ou les appels téléphoniques, pourrait ainsi considérablement améliorer ce processus. Elle permettrait de s’assurer, de manière plus fiable, que les électeurs ont bien reçu l’information avant qu’une décision de radiation ne soit prise. Une telle approche pourrait contribuer à résoudre les difficultés observées dans certaines communes, où des radiations massives ont engendré des complications notables, notamment pour la réinscription le jour du scrutin.

Bien que je souscrive pleinement aux actions de la CNIL en matière de protection des données personnelles, il me semble donc indispensable de rechercher un équilibre entre cette exigence de protection et la préservation du droit fondamental de participation électorale.

Mme Laurence Franceschini. Cette proposition pourrait effectivement être intégrée comme une nouvelle finalité dans le cadre réglementaire existant. Notre rôle est de veiller à ce que les finalités soient clairement définies et que les données collectées leur correspondent. Si cette finalité est inscrite dans le texte réglementaire, elle peut se concevoir.

M. Mathias Moulin. Il est important de préciser que nous parlons ici d'une modification potentielle au niveau du décret, qui nécessiterait la consultation préalable de la CNIL et du Conseil d’État.

Dans la mesure où nous n’avons pas été saisis de manière formelle sur cette question spécifique, notre première démarche consisterait à vérifier si la finalité nouvellement envisagée est conforme à la loi sur laquelle repose le décret. Notre analyse s’articulerait autour de trois axes fondamentaux, que sont la légitimité et la précision de la finalité poursuivie, la proportionnalité des données collectées au regard de cette finalité et, enfin, l’adéquation de la durée de conservation envisagée.

M. le président Thomas Cazenave. La CNIL est particulièrement bien placée pour observer les menaces pesant sur la qualité de l'information, sa manipulation, ainsi que l'usage qui est fait des données personnelles et des préférences individuelles par les algorithmes.

Considérez-vous que les réseaux sociaux constituent aujourd'hui une nouvelle forme de menace pour le bon déroulement des élections en France ? Ce constat justifie-t-il les investissements particuliers que vous consacrez notamment à l'intelligence artificielle ? Estimez-vous, au sein de la CNIL, que ces évolutions font émerger de nouveaux risques ?

Je souhaiterais, à cet égard, mettre en perspective cette problématique avec le contrôle extrêmement rigoureux exercé sur les campagnes menées par SMS ou par courriel, dont l'impact sur l'opinion publique semble, à bien des égards, sans commune mesure avec les opérations massives pouvant être conduites à l'aide d'outils plus puissants. Comment le collège de la CNIL appréhende-t-il cette nouvelle donne ?

Mme Laurence Franceschini. Vous posez une question très pertinente. Pour le collège de la CNIL, il ne s'agit nullement de considérer l'univers des réseaux sociaux comme intrinsèquement hostile, prédateur ou systématiquement orienté vers la manipulation de l'information et des esprits.

Cela étant dit, il serait illusoire de nier l'existence de risques réels, multiples et complexes. Parmi ceux-ci, la question de la souveraineté numérique confère aux réseaux sociaux une dimension singulière dans les menaces qu'ils peuvent faire peser sur l'intégrité du débat public et, plus largement, sur la manipulation des consciences.

Pour autant, la CNIL doit s'en tenir strictement à son champ de compétences. S'agissant des campagnes menées par SMS, il s'agit sans ambiguïté d'un sujet relevant de la manipulation de données à caractère personnel. À l'inverse, les réseaux sociaux, par leur capacité à façonner l'opinion de manière massive, exigent une approche plus transversale, fondée sur une coopération étroite entre autorités indépendantes. À cet égard, je pense en particulier à la collaboration engagée dans le cadre de la convention signée en juin dernier entre l'Arcom, la CNIL et la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), visant à la mise en œuvre du règlement sur les services numériques. Cette coopération repose notamment sur le partage d'informations recueillies et sur les exigences accrues de transparence imposées par le texte, qui sont susceptibles de jouer un rôle déterminant.

M. le président Thomas Cazenave. En partant de l'hypothèse que la manière dont nous sommes informés et ciblés en termes de flux d'information sur différents réseaux constitue également une forme d'utilisation algorithmique des préférences individuelles, ne pensez-vous pas que cela relève précisément de votre champ d'action ?

Mme Laurence Franceschini. S'il y a un profilage avéré, nous sommes effectivement pleinement dans notre champ de compétences.

M. le président Thomas Cazenave. Sans être un spécialiste, si le principe même des réseaux sociaux consiste à exploiter les préférences et caractéristiques individuelles pour diffuser ensuite une information ciblée, alors cette menace et ce risque ne relèvent-ils pas pleinement de vos attributions et de vos missions ?

Quelles conclusions en tirez-vous ? Je vous invite à prolonger votre réflexion au-delà de la stricte question du recueil du consentement à la réception d'une communication. Ne sommes-nous pas, ici, face à un enjeu d'une ampleur bien supérieure aux problématiques plus classiques que représentent les campagnes par SMS ou par courrier électronique ?

M. Antoine Léaument, rapporteur. Pour approfondir cette réflexion, je souhaiterais revenir sur un point soulevé lors de l'audition du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), au cours de laquelle il nous a été indiqué que les pratiques d'Elon Musk en France relevaient de l'ingérence.

Dans cette perspective, et compte tenu des propos récemment tenus par le président de la République à propos de la mise en avant de certains contenus sur les réseaux sociaux, considérez-vous qu'une personne détenant une telle plateforme, capable de promouvoir des contenus dans de nombreux espaces et, potentiellement, d'opérer un ciblage algorithmique, puisse tenter d'influencer les esprits et, par voie de conséquence, le résultat d'un scrutin électoral ?

Cette interrogation prend une acuité particulière à la lumière des événements observés en Allemagne, où il semble que des efforts aient été déployés en vue de favoriser spécifiquement le parti Alternativ für Deutschland (AFD), dont les positions apparaissent proches de celles défendues par M. Musk dans son propre pays.

Mme Laurence Franceschini. Je considère effectivement qu'il existe un risque majeur en la matière. L'utilisation des algorithmes relève incontestablement du champ de compétences de la CNIL. La mise en œuvre et l'entrée en vigueur du règlement européen de 2024, consacré précisément à la transparence et au ciblage de l'information, constituent à cet égard une opportunité déterminante pour s'emparer pleinement de cette problématique et intégrer cette dimension de manière proactive dans la perspective des prochaines échéances électorales.

M. le président Thomas Cazenave. S'il apparaissait qu'un réseau social, par le biais du fonctionnement de son algorithme, privilégiait systématiquement la mise en avant de contenus fortement orientés politiquement à destination de ses utilisateurs, la CNIL serait-elle, d'une part, fondée à s'autosaisir, et, d'autre part, habilitée à ouvrir la boîte noire et à procéder elle-même aux vérifications nécessaires, en accédant directement à l'algorithme ? Les capacités de contrôle sur pièces et sur place dont dispose la CNIL lui permettraient-elles d'exercer véritablement sa capacité d'intervention ?

M. Mathias Moulin. La CNIL est compétente dès lors qu'il existe un traitement de données à caractère personnel. Dès lors que de telles données sont mobilisées, nous sommes habilités à intervenir, sous réserve toutefois des règles relatives à l'établissement principal qui déterminent si la CNIL agit en tant qu'autorité chef de file ou en tant qu'autorité concernée.

S'agissant des campagnes par SMS ou par courriel, mes propos faisaient référence à une séquence électorale passée et aux constats issus de nos observatoires. Dans la mesure où les citoyens nous ont eux-mêmes saisis de ces sujets, nous avons agi sur ces vecteurs de communication, mais cela ne signifie en rien que nous nous désintéressons d'autres aspects. Il est d'ailleurs logique que nous n'ayons pas été saisis, jusqu'à présent, sur la question de la manipulation algorithmique, dans la mesure où celle-ci demeure opaque et passe inaperçue. Nous verrons si des utilisateurs avertis nous interpellent sur ces problématiques à l'occasion du prochain observatoire des élections.

Il s'agit précisément de l'objet du travail conduit dans le cadre de la mise en œuvre du règlement relatif au ciblage politique. Ce texte vise principalement l'usage de données par les plateformes et les réseaux sociaux à des fins de ciblage électoral. Les règles, claires et rigoureuses, incluent l'interdiction de tout ciblage fondé sur des données sensibles, la nécessité du consentement explicite de la personne concernée et l'exigence d'une collecte directe des données. Notre mission consiste à vérifier que ces obligations sont effectivement respectées lors de leur mise en œuvre.

En ce qui concerne les responsabilités juridiques, la loi informatique et libertés opère une distinction fondamentale entre le responsable de traitement, qui détermine les finalités et les moyens du traitement, et le sous-traitant, qui agit pour le compte du responsable. Le règlement relatif au ciblage politique introduit des catégories supplémentaires, plus détaillées, qui impliquent une répartition des responsabilités légèrement différente. Il nous appartient de faire converger ces deux cadres réglementaires.

L'un des enjeux centraux de notre action réside dans l'application concrète du RGPD au contexte politique. Lorsqu'un parti politique recourt à un réseau social à des fins de ciblage, nous procédons à une vérification rigoureuse du respect des règles applicables. En cas de manquement constaté, nous n'hésitons pas à engager des procédures de sanction. Dans l'hypothèse d'une ingérence étatique, où une personne ou un État mobilise les moyens d'un réseau social pour mener une action d'influence, cette entité est considérée comme responsable du traitement et peut donc faire l'objet de sanctions. La CNIL a d'ailleurs déjà pris des décisions importantes concernant l'ensemble des géants du numérique, dits Gafam, notamment sur des questions liées aux cookies, aux politiques de confidentialité ou encore à la transparence des traitements.

Si un réseau social décide demain d'utiliser ses ressources pour influencer une élection, notre priorité ne réside pas dans l'influence en tant que telle, mais bien dans le respect des conditions régissant le traitement des données personnelles, à savoir l'information des personnes concernées, le recueil de leur consentement et la possibilité effective d'exercer leurs droits.

Mme Laurence Franceschini. Bien qu'il n'existe pas de régime d'autorisation préalable, le plan d'action évoqué aboutira à la mise en place de ressources spécifiques pour faire face à ces risques. Notre approche ne se limite pas à une intervention *a posteriori*, une fois le préjudice causé, pour déterminer la nature de ce préjudice et identifier les responsables à sanctionner. Il est crucial de souligner l'importance d'un cadrage général en amont.

M. Antoine Léaument, rapporteur. Avez-vous identifié certains fournisseurs de réseaux sociaux dont les pratiques, qu'il s'agisse de l'utilisation des données personnelles ou de la diffusion de contenus, vous apparaîtraient comme problématiques ?

Cette question revêt une acuité particulière lorsque Viginum nous indique qu'une personne détenant un réseau social se livre à des activités d'ingérence sur le territoire national. Les modalités techniques de cette ingérence, en particulier l'usage d'algorithmes destinés à mettre en avant certains contenus, constituent le cœur des préoccupations de notre commission d'enquête. En poussant le raisonnement, nous sommes confrontés à l'hypothèse dans laquelle un ministre d'une puissance étrangère, porteur d'une orientation politique spécifique et disposant d'une capacité d'influence significative à l'échelle mondiale, utiliserait un réseau social comme vecteur de diffusion d'une forme de propagande. Cette dernière viserait à la fois à servir les intérêts de l'État concerné et à favoriser certaines forces politiques déterminées. Une telle

situation soulève des enjeux fondamentaux en matière de souveraineté pour notre pays, ainsi que des interrogations relatives à l'accès aux données, qui relèvent directement des compétences de la CNIL, notamment lorsqu'il s'agit d'apprécier la véracité des contenus diffusés.

Je souhaiterais ainsi savoir si la CNIL a d'ores et déjà engagé des travaux sur ce sujet, formulé des recommandations ou conduit des analyses. Êtes-vous en mesure, dans le cadre de cette commission d'enquête, d'adresser des observations, des alertes ou des critiques à la représentation nationale, ou bien s'agit-il d'un domaine qui, à ce jour, n'a pas encore été formellement investi par votre institution ?

Mme Laurence Franceschini. Ce sujet se trouve, en effet, au cœur de nos préoccupations et ne saurait être réduit au seul réseau social que vous évoquez. Il peut concerner d'autres plateformes, ce qui confère à la question de la souveraineté une importance toute particulière. Sous l'impulsion de la présidente de la CNIL, nos équipes font preuve d'une vigilance constante à l'égard de ces problématiques. Bien que ce thème n'ait pas été abordé récemment au niveau du collège, il fait néanmoins l'objet d'une surveillance attentive et régulière.

Je tiens également à réaffirmer que cette problématique sera pleinement intégrée aux conclusions de notre plan d'action relatif à la mise en œuvre du règlement européen sur le ciblage politique.

M. Mathias Moulin. Notre perspective dépasse le seul champ de l'influence politique, pour englober également l'usage des algorithmes à des fins commerciales. Cette problématique a déjà fait l'objet d'investigations approfondies, notamment de la part de l'autorité britannique de protection des données, qui a prononcé des sanctions en la matière. Nous avons participé activement à ces travaux ainsi qu'aux échanges qu'ils ont suscités.

Nous sommes pleinement conscients des enjeux en présence et avons d'ores et déjà formulé des recommandations concernant le traitement des données personnelles par les réseaux sociaux. Toutefois, notre champ d'action demeure encadré par les règles de compétence territoriale et nous ne pouvons intervenir directement que sur les responsables de traitement relevant de notre compétence territoriale. Pour les problématiques de portée plus globale, nous œuvrons dans le cadre d'une coopération renforcée au sein du collectif européen.

Notre travail actuel consiste à articuler le Digital Services Act (DSA), le règlement sur le ciblage politique et le RGPD et à élaborer un modèle d'intervention cohérent, intégrant les exigences de ces différentes législations. La question des algorithmes, de leur influence et des bulles de filtres qu'ils peuvent générer, constitue un point central de nos préoccupations. Sur ces sujets, nous avons déjà publié des lignes directrices, émis des recommandations et mené des investigations.

Nous réfléchissons par ailleurs à l'élaboration d'un plan d'action systémique, impliquant conjointement les autorités de protection des données et l'Arcom, afin de mettre en œuvre de manière effective les textes existants. Plusieurs de ces textes étant récents, leur articulation demande un travail rigoureux et coordonné.

Il convient également de rappeler que la menace est protéiforme et que l'influence ne suppose pas nécessairement le contrôle direct d'une plateforme. Le simple recours à des influenceurs rémunérés ou à des campagnes ciblées peut suffire à exercer une pression significative sur l'opinion publique.

Nous portons également une attention particulière aux évolutions liées à l'intelligence artificielle, en particulier générative, et à ses effets potentiels sur la manipulation des processus électoraux et les enjeux démocratiques. Le règlement sur l'intelligence artificielle (RIA) prévoit d'ailleurs une régulation spécifique pour les systèmes d'IA à haut risque dans ce domaine.

En résumé, nous disposons d'ores et déjà d'une base solide de connaissances sur le fonctionnement des algorithmes, fondée sur des contrôles, des recommandations et des mesures prises, mais l'émergence de nouvelles technologies et de nouvelles réglementations requiert une articulation complexe dans le périmètre de nos compétences, en lien étroit avec les autres autorités concernées. Le plan d'action que nous préparons, dont une première déclinaison est attendue pour le mois d'octobre, aura pour objectif de clarifier les aspects juridiques en jeu et de formuler des recommandations concrètes. Il sera suivi d'une phase de vérification et de mise en œuvre.

M. Antoine Léaument, rapporteur. Même si mes propos précédents visaient en effet un réseau social en particulier, notre intérêt ne se limite pas à cette seule plateforme. Dans cette perspective, certains d'entre eux suscitent-ils, à vos yeux, des inquiétudes particulières ?

Une telle information nous serait précieuse pour orienter utilement nos prochaines auditions, dans la mesure où vous avez peut-être d'ores et déjà identifié certaines plateformes présentant des difficultés spécifiques au regard des enjeux que nous avons abordés au cours de cette audition.

M. le président Thomas Cazenave. Pour être plus précis, traitez-vous actuellement des enquêtes concernant les algorithmes d'une plateforme ou d'un réseau social spécifique sur cette base ?

M. Mathias Moulin. La CNIL ne mène, à ce jour, aucun contrôle sur un réseau social en lien avec des dispositifs de ciblage politique mis en œuvre. Des missions de vérification, menées notamment en coopération avec l'autorité irlandaise, sont toutefois en cours sur ces plateformes. Ces procédures portent principalement sur des enjeux liés au recueil du consentement, au modèle économique des acteurs concernés ainsi qu'au traitement des données personnelles. Elles n'intègrent pas encore, à ce stade, les problématiques directement liées au ciblage politique.

Mme Laurence Franceschini. La CNIL est pleinement consciente de l'importance capitale de ces questions, que je n'hésiterais pas à qualifier d'enjeu de civilisation. Le caractère profondément multiforme de cette problématique exige une réponse à la hauteur des défis posés et justifie pleinement le recours à une coopération étroite entre l'ensemble des entités concernées, ce qu'on appelle l'interrégulation.

La séance s'achève à dix-sept heures quarante.

Membres présents ou excusés

Présents. – M. Thomas Cazenave, M. Antoine Léaument, M. Stéphane Rambaud