ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mardi
28 avril 2026
Séance de 16 heures 30

Compte rendu n° 58

Compte rendu

Commission des affaires étrangères

SESSION ORDINAIRE 2025-2026

Co-Présidence de

M. Bruno Fuchs,
Président de la commission des affaires étrangères, puis de
M. Alain David,
Vice-président,

et de

M. Alexandre Portier,
Président de la commission des affaires culturelles et de l'éducation

ASSEMBLÉE NATIONALE

La commission procède à l'audition à huis clos, conjointe avec la commission des affaires culturelles et de l'éducation, de M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale, et de M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), sur la lutte contre les ingérences étrangères dans les processus électoraux.

La séance est ouverte à 16 h 30.

Co-présidence de M. Bruno Fuchs, président de la commission des affaires étrangères, puis de M. Alain David, vice-président, et de M. Alexandre Portier, président de la commission des affaires culturelles et de l'éducation

M. le président Alexandre Portier. Cette audition se déroulant à huis clos, j'invite nos collègues à faire preuve de la plus grande discrétion quant au contenu de nos futurs échanges, du moins jusqu'à la publication du compte rendu. Il me semblait intéressant que nous puissions avoir l'échange le plus franc, le plus direct et le plus ouvert possible avec les responsables du secrétariat général de la défense et de la sécurité nationale (SGDSN) sur des sujets décisifs pour l'avenir.

Après les élections municipales et alors que des échéances électorales majeures se profilent, il nous a semblé utile d'échanger sur un phénomène qui, s'il n'est pas nouveau, tend à prendre des formes et une ampleur inédites. Les outils à disposition des acteurs malveillants se sont multipliés, ont gagné en sophistication et peuvent causer des dégâts majeurs pour des coûts modiques. En outre, alors que les acteurs étatiques susceptibles de s'adonner à ce type d'opérations de déstabilisation étaient jusqu'alors relativement bien identifiés, l'évolution politique de certains pays nous conduit à actualiser notre grille de lecture en la matière.

Au-delà de cet aspect, que le président Fuchs évoquera certainement, la question des ingérences étrangères dans les processus électoraux intéresse très directement la commission des affaires culturelles, car ces actions sont susceptibles d'emprunter l'ensemble des canaux de communication, en prenant notamment la forme d'opérations de manipulation de l'information dans les médias classiques ou en ligne. Par ailleurs, au-delà de la production de fausses nouvelles, on peut imaginer des opérations de nature plus technique visant à affecter le fonctionnement normal des médias, support incontournable de communication et de promotion du débat public en période électorale.

M. le président Bruno Fuchs. Le sujet absolument central qui nous réunit est en effet un sujet de préoccupation commune à nos commissions.

Nous avons vu de premières ingérences lors de la campagne présidentielle de 2017, puis, très rapidement, au Sahel – notamment dans les pays de la future AES (Alliance des États du Sahel). À l'époque, la réaction politique a été de considérer ces faits comme relativement marginaux, localisés, et de les minorer : nous n'avons pas pris conscience de l'importance du phénomène. À partir de 2019, nous avons compris que ce mode opératoire devenait beaucoup plus complexe, massif, et menaçait une partie de nos intérêts. Nous avons toujours un peu de retard sur les événements. En 2023 et 2024, en Moldavie, en Géorgie, en Roumanie, le sujet a été chaque fois abordé par mes interlocuteurs – le premier ministre, le ministère des affaires étrangères ou des membres du parlement. Ces ingérences directes de la part de la Russie ont pris diverses formes : achat de voix, pressions, beaucoup de désinformation. Par exemple, en Moldavie, l'influence russe se serait exercée sur 300 000 à

350 000 voix – souvent avec succès : rapporté à 1,5 million de votants, c'est un levier important.

Désormais, la prise de conscience est réelle. Nous disposons d'une structure dédiée, chargée de nombreuses missions. Nous avons atteint un bon, voire très bon niveau opérationnel dans l'identification et la dénonciation des phénomènes – à plusieurs reprises, le ministre de l'Europe et des affaires étrangères a utilisé les travaux du SGDSN pour dénoncer des campagnes de désinformation –, mais le travail de réfutation demeure imparfait. Nous ne sommes pas complètement armés dans ce domaine.

Nous manquons de moyens, notamment les médias officiels : Russia Today a davantage de ressources que France Médias Monde, par exemple, qui fait un très bon travail de *debunking* partout dans le monde, mais dont les moyens baissent. Sans parler de la désinformation par des moyens plus informels et moins connus, du moins quant aux sources de financement. Nous manquons également d'outils de réfutation ; peut-être faudra-t-il passer pour cela par des acteurs privés. C'est une piste que je vous soumets, car les comptes identifiés comme institutionnels n'ont ni la même puissance ni le même écosystème pour combattre la désinformation. Il y va aussi du respect des engagements et principes de la France de ne pas utiliser les mêmes méthodes que certains.

M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale. C'est un plaisir et un honneur pour nous d'être présents devant vous. Il n'est pas fréquent que le secrétaire général de la défense et de la sécurité nationale et le chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) interviennent conjointement devant deux commissions comme les vôtres – nous sommes plus habitués à venir devant la commission de la défense. Cette approche dit quelque chose de notre époque et du sujet qui nous occupe.

Avant d'en venir à la dimension électorale du sujet, permettez-moi de décrire le cadre plus large de la lutte contre les manipulations de l'information et les ingérences numériques étrangères (INE), une politique publique à part entière depuis les années 2020-2021.

En 2025, à la demande du président de la République et du premier ministre, nous avons mis à jour nos grandes stratégies : la revue nationale stratégique (RNS), qui est la clé de voûte et dont toute une partie est consacrée aux manipulations de l'information – une des nombreuses menaces hybrides que nous y avons listées –, mais aussi la stratégie nationale spatiale, la stratégie nationale de cybersécurité, la feuille de route de l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (INESIA). Nous avons publié le guide « Tous responsables » dans le cadre de la stratégie nationale de résilience, et élaboré la dernière-née de nos stratégies, la stratégie nationale de lutte contre les manipulations de l'information (LMI) d'origine étrangère, publiée en février 2026. Chaque fois – en particulier pour la revue nationale stratégique et la stratégie nationale de lutte contre les manipulations de l'information –, nous avons eu à cœur d'associer très étroitement le Parlement à nos travaux, par l'intermédiaire des commissions principalement compétentes de l'Assemblée nationale et du Sénat. De mon point de vue, ce travail a été extrêmement profitable et nous avons intégré l'ensemble de vos contributions.

L'élaboration de la stratégie nationale de lutte contre les manipulations de l'information d'origine étrangère a été fondée sur une approche nouvelle. Au-delà du Parlement, nous avons mené de larges consultations incluant l'ensemble de l'écosystème de

lutte contre les manipulations de l'information et les ingérences numériques étrangères – experts, chercheurs, scientifiques, universitaires, organisations non gouvernementales (ONG), associations. Pour la première fois s'agissant d'un document stratégique encadrant nos objectifs de défense et de sécurité nationale, nous avons aussi mené une consultation citoyenne par l'intermédiaire de la plateforme make.org, qui a rencontré un grand succès avec près de 5 000 contributions et avis.

Une vraie stratégie de lutte contre les manipulations de l'information repose évidemment sur les moyens de l'État – j'y reviendrai –, mais aussi sur la résilience de toute la société. Ce n'est pas un hasard si le premier pilier de la stratégie y est consacré : nous sommes chargés des politiques de défense et de sécurité nationale, mais nous savons que le succès de la stratégie nécessite d'aller bien au-delà de ces domaines et s'étend notamment à l'information et à l'éducation des citoyens – y compris très jeunes. Le premier pilier de la stratégie prévoit donc notamment la création d'une académie de la lutte contre les manipulations de l'information et la préparation de programmes éducatifs destinés aux enseignants et au monde éducatif et pédagogique, afin d'intégrer cette dimension le plus tôt possible dans les différents programmes.

Pour amener l'ensemble du monde de la production de l'information, les ONG et les citoyens à être acteurs de la lutte contre les manipulations de l'information, il faut définir correctement la menace. Or j'ai constaté que l'on prenait parfois un mot pour un autre, y compris dans les travaux internes à l'État, auxquels la quasi-totalité des ministères – pas seulement les ministères régaliens, le ministère de l'Europe et des affaires étrangères et le ministère de la culture – a été associée. *Fake news*, désinformation, manipulation de l'information, ingérence numérique étrangère : ces mots, ces concepts ont chacun une définition précise, y compris en droit ; ils ne sont pas totalement interchangeables. Une bonne stratégie de lutte contre les manipulations de l'information, c'est aussi bien nommer ce contre quoi nous luttons et s'adapter à chacune de ses dimensions.

Cela suppose aussi de savoir qui fait quoi. Je vous expliquerai comment nous pensons l'articulation entre l'action du SGDSN en tant que coordinateur interministériel, celle de Viginum en tant qu'expert technique et celle du Quai d'Orsay – le ministre de l'Europe et des affaires étrangères a donné une nouvelle ampleur à cette partie spécifique de notre politique étrangère, qui s'intègre dans un ensemble plus large.

Sur tous ces points, je vous renvoie à la stratégie, construite et conçue pour être aussi un outil pédagogique.

J'en viens à la mobilisation de l'État au sein du SGDSN et de Viginum. J'avais eu la chance d'être de l'autre côté de la table au moment de la naissance de Viginum ; lorsque j'ai pris mes fonctions de SGDSN en mars dernier, de retour de Téhéran, j'ai retrouvé un dispositif opérationnel relativement précurseur en Europe. Parfois, nous nous flagellons ; il faut aussi savoir reconnaître ce que nous avons bien fait. La création de Viginum fait partie de ces mesures efficaces décidées assez tôt dans le processus de prise de conscience de la menace : la réflexion lancée en 2020 a abouti à la publication, en juillet et décembre 2021, des deux décrets fondateurs.

Les choix d'alors restent au cœur des équilibres qui fondent cette réussite opérationnelle et technique.

Tout d'abord, une approche technique et technologique. Viginum a vocation non pas à être le ministère de la vérité du gouvernement français, mais à détecter, grâce à toute une série de moyens techniques et technologiques, les tentatives d'acteurs étrangers de s'immiscer – de s'ingérer, au plein sens du terme – clandestinement dans notre débat numérique, en se faisant passer pour des acteurs légitimes de celui-ci, afin de chercher à l'influencer à leur profit et dans leur intérêt. Il peut s'agir de promouvoir des narratifs, dans une logique de propagande classique, ou de semer le chaos et la confusion – j'y reviendrai en abordant la dimension électorale. Car il ne faut pas croire que la stratégie de lutte contre les manipulations de l'information et les ingérences numériques étrangères se résume à une question de narratif et de substance. Le travail de Viginum consiste d'abord à dévoiler des architectures et infrastructures d'attaque par lesquelles des acteurs étrangers, étatiques ou non, cherchent à s'immiscer numériquement dans le débat politique national. C'est un travail souterrain mais nécessaire, qui requiert des moyens techniques importants. L'approche technique et technologique, au centre de la création de Viginum, reste au cœur de son métier, y compris du point de vue de l'affectation de ses moyens et ressources.

Ensuite, nous ne nous intéressons qu'aux ingérences numériques d'origine étrangère. C'est un élément fondamental, car cette dimension nous prémunit contre le risque d'une surveillance de masse qui porterait sur ce que les Français disent aux Français sur les Français. Comme j'ai pu le dire dans d'autres enceintes, ce que nous cherchons à préserver, c'est la souveraineté du débat numérique français, en particulier en matière électorale.

Troisième élément fondamental : la transparence. Viginum n'est pas – et ne sera pas – un service de renseignement. Son cadre juridique ne relève pas du code de la défense et des dispositions relatives aux techniques de renseignement. Il est placé sous le contrôle de la CNIL (Commission nationale de l'informatique et des libertés) – le décret relatif à Viginum est pris après consultation de cette instance – et sous le regard du comité éthique et scientifique, qui publie un rapport sur les activités du service pour en renforcer la transparence ; à cet égard, nous allons tirer tous les enseignements possibles de ce qui s'est passé pendant la campagne des élections municipales – j'y reviendrai.

Enfin, Viginum est un service opérationnel, qui ne fait que des recherches en source ouverte, mais qui s'insère dans un écosystème ministériel plus large. En 2021, outre la gestion de Viginum, le SGDSN a reçu pour mission la coordination interministérielle de l'ensemble des actions de lutte contre les manipulations de l'information, mais il est évident que nous ne pouvons rien faire tous seuls. Parmi nos principaux partenaires, le Quai d'Orsay joue un rôle très important dans la détection des narratifs hostiles, c'est-à-dire ce que nos potentiels adversaires étrangers disent sur nous – parfois de façon très ouverte, car tout n'est pas clandestin : en cela, la désinformation et l'ingérence numérique étrangère sont deux concepts qui ne se recouvrent pas complètement. Nous n'avons pas besoin de Viginum pour détecter les attaques informationnelles hybrides que mènent des acteurs étrangers contre les intérêts français de manière tout à fait ouverte, mais nous avons besoin du Quai d'Orsay pour les détecter très tôt et y répondre. C'est tout l'objet de la stratégie de Jean-Noël Barrot, qui a fait fructifier les graines semées avant son arrivée – une logique qui s'incarne notamment dans le compte X French Response. Le ministère des armées, le ministère de l'intérieur et le ministère de la justice sont aussi des acteurs importants de l'écosystème que le SGDSN est chargé d'animer.

La préservation des équilibres fondamentaux de Viginum au cours de ses presque cinq ans d'existence est l'un des éléments essentiels de son succès opérationnel et politique. C'est en tout cas ce que nos partenaires européens nous disent. C'est le cas en particulier de la

Roumanie, de la Moldavie et de la Géorgie, que vous avez citées, monsieur le président, et qui ont fait appel à l'expertise de Viginum pour faire face à cette menace à laquelle nous sommes tous confrontés.

Mais préservation ne signifie pas immobilité : le cadre juridique de Viginum a connu plusieurs évolutions en tout début d'année. Les deux décrets ont été fondus en un seul, après avis conforme de la CNIL. Quelques paramètres juridiques ont également été modifiés pour préserver l'équilibre au cœur de notre modèle républicain et démocratique tout en s'adaptant à l'évolution de la menace. J'en citerai deux – Marc-Antoine Brillant pourra y revenir plus en détail si vous le souhaitez.

D'une part, nous ne pouvions collecter les données en source ouverte que sur les réseaux sociaux cumulant plus de 5 millions de visiteurs uniques par mois. Or nous constatons que certaines ingérences commencent sur de toutes petites plateformes. Pour assurer la détection la plus précoce possible de la menace, il faut pouvoir collecter les données sur des plateformes et réseaux sociaux beaucoup plus confidentiels et fermés. Nous avons donc obtenu de la CNIL et du Conseil d'État la suppression de ce seuil – le décret est paru au *Journal officiel*.

D'autre part, la menace étant de plus en plus persistante et les acteurs étrangers cherchant à créer des infrastructures d'ingérence vouées à durer, nous avons besoin de capitaliser sur la connaissance technique accumulée, ce qui implique un léger allongement de la durée de conservation des données.

Sachant vos deux commissions très sensibles à ces questions juridiques et à l'équilibre de notre modèle républicain et démocratique, je précise que ces deux modifications juridiques ont été compensées par une extension des prérogatives du comité éthique et scientifique en matière de supervision quotidienne des travaux de Viginum – notamment ceux de collecte – et de compte rendu à l'ensemble des citoyens, puisque le comité est désormais mandaté pour publier un avis sur le rapport d'activité annuel du service.

Voilà pour la dimension opérationnelle de l'outil que nous avons construit, puis modernisé efficacement en préservant les fondamentaux tout en l'adaptant à l'évolution de la menace.

J'en viens à la question du droit. Monsieur le président Fuchs, vous avez souligné le besoin de réponse, la nécessité d'être plus offensif, au-delà du *debunking*. Ces missions sont au cœur du travail du Quai d'Orsay, mais nous avons aussi besoin d'autres outils, notamment juridiques. Or notre droit positif – droit électoral, droit de la presse, droit civil, droit pénal – prévoit de très nombreuses dispositions, notamment à la main du juge pénal, administratif et civil, pour lutter efficacement contre les ingérences numériques étrangères et les manipulations de l'information. D'où l'intérêt de les mobiliser. Ce travail mené avec la Chancellerie et l'ensemble des magistrats dans le cadre de la stratégie nationale a conduit le garde des sceaux à publier, les 21 et 26 janvier, deux circulaires relatives à la mobilisation de l'autorité judiciaire dans la lutte contre les manipulations de l'information. Sans entrer dans le détail, je pense que nous pouvons être beaucoup plus agressifs dans la judiciarisation d'un certain nombre d'attaques contre la souveraineté de notre débat numérique national.

D'autres évolutions seraient importantes. Par exemple, l'article L. 163-2 du code électoral prévoit un référé auprès du juge judiciaire en période électorale. Mais celui-ci est réservé aux élections nationales – cela correspond à ce qu'était l'état de la menace lorsque

vous avez adopté la loi, en décembre 2018 : nous n'avons pas pu le mobiliser dans le cadre des élections municipales. Au regard de l'évolution de la menace et de ce que nous avons constaté lors des municipales, il ne nous semble pas absurde de réfléchir à l'élargissement du champ de l'article, notamment compte tenu du cycle électoral à venir – au-delà de la présidentielle et des législatives, les sénatoriales et les élections en Nouvelle-Calédonie, qui ne sont pas couvertes, sont pourtant des cibles évidentes de manipulation de l'information et d'ingérences numériques étrangères.

M. Michel Herbillon (DR). Toutes les élections, en somme.

M. Nicolas Roche. Exactement.

De même, l'article L. 97 du même code pénalise un certain nombre d'actions informationnelles contre les scrutins, mais les peines encourues sont ridicules. Il ne serait pas absurde de réfléchir à l'augmentation du quantum de peine.

Je ne cite que ces deux mesures, de nature législative et susceptibles de renforcer notre arsenal juridique et judiciaire, même si l'essentiel reste de dynamiser les dispositions existantes.

Depuis l'été dernier, nous nous sommes interrogés sur la nature de la menace pesant sur les élections et la manière de mieux protéger notre processus électoral, à commencer par celui des municipales. Nous sommes partis d'un constat très simple : puisque tous nos adversaires se livrent tous les jours à des ingérences numériques étrangères et des actions de manipulation de l'information, il n'y a aucune raison qu'il y ait une sorte de trêve pendant nos périodes électorales. Au contraire : nous avions anticipé, courant 2025, une probable augmentation de la menace informationnelle pendant le cycle électoral qui s'est ouvert avec les municipales – y compris pour ces dernières, même si elles n'en sont pas, *a priori*, la cible la plus évidente –, pour venir influencer le débat numérique national. Nous avons également regardé ce qui s'était passé chez nos partenaires qui avaient déjà été attaqués – l'Allemagne, le Royaume-Uni, la Roumanie, la Géorgie, la Moldavie. Si tous les scrutins électoraux en Europe sont des cibles, il n'y a aucune raison que nous fassions exception. Ces deux constats nous ont conduits à la nécessité de durcir notre dispositif de protection bien en amont des élections.

Pour faire cela, nous nous sommes inspirés d'un certain nombre de principes adoptés par nos partenaires canadiens.

Tout d'abord, la précocité de l'instauration du dispositif. Celui-ci ne doit pas être un strict dispositif de gestion de crise face à une menace informationnelle déjà matérialisée. Vous le savez, nous avons engagé en décembre et janvier une large concertation avec les présidents des commissions compétentes à l'Assemblée et au Sénat ainsi que l'ensemble des représentants des groupes parlementaires au sujet de ce dispositif, baptisé réseau de coordination et de protection des élections (RCPE). Nous avons donc commencé très tôt ce travail d'information et de pédagogie au sujet de cette organisation collégiale regroupant des administrations de l'État – le SGDSN, Viginum, le ministère de l'intérieur, le SGG (secrétariat général du gouvernement) –, des autorités administratives indépendantes – l'Arcom (Autorité de régulation de la communication audiovisuelle et numérique) et la Commission nationale des comptes de campagne et des financements politiques (CNCCFP) – ainsi que le comité éthique et scientifique.

Deuxième principe : la routine. Pour que le dispositif de protection des élections ne soit pas un strict instrument de gestion de crise, nous avons organisé dès la fin janvier une réunion régulière du RCPE, devenue hebdomadaire début février – les dernières auront lieu prochainement –, afin de vérifier si nous avions détecté une ingérence numérique étrangère – ne rien détecter est en soi une information intéressante – et, dans l'affirmative, de déterminer ce que nous devions en faire.

Troisième principe essentiel : la transparence. Nous avons décidé de publier tous les vendredis sur le site du SGDSN un bulletin d'information indiquant quelles ingérences numériques étrangères avaient été détectées – ou pas – pour chacune des grandes stratégies que nous avons identifiées. Onze bulletins ont déjà été publiés. Nous sommes par ailleurs en train de finaliser, avec les membres du RCPE, le rapport d'ensemble sur les investigations menées lors de la période des élections municipales, qui sera publié dans le courant du mois de mai.

Ce que nous avons constaté est très simple. D'abord, la menace était réelle et elle s'est matérialisée. Selon la façon de compter, qui fait encore l'objet de discussions, quatre ou cinq grandes opérations d'ingérence numérique étrangère ont été détectées par nos soins pendant la campagne.

Deuxième constat : ces opérations ont touché de nombreux partis et candidats différents au niveau national et local. L'une de nos intuitions, à savoir que personne n'est *a priori* à l'abri des manipulations de l'information, s'est vérifiée : nombre de stratégies de nos adversaires consistent non pas à promouvoir un narratif ou un intérêt spécifique à cet adversaire, ou à soutenir tel parti ou tel candidat, mais à semer le chaos, la confusion et la division et à jeter le doute sur la régularité et la légitimité même du processus électoral. La préservation de notre souveraineté à cet égard est essentielle.

Notre troisième constat a trait au dilemme auquel on se trouve toujours confronté quand on conduit des investigations numériques techniques un peu compliquées : faut-il laisser l'opération d'ingérence numérique étrangère se dérouler pour mieux la caractériser et remonter le plus loin possible vers la source, ou la dénoncer publiquement afin de l'entraver, au risque d'empêcher les investigations ? Hors période électorale, nous privilégions la première logique, car elle nous permet d'aller au bout des investigations techniques. En période électorale, le calendrier qu'a imposé la campagne nous a amenés à informer assez tôt les groupes politiques et les candidats – en amont de toute publication, conformément à l'engagement que nous avions pris – et à publier rapidement le résultat de nos investigations.

Nous avons également cherché à entraver les opérations, par un moyen technique simple, c'est-à-dire en signalant les sites web et les comptes inauthentiques – avatars, bots, trolls – auprès des plateformes, qui ont mieux coopéré qu'elles ne le faisaient hors période électorale. L'annonce qu'un bulletin d'information public paraîtrait toutes les semaines a probablement joué dans leur mobilisation ; quoi qu'il en soit, nous avons eu de bons résultats en matière de fermeture de comptes et de sites – ce n'est pas l'État qui le fait, c'est l'AFNIC (Association française pour le nommage internet en coopération), pour les sites web, et les plateformes, pour les comptes, après avoir vérifié que ce que nous leur communiquons est vrai vu leurs conditions générales d'utilisation. Globalement, les infrastructures numériques des quatre à cinq grosses opérations détectées ont été rapidement entravées.

Le rendement global pour nos adversaires n'est pas très bon. La visibilité des opérations d'ingérence numérique que nous avons détectées pendant la campagne municipale

a été plutôt faible. Je précise qu'au regard de la jurisprudence, il ne nous appartient pas de porter un jugement sur l'altération manifeste de la sincérité du scrutin ; cela relève du juge *a posteriori*. Nous ne sommes pas en mesure, ni techniquement, ni juridiquement, de le faire. Notre critère d'appréciation est donc la visibilité. Est-ce visible, est-ce vraiment viral, avec un déploiement sur plusieurs plateformes différentes ? Viginum a créé un indicateur technique, le Vigiscore, qui essaie de caractériser le degré de visibilité et de viralité d'une opération d'ingérence numérique étrangère. Il revient ensuite au juge, s'il est saisi d'un contentieux électoral, de déterminer si l'opération a manifestement altéré la sincérité du scrutin.

Le bilan du dispositif de protection des élections municipales est donc plutôt bon s'agissant de la capacité de détection, de caractérisation, d'entrave, d'information du public, des tests de méthode et des relations avec les candidats et les partis politiques. Néanmoins, je ne crois pas que ce modèle permette de penser pleinement les enjeux du cycle électoral de 2027, pour lequel il faut s'attendre à une menace beaucoup plus massive.

Nous continuons notre réflexion pour déterminer si d'autres dispositions législatives ou réglementaires permettraient de durcir notre modèle de protection de la souveraineté électorale et numérique, au-delà des deux articles de code que j'ai mentionnés. Les fondements de notre réflexion restent ceux que j'ai mentionnés ; nous la finaliserons prochainement et formulerons des propositions qui devraient susciter votre intérêt – nous serons toujours heureux de contribuer à vos travaux.

M. le président Alexandre Portier. Nous en venons aux interventions des orateurs des groupes.

Mme Sylvie Josserand (RN). Dans son rapport de septembre 2025 « Lutter efficacement contre les manipulations de l'information », Viginum indique que « *la prévalence des fausses informations en ligne est surestimée […]. Si les fausses informations circulent à large échelle, leur poids réel dans la consommation générale d'information semble largement surestimé et ne représenterait que 0,16 % du temps total de consommation médiatique en France* ». Ce constat semble démontrer que les effets allégués – notamment par la Commission européenne – de la désinformation sur les dynamiques politiques contemporaines sont largement amplifiés. Le narratif relatif aux ingérences étrangères suggère que les électeurs ne recevraient pas de bonnes informations et que le résultat des scrutins en serait affecté. L'influence infinitésimale soulignée par Viginum prive cette approche de fondement.

Il faut y ajouter la faculté des citoyens et électeurs à distinguer le vrai du faux. Le rapport Viginum souligne que « *la capacité de discernement des individus est sous-estimée* » : « *les études consultées […] semblent indiquer que les individus disposent de bonnes capacités de discernement entre les informations correctes et incorrectes, apparaissant ainsi peu crédules face aux fausses informations* ».

Sous couvert d'une dénomination bienveillante, celle de bouclier européen de la démocratie, la création d'un réseau européen de vérificateurs de faits et d'influenceurs présentés par Mme Von der Leyen comme indépendants mais financés par la Commission mérite d'être interrogée. Loin d'un bouclier démocratique, ne serait-ce pas un bouclier technocratique européen contre la démocratie réelle des peuples qui se met en place ? Sans lien causal établi entre l'exposition des électeurs à des contenus de désinformation et une modification des comportements électoraux, comment apprécier la proportionnalité des dispositifs européens de contrôle imaginés par Bruxelles ?

Fidèle à une approche souverainiste, le groupe Rassemblement national rappelle que Viginum constitue un outil essentiel dans la lutte contre les ingérences numériques et que son efficacité repose sur son indépendance.

Mme Constance Le Grip (EPR). Permettez-moi de saluer la très grande qualité et l'extrême utilité des travaux du SGDSN et de Viginum dans un contexte où la guerre informationnelle est plus forte que jamais et où la protection de nos institutions démocratiques est devenue vitale. La publication récente de la stratégie nationale de lutte contre les manipulations de l'information pour la période 2026-2030 l'atteste tout particulièrement.

Pour avoir auditionné Viginum avant les élections municipales, je constate la pertinence du réseau de coordination et de protection des élections. J'ai conscience que vous ne pouvez pas nous en dire beaucoup plus avant la remise du rapport final, mais je serais heureuse de pouvoir obtenir quelques informations supplémentaires. Quels sont les chaînons manquants dans la protection des élections, au-delà des deux articles que vous avez cités ? Je vous pose la question dans la droite ligne de l'annonce par le chef de l'État d'un projet de loi visant à renforcer notre arsenal législatif et réglementaire contre les ingérences étrangères.

Enfin, comment articulez-vous votre action avec le bouclier européen de la démocratie ? Quelle coopération entretenez-vous avec les institutions européennes et avec vos homologues européens, si vous en avez ?

M. Arnaud Le Gall (LFI-NFP). Une fois les ingérences détectées, leur imputation est une question sensible, car politique : elle est parfois plus facile quand l'entité à leur origine est réputée hostile à la France plutôt qu'alliée ou amie, si tant est que cette notion ait le moindre sens dans le champ des relations internationales. Nous venons d'en voir un cas d'école : lors des élections municipales, le candidat à Paris, Pierre-Yves Bournazel, a été victime de calomnie par une entité russe, Storm-1516. Mais on sait que François Piquemal, Sébastien Delogu et David Guiraud ont aussi été victimes d'opérations d'ingérence reconnues par Viginum. Celles-ci n'ont pas été imputées. Pourtant, selon *Le Canard Enchaîné*, elles émaneraient de sociétés israéliennes. Des faisceaux d'indices tendaient à le confirmer : c'est systématiquement à propos de leur position sur la Palestine qu'ils ont été visés. Quelle suite Viginum entend-elle donner à ces révélations ?

Eu égard à la stratégie de sécurité nationale des États-Unis, qui entendent officiellement favoriser l'extrême droite en Europe et rééduquer l'Europe politiquement, et au fait que les GAMAM (Google, Apple, Meta, Amazon, Microsoft) sont largement au service de la stratégie étatique impériale des États-Unis, comment anticipez-vous les menaces issues de X ou de Facebook pour les élections présidentielles de 2027 ? C'est un pays réputé ami. Je pense qu'il est temps de mettre à jour notre vision des choses.

M. Nicolas Roche. La désinformation n'est pas la même chose que l'ingérence numérique étrangère. L'ingérence numérique étrangère, qui constitue le cœur de notre mission, est une stratégie clandestine d'infiltration de notre débat numérique qui vise à porter atteinte à la souveraineté de ce débat, notamment en période électorale. Ce n'est pas exactement la même chose que la désinformation, les *fake news* ou la mauvaise information, qui relèvent d'une stratégie différente.

Concernant le bouclier européen de la démocratie, les choses sont simples : on peut faire les deux. On peut préserver l'indépendance de Viginum – en tant que SGDSN, je vous garantis que cela fait partie de mes missions –, qui est un acteur opérationnel doté de moyens

souverains d'investigation numérique – c'est un fait qui perdurera. En même temps, nous bénéficions de nos échanges avec les Roumains, les Moldaves, les Allemands ou les Suédois, qui ont le modèle le plus développé et le plus proche du nôtre, concernant les marqueurs techniques, notre connaissance de la menace et de son évolution technologique. Ce n'est pas à moi, fonctionnaire, de porter un jugement politique sur ces choses-là, mais le terme de bouclier démocratique européen ne me choque pas, à condition de trouver le bon équilibre entre la préservation des outils opérationnels, qui resteront essentiellement nationaux, et la coopération européenne dont nous avons besoin car nous sommes tous confrontés à des menaces de même nature. Je vais être direct : notre préoccupation fondamentale, c'est d'éviter la situation roumaine, c'est-à-dire que des acteurs étrangers produisent sur le débat national des effets tels que le juge électoral soit poussé à annuler une élection présidentielle.

Le rapport du RCPE sera finalisé la semaine prochaine. Les leçons que nous pouvons tirer du dispositif tiennent en trois points. Le premier est que les principes sur lesquels il s'est basé ont démontré leur valeur et leur efficacité ; il faut les préserver et les durcir. Le deuxième consiste en quelques modifications des outils juridiques. J'ai cité deux articles ; il y en a peut-être un autre, mais c'est un champ d'intervention assez circonscrit. Le troisième est que nous devons définir le degré d'indépendance du dispositif de protection des élections. Aujourd'hui, c'est moi qui préside le RCPE : je suis un fonctionnaire, je préserve les intérêts de la République, car c'est le mandat qui m'est donné par le code de la défense ; je suis aussi nommé en Conseil des ministres. Veut-on reproduire ce dispositif pour 2027 ou s'inspirer de la CNCCEP, la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle ? La question reste ouverte.

Je n'ai pas l'habitude de la langue de bois, monsieur Le Gall : les menaces viennent de la totalité des endroits que vous avez cités, mais elles ne prennent pas chaque fois la même forme. Les manœuvres de la Russie, de la Chine, de l'Iran, de la Turquie et de l'Azerbaïdjan sont qualifiées d'ingérences numériques étrangères, car elles correspondent aux quatre critères : information manifestement inexacte ou trompeuse, diffusion massive et délibérée par des moyens techniques, atteinte aux intérêts fondamentaux de la nation et origine étrangère. Dans l'ensemble de la sphère MAGA (*Make America Great Again*, « rendre sa grandeur à l'Amérique »), en revanche, il y a assez peu d'ingérences numériques, car ils ne se cachent pas : c'est de la propagande en tant que telle. Quand vous avez 60 millions de *followers* sur un compte, vous n'avez ni besoin, ni envie de vous cacher. Leur action relève davantage de l'influence – ou de l'ingérence, selon l'endroit où vous placez le curseur, mais je dirais plutôt de l'influence ou de la propagande classique. Au milieu de tout cela, il y a les GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Des travaux sont en cours, y compris sur l'utilisation des instruments d'intelligence artificielle à des fins d'amplification des opérations d'ingérence numérique étrangère et de manipulation de l'information. Des procédures judiciaires ont été ouvertes devant le parquet de Paris, section J3, pour atteinte à plusieurs dispositions du code pénal – plusieurs services de l'État, y compris le SGDSN, apportent leur contribution technique à ces enquêtes.

S'agissant de votre première question, les investigations de Viginum se sont poursuivies et vous devriez trouver une réponse dans le rapport final du RCPE. Le temps de l'investigation n'est pas le même dans les deux cas auxquels vous faites référence. Storm-1516 est une infrastructure numérique que nous connaissons extrêmement bien, malheureusement, et nous savons quels actifs numériques sont utilisés par la fédération de Russie pour conduire une opération d'ingérence numérique étrangère. Quand on découvre une nouvelle infrastructure, il faut parfois du temps pour remonter la chaîne et trouver d'où vient l'opération. Pour une opération d'ingérence numérique étrangère dont le cas a été publié dans

un de nos bulletins d'information, nous sommes remontés jusqu'à une société privée dont nous avons considéré que le but était *a priori* lucratif – ce qui n'est pas le cas dans les opérations visant les candidats que vous mentionnez à Toulouse, Marseille et Paris – et l'on ne peut pas toujours savoir, en source ouverte, qui se trouve derrière une telle société. C'est pourquoi ce que nous pouvons dire publiquement à l'instant T diffère dans chacun de ces deux types de cas.

M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères. Concernant la première question qui nous a été posée, sur la prévalence des fausses informations dans le débat, la mémoire me fait défaut et je n'ai pas en tête la publication de septembre…

Mme Sylvie Josserand (RN). Je l'ai citée précisément.

M. Marc-Antoine Brillant. Cela m'intéresse beaucoup, car je ne parle jamais de fausses informations – plutôt d'ingérences numériques étrangères.

Nous observons de la part des acteurs étrangers malveillants une volonté de diluer l'information manipulée dans de l'opinion, de manière à rendre toujours plus difficile la détection de cette information, diffusée par des moyens inauthentiques. C'est la mission de Viginum que de détecter et caractériser ces procédés techniques de diffusion – par faux comptes, faux sites web, vidéos décontextualisées, outils liés à l'IA générative. La sophistication croissante des modes opératoires nous fait dire que c'est un axe d'investissement fort des acteurs étrangers malveillants. Cela pose d'ores et déjà la question de notre capacité à distinguer, dans un débat public en ligne, ce qui est authentique de ce qui est inauthentique.

Pour résumer le schéma de fonctionnement de la gouvernance interministérielle concernant l'imputation des ingérences étrangères, je précise que Viginum a la compétence sur la détection des phénomènes inauthentiques et la caractérisation de l'opération d'ingérence numérique étrangère. Concrètement, selon nos critères, une opération d'ingérence numérique étrangère est un dispositif technique clandestin dissimulé dans notre débat public qui diffuse des choses. C'est rarement du faux : à 80 %, c'est du vrai, instrumentalisé ; seules 20 % des opérations vont créer du faux. C'est un paramètre intéressant de l'évolution de la menace. Une fois l'opération caractérisée, notre travail s'arrête. Mais cela ne suffit pas pour entamer un processus de réponse ou une judiciarisation. La caractérisation, ce n'est ni plus ni moins que la collecte et l'analyse d'indices ; pour aller plus loin, il faut des preuves. Ces preuves relèvent de l'imputation technique, laquelle est faite par d'autres services, notamment les services de renseignement, qui ont un mandat spécifique pour cela.

Storm-1516 est un mode opératoire pro-russe que nous connaissons très bien. Nous avons publié en mai 2025 un rapport technique qui lui attribuait 77 opérations d'ingérence numérique étrangère. Nous en sommes aujourd'hui à plus de 160. En dépit de notre travail de signalement et de l'entrave que permettent les plateformes en réagissant à nos signalements, ce mode opératoire se poursuit. Nous en trouvons régulièrement de nouveaux cas. Or, parce que les ingérences sont de plus en plus sophistiquées, parce qu'une des tendances de la menace est le recours à des prestataires privés et à de l'intermédiation, nous sommes actuellement confrontés à une difficulté de caractérisation. En effet, le savoir-faire de Viginum ne tient pas à des outils techniques, mais à l'expertise de nos agents : c'est une méthodologie qui consiste à faire des pivots techniques, de données en données, jusqu'à remonter à un primo-diffuseur dont on caractérise l'environnement. Or, parfois, celui-ci

utilise des outils de sécurité opérationnelle qui rendent extrêmement difficiles les pivots techniques. Le rattachement prend alors beaucoup de temps. Quand le mode opératoire est connu, on peut y rattacher une opération d'ingérence en six heures ; pour un mode opératoire nouveau, il faut parfois deux mois et demi.

L'audition est suspendue de dix-sept heures trente à dix-sept heures cinquante.

M. Alain David (SOC). Les municipales passées, nous nous engageons dans la campagne encore plus exposée qui nous conduira à la présidentielle. Avec ma collègue Laetitia Saint-Paul, nous avons présenté devant la commission des affaires étrangères, en décembre dernier, un rapport d'information qui constatait notamment la massification de l'usage de l'intelligence artificielle (IA) dans les ingérences étrangères. Nous avons formulé des propositions qui vont dans le sens des changements législatifs qui font désormais l'objet d'un consensus allant jusqu'à la présidence de la République, dont l'interdiction des faux comptes sur les réseaux sociaux au niveau européen.

Je me permets également de citer une autre de nos propositions qui fait écho à un débat d'actualité connexe, car elle concerne les moyens de l'audiovisuel public, notamment de notre audiovisuel extérieur. On sait que France Médias Monde consacre une partie de ses antennes à combattre d'une façon remarquable les *fake new*s et autres ingérences. La guerre informationnelle nous a conduits à interdire les médias de propagande Russia Today et Sputnik après l'invasion de l'Ukraine. Selon vous, d'autres médias pourraient-ils être identifiés comme relais d'une propagande étrangère ?

M. Michel Herbillon (DR). Les ingérences constituent une menace capitale pour la France et pour notre démocratie. Ces ingérences sont diverses tant par leurs auteurs que par leurs méthodes ou leurs objectifs. La Russie se distingue, bien évidemment, mais nous ne devons pas être aveugles ni naïfs face aux autres acteurs qui pourraient intervenir. Les méthodes évoluent dans le sens d'un recours renforcé à l'intelligence artificielle et aux plateformes. Les modes opératoires sont de plus en plus sophistiqués. Les objectifs, enfin, semblent prendre une ampleur nouvelle : la déstabilisation de notre système démocratique et la dislocation de notre corps politique et social. Ces objectifs s'inscrivent dans le temps long, mais notre réponse doit être immédiate.

Deux enjeux sont à mes yeux centraux : l'éducation et la culture d'un côté, la sécurité et la coopération internationale de l'autre ; aussi l'audition conjointe de nos deux commissions est-elle la bienvenue.

En ce qui concerne l'éducation, si la loi de 2024 visant à prévenir les ingérences étrangères en France constitue une avancée majeure, seuls deux de ses trois décrets d'application ont été publiés. La mesure dans l'attente de la publication d'un décret dispose que les établissements éducatifs publics œuvrant avec un partenaire étranger sont tenus de transmettre à la Haute Autorité pour la transparence de la vie publique (HATVP) la liste des versements reçus de puissances étrangères. Pouvez-vous nous indiquer de quelles informations vous disposez à ce sujet et nous renseigner quant à la date de publication de ce décret d'application ?

Pour ce qui touche à la coopération internationale, un groupe de travail du G7 consacré à la cybersécurité a été créé en 2024. L'Agence nationale de sécurité des systèmes d'information, l'ANSSI, a pris la présidence de ce groupe le 1er janvier de cette année. Pouvez-vous nous indiquer les priorités qui ont été fixées pour cette présidence et ce que nous pouvons en attendre ?

M. Jérémie Iordanoff (EcoS). Ce débat mériterait d'avoir lieu dans l'hémicycle tant le sujet des ingérences est fondamental pour notre démocratie attaquée. Le débat public devient insincère à bien des égards et les réseaux sociaux jouent un rôle particulier du fait d'opérateurs étrangers dont les protocoles sont connus.

J'aimerais vous entendre sur la question des algorithmes, dont on peut considérer qu'ils influencent l'opinion par la mise en avant de certains contenus et l'invisibilisation des autres. Ces algorithmes ne sont absolument pas transparents ; ce n'est pas de l'influence. On pourrait donc les qualifier d'ingérence si l'intention de perturber le débat était établie, ce qui n'est pas totalement incongru dans la mesure où on a entendu J.D. Vance et d'autres Américains, comme Elon Musk, assumer des positions anti-européennes et appeler à l'affaiblissement de l'Union européenne. Travaillez-vous sur les algorithmes ? Pensez-vous qu'il y a là des ingérences ?

J'aimerais par ailleurs connaître le niveau de chacune des menaces que vous avez citées : États-Unis, Russie, Chine, Iran, Azerbaïdjan.

Même si vous distinguez l'influence de l'ingérence, le résultat est le même, à savoir un changement de l'opinion publique au moment des élections. Pourquoi n'y a-t-il pas un observatoire des influences ? Il pourrait compléter votre travail sur les ingérences.

Enfin, l'intelligence artificielle figure-t-elle parmi les sujets que vous observez ? Avons-nous vraiment les moyens de regarder ce qui se passe dans ses boîtes noires ?

M. Nicolas Roche. Je laisse à Marc-Antoine Brillant le soin de vous répondre sur ce que nous essayons de faire à Bruxelles pour aller au bout de l'interprétation du DSA (Digital Services Act), notamment concernant l'interdiction des faux comptes et la publicité programmatique. Il vous précisera également l'impact mesuré pour chaque menace.

L'identification de médias étrangers qui seraient des relais de propagande relève plutôt du Quai d'Orsay. Au niveau interministériel, il n'y a pas, à ma connaissance, de sanctions en préparation contre de nouveaux médias. Si tel devait être le cas, l'initiative viendrait soit du ministère de l'intérieur, dans les vrais cas d'ingérence au sens classique du terme, soit du Quai d'Orsay, car cela relève de notre politique étrangère.

Je bois vos paroles, monsieur Herbillon ! Marc-Antoine Brillant vous détaillera nos actions pour la partie éducation et culture et nous reviendrons vers vous par la suite sur l'application de la loi visant à prévenir les ingérences étrangères, qui doit bientôt faire l'objet d'un rapport de notre part, car il y a plusieurs points techniques complexes à traiter.

La cybersécurité mériterait une audition à part entière, surtout en ce moment. Je laisse donc de côté la question de l'ANSSI. Le premier ministre a annoncé son déplacement à l'ANTS (Agence nationale des titres sécurisés) jeudi et je ne doute pas qu'il fera des annonces sur notre politique de cybersécurité. Nous avons publié, lors de notre vaste travail de

rénovation stratégique, une stratégie nationale de cybersécurité qui est le cœur de ce que l'ANSSI fera au sein du G7.

L'IA et les algorithmes sont pour nous des préoccupations majeures qui forment le cœur des travaux du SGDSN et de Viginum. Vous savez que le sommet sur l'IA de l'an dernier a décidé de la création de l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle, l'INESIA, que je copréside avec le directeur général des entreprises et où je suis chargé de la dimension de la sécurité nationale. C'est là que se pose la question de l'impact des intelligences artificielles sur les opérations d'ingérence numérique étrangères et la manipulation de l'information. Et à tous ceux qui pensent que cela s'arrête à la diffusion massive de *deepfakes*, je dis que si nous n'avions que cela à traiter, nous serions dans le meilleur des mondes.

Le vrai sujet se situe plutôt, d'une part, du côté de la massification des opérations d'INE grâce à des outils d'IA et, d'autre part, de la pollution potentielle des modèles d'IA au stade de leur inférence, à des fins de manipulation de l'information. C'est pour cela que nous avons créé un laboratoire d'IA au sein de Viginum. Il a précisément pour fonction, grâce à l'INESIA, de travailler avec les autres acteurs que sont l'INRIA (Institut national de recherche en sciences et technologies du numérique), le PEREN (pôle d'expertise de la régulation numérique) et le LNE (Laboratoire national de métrologie et d'essais).

Même chose s'agissant des algorithmes, qui constituent un sujet majeur. Nous savons tous de manière empirique qu'ils ont un effet puissant, mais cela ne suffit pas. Il nous faut des preuves scientifiques. C'est pourquoi nous avons lancé un programme de recherche, dont le cœur est formé par Viginum en y associant l'écosystème des acteurs précités, pour essayer de démontrer quels sont les biais algorithmiques – évidemment dans une logique de « boîte noire » où nous n'avons pas accès à toutes les API (*application programming interfaces,* interfaces de programmation d'application). Il s'agit tout d'abord de mesurer les biais algorithmiques. Cela va être compliqué, mais nous nous sommes donné les moyens de le faire dans le courant de l'année. Une fois qu'un tel biais a été démontré, il faut ensuite savoir quelle en est l'intention – et c'est encore plus compliqué.

On sait que certains biais algorithmiques sont consubstantiels au modèle économique de monétisation des plateformes. On le constate aussi dans le cas de certaines opérations d'INE qui sont désormais à but lucratif. Le paragraphe à ce sujet que nous avons inséré dans l'un des bulletins d'information du RCPE n'a pas été bien compris. Pour la première fois, nous avons détecté et caractérisé une opération d'ingérence numérique étrangère à des fins lucratives. En créant des faux comptes, on met en place une infrastructure numérique destinée à influencer le débat numérique et à créer de la polarisation, laquelle va permettre la monétisation et l'augmentation des revenus de la société privée à l'origine de la chose.

Qu'il y ait un modèle économique derrière les algorithmes des plateformes est en soi un élément important. À ce stade, nous n'avons pas réussi à caractériser une intention informationnelle de nature politique pour s'ingérer dans nos débats numériques par des biais algorithmiques. Mais cela fait partie des questions que nous nous posons.

M. Marc-Antoine Brillant. De notre point de vue, l'IA est une merveilleuse technologie. Elle pose un problème lorsqu'on la détourne de ses finalités initiales pour des usages malveillants.

Dans le domaine de l'ingérence numérique étrangère, nous avons commencé à documenter de manière de plus en plus fréquente trois usages malveillants depuis mi-2024.

Il s'agit tout d'abord de la création de contenus faux crédibles. On l'observe beaucoup en période électorale ; il ne s'agit pas forcément de *deepfakes*, plutôt de contenus et visuels de nature humoristique qui vont accompagner des narratifs et facilitent la pénétration de ces derniers dans l'audience, quelle qu'elle soit. Faire sourire les gens les incite à l'engagement – à liker, à partager –, ce qui donne de la visibilité aux contenus.

Ensuite, on constate que l'IA permet de créer des faux comptes et de les animer de manière presque humaine. Un faux compte est un bot, un programme informatique qui a une fréquence d'activité. On s'en sert pour automatiser des tâches auparavant dévolues à des humains. Le bot est facile à détecter précisément en raison de sa fréquence d'activité. La plupart des plateformes et d'autres entités font ce travail de détection. L'IA rend la chose plus difficile car, en rendant aléatoire l'activité du faux compte, elle la fait passer pour pratiquement humaine. Cette utilisation de l'IA est croissante. Rappelez-vous l'excellente enquête menée il y a deux ou trois ans par le consortium Forbidden Stories sur la fameuse Team Jorge. Celle-ci avait exercé une influence sur des scrutins, notamment en Afrique. Son activité reposait sur une plateforme d'IA qui générait des faux comptes extrêmement réalistes et était capable d'en piloter l'activité pour produire des mouvements d'opinion en ligne.

Enfin, même si nous ne le voyons pas encore, nous anticipons la capacité de l'IA à massifier la diffusion d'un contenu. Cela permettra concrètement de saturer le débat public en un temps très court, en utilisant plusieurs langues et plusieurs plateformes.

Forts de ce constat, nous avons tout d'abord choisi d'avoir une meilleure capacité technique afin de continuer à suivre l'évolution de l'état de l'art de la menace. D'où la création cette année d'un centre d'excellence en IA, qui s'appuie sur les capacités de Viginum pour développer de nouveaux outils. Ensuite, nous diffusons les instruments performants au plus grand nombre pour outiller la société civile. C'est ce que nous avons fait en mars 2025 lors du sommet sur l'IA, en publiant deux codes informatiques d'outils de détection d'IA.

Je vais élargir la question des algorithmes à celle des plateformes. Notre débat public en ligne est hébergé sur des plateformes qui ne sont pas européennes, mais américaines ou chinoises. Or ce débat est un enjeu de souveraineté.

Premièrement, on constate qu'un certain nombre d'acteurs étrangers malveillants vont détourner des outils et solutions de ces grandes plateformes et réseaux sociaux en provoquant des risques systémiques – cette notion est importante puisqu'elle fait écho au DSA.

Deuxièmement, certaines plateformes semblent préférer le contentieux à la mise en conformité. Elles arguent que les règles sont très compliquées et qu'elles ne sont pas responsables, puisqu'elles ne sont pas des éditeurs mais seulement des plateformes d'hébergement.

Troisièmement, il est utile de rappeler que les réseaux sociaux ne sont pas des services publics d'information. Un réseau social est un service à finalité lucrative qui vise à gagner de l'argent en diffusant du contenu. Ces réseaux ont donc des obligations, puisque nous devons être considérés vis-à-vis d'eux comme des consommateurs.

Nous avons la chance d'avoir un règlement européen pour les services numériques, le DSA, dont le coordinateur national est l'Arcom. Viginum joue auprès de celle-ci le rôle d'autorité d'expertise dans son domaine de compétence, c'est-à-dire la caractérisation d'ingérences numériques étrangères sous l'angle de comportements inauthentiques, *via* des procédés techniques de diffusion dissimulée – des bots, des trolls et de l'IA générative. Nous pouvons être amenés à contribuer aux enquêtes menées par l'Arcom dans le cadre du DSA. Pourquoi ? Tout simplement parce qu'un réseau de 25 000 faux comptes agissant de manière coordonnée est un risque systémique pour une plateforme.

J'en viens à la question de l'impact des différentes menaces. L'activité de détection du service n'a cessé de croître depuis 2021. J'ai la faiblesse de croire que nous détectons de plus en plus de choses parce que nous sommes un peu meilleurs en 2026. Mais je crois surtout que, malheureusement, de plus en plus d'acteurs étrangers veulent influencer notre débat public. Comme nous sommes dans une démocratie, il est libre et ouvert, donc vulnérable aux acteurs étrangers malveillants, qui exploitent ces fameux procédés techniques dissimulés.

En 2024, nous avons détecté autour de 300 opérations d'ingérence numérique étrangère. Nous sommes en train de compiler les données pour 2025, mais cela m'étonnerait que nous soyons en dessous de ce niveau.

La question de l'impact est essentielle. Bien souvent, on confond celui-ci avec la visibilité : parce qu'un contenu a 1 million de vues, on pense qu'il a un impact. C'est faux. Dans notre acception, il y en a un en cas de changement de comportement. Actuellement, il n'existe pas d'étude scientifique sérieuse qui ait permis de trouver un outil mesurant de façon fiable l'impact d'une campagne de manipulation de l'information.

Le cas de l'Azerbaïdjan est de ce point de vue intéressant. Viginum a détecté des activités liées aux événements en Nouvelle-Calédonie à la fin de 2023 et, surtout, au cours de 2024. Les manœuvres de la fameuse pseudo-ONG Baku Initiative Group reposaient principalement sur des faux comptes, mais ces derniers avaient peu de visibilité, avec seulement quelques dizaines de vues. Pourtant, ils ont probablement eu un effet en radicalisant les positions de certains responsables indépendantistes.

C'est toute la difficulté : une opération qui a beaucoup de vues n'a pas forcément beaucoup d'effet, alors qu'une autre très ciblée peut en avoir.

Mme Carole Guillerm (Dem). On a un peu le sentiment d'être dans un roman d'anticipation dystopique comme *Le Meilleur des mondes*, et pourtant c'est déjà une réalité.

Nous savons que les ingérences étrangères dans les processus électoraux ne passent plus uniquement par des cyberattaques classiques ou par des médias identifiés comme relais d'influence. Elles empruntent des canaux beaucoup plus diffus : des plateformes sociales, des messageries cryptées, des influenceurs relais, des campagnes de désinformation très ciblées et, désormais, des outils d'IA capables de produire en quelques heures des contenus falsifiés extrêmement crédibles.

Cette évolution pose évidemment une difficulté majeure. Nos institutions publiques sont souvent organisées pour répondre à des menaces identifiables, revendiquées ou au moins traçables, alors que les nouvelles formes d'ingérence reposent précisément sur l'opacité, la viralité et, parfois, l'impossibilité d'attribuer formellement l'attaque à un État ou à une entité tierce.

À l'approche d'échéances électorales majeures, quels sont les principaux points de vulnérabilité en France, voire en Europe ? Est-ce la capacité de détection ? Notre cadre juridique ? Les moyens humains dont vous disposez ? Le travail interministériel ? La coopération avec les plateformes – qui s'est améliorée mais qui doit encore progresser ? Ou bien s'agit-il de la menace émergente des *deepfakes* et de l'IA générative ?

Quelles sont les lacunes législatives et réglementaires ? Quels points le Parlement devrait-il examiner en priorité ?

Vous avez évoqué des travaux en cours au sein de l'administration. Savez-vous quand ils aboutiront ?

Par-delà la technologie, notre collègue Herbillon a abordé le rôle de l'éducation. Qu'envisagez-vous en matière d'enseignement de l'esprit critique ?

Mme Laetitia Saint-Paul (HOR). Je tiens à vous remercier pour l'accueil réservé à mon corapporteur Alain David et à moi-même dans les services de Viginum. Nous avons présenté en décembre dernier notre rapport d'information sur l'irruption de l'IA dans les ingérences étrangères et la commission des affaires étrangères vient de décider de créer une mission d'actualisation pour 2026, précisément afin de préparer les échéances électorales de 2027. Nous aurons l'occasion de poursuivre nos échanges. Je suis notamment très intéressée par le cas canadien, que vous avez évoqué dans votre propos liminaire.

Dans quelle mesure avez-vous développé le volet prévention, à l'instar de la Psychological Defence Agency suédoise – qui est bien mieux connue par la population que ne l'est Viginum en France ?

Nous avions préconisé dans notre rapport d'interdire les réseaux sociaux aux jeunes de moins de 15 ans. Un important travail législatif est mené en matière de prévention. Mais les jeunes peuvent avoir l'impression qu'on les soumet à des contraintes. Comment faire pour mieux les associer et en faire des acteurs ? On voit bien que c'est la jeunesse qui nous encourage à aller plus loin et à être davantage créatifs dans le domaine de l'écologie, par exemple.

M. Jean-Paul Lecoq (GDR). Je bois les paroles des uns et des autres ; cette audition est très enrichissante.

Le citoyen estime-t-il que son vote est utile et contribue au fonctionnement de la démocratie, ou bien considère-t-il que le résultat de l'élection est biaisé ?

Dans ma ville, on utilise des machines à voter. Les gens ont des doutes avant même d'aller voter, notamment depuis les problèmes rencontrés aux États-Unis. Certains disent même que le résultat est connu d'avance. Pas de pot : lors des dernières élections municipales, le candidat arrivé en seconde position a obtenu 41,17 % des suffrages, soit au centième près le même pourcentage que celui obtenu il y a six ans, alors que le nombre de votants est très différent. Le candidat arrivé premier a obtenu 47,71 %.

Certains m'ont dit : « C'est la Chine ! » Lorsque j'ai demandé pourquoi, on m'a répondu que si l'on additionne le pourcentage obtenu par le candidat arrivé second et celui du vainqueur, on obtient 88,88. Donc, c'est la Chine. *(Rires.)* Et là, je me dis : « Waow ! » Les gens me disent que ça ne sert plus à rien d'être candidat ou d'aller voter.

Je me dis que cela mérite qu'on étudie la question, même si je ne sais pas si votre service est compétent en matière de machines à voter.

On m'avait toujours dit qu'il n'y avait pas de problème parce que celles-ci ne sont pas connectées. Mais un informaticien m'a indiqué qu'elles l'étaient de fait en étant branchées sur le réseau électrique, ce qui permet d'aller chercher des informations dans des appareils électroniques grâce à la technologie des courants porteurs en ligne, utilisée pour les compteurs Linky. Dès lors qu'on est branché au réseau électrique, on est connecté. Cela pose des questions sur la sécurité des machines à voter.

M. le président Alexandre Portier. Sur les enseignements des élections municipales, je pense que vous pouvez apporter des réponses plus substantielles. Nous avons bien compris qu'un travail était en cours sur ce point mais, sans pour autant donner le nom de la commune concernée, pourriez-vous fournir des éléments relatifs au dispositif mis en place dans un cas très précis, afin que les non-initiés que nous sommes parfois comprennent mieux de quoi il retourne ?

Deuxièmement, pourriez-vous préciser quelles sont vos relations avec l'Arcom ? Que pouvez-vous lui demander et que pourriez-vous attendre d'elle à l'avenir si nous étions appelés à revoir ses compétences ou à accroître ses prérogatives ?

M. Nicolas Roche. Je laisserai Marc-Antoine Brillant présenter l'action de Viginum vis-à-vis des jeunes ainsi qu'un très bon exemple d'une opération numérique d'ingérence étrangère réalisée bien en amont des élections municipales au moyen de faux sites d'informations régionales et locales.

Je ferai plusieurs commentaires plus généraux.

Le premier concerne les points de vulnérabilité pour 2027. En vérité, je suis bien plus confiant que je ne l'étais il y a six mois. Nous en sommes globalement là où nous devions en être, grâce au travail collectif qui a été réalisé : la stratégie nationale de lutte contre les manipulations de l'information, les deux circulaires publiées par le garde des sceaux, la mobilisation de l'autorité judiciaire, la mise en place du RCPE et les travaux que nous avons menés auprès des groupes politiques – et la manière dont ils y ont répondu.

Nous avons correctement identifié ce qu'il reste à faire pour durcir notre dispositif. Cependant, je ne m'élève jamais au-dessus de ma condition et je ne m'aventurerai pas à dire à quel moment le premier ministre et le gouvernement décideront de déposer un projet de loi.

Deux sujets sont devant nous.

Le premier est technologique et on en a beaucoup parlé. Il faut conserver un dispositif au sein de l'État capable de rester efficace malgré les révolutions technologiques à venir, notamment dans le domaine de l'IA et de la complexification des modèles algorithmiques des plateformes. Je suis certes plus rassuré sur notre capacité d'action et d'entrave après les élections municipales, mais elle suppose de pouvoir détecter et caractériser. Pour cela, il faut être en mesure de suivre le rythme très rapide de l'évolution des technologies.

J'espère ne pas vous choquer en disant que le deuxième sujet ne relève pas de la dimension nationale mais de la dimension européenne. Il faudra à un moment ou à un autre rendre le DSA plus agressif du point de vue opérationnel. Son article 35 comprend déjà bien

des dispositions efficaces en cas de risque systémique, mais il n'est pas assez appliqué et pas de façon suffisamment volontariste. Je pense notamment à la régulation pendant les périodes électorales, avec l'interdiction des faux comptes, de la publicité programmatique et de la publicité politique. Ce sont des sujets majeurs. Quand nous détectons des faux comptes ou des comptes inauthentiques, nous les signalons aux plateformes et nous dépendons ensuite de la décision de ces dernières.

Je pense en fait que nous sommes beaucoup plus vulnérables que les jeunes aux manipulations de l'information. On fait une grave erreur d'analyse en croyant que cette vulnérabilité est inversement proportionnelle à l'âge. Les très jeunes et ceux qui sont nés avec le numérique sont beaucoup moins susceptibles d'être influencés que ceux qui appartiennent à notre génération. Pour ceux qui se situent entre les deux, cela dépend du niveau d'éducation et de la capacité de compréhension des enjeux technologiques.

M. Lecoq a bien mis le doigt sur le problème. On l'aborde souvent sous l'angle de la désinformation ou des *fake news*. S'il ne s'agissait que de ça, nous serions assez tranquilles. Mais le véritable objectif stratégique de nos adversaires consiste à détruire la possibilité même d'un débat électoral souverain et à créer la confusion et le chaos. Il existe de très nombreuses façons de le faire. Des opérations d'ingérence numérique étrangère ont pour objectif central de délégitimer le processus électoral lui-même, c'est-à-dire la capacité d'une nation à décider souverainement de son avenir. C'est bien plus important que les affaires de propagande ou de promotion de narratifs alternatifs qui nous sont hostiles.

Cela concerne également la cybersécurité. Si l'ANSSI est aussi précautionneuse – pour dire les choses diplomatiquement – en matière de certification des outils de vote électronique, c'est exactement pour les raisons que vous avez évoquées. Le niveau d'exigence pour sécuriser les instruments électroniques de vote est tel que je vois mal comment on pourrait les diffuser de façon massive.

Cela dit, si des citoyens français pensent qu'on arrive à démontrer l'ingérence chinoise en additionnant des pourcentages de voix aux élections, je n'y peux sincèrement rien et cela dépasse ma compétence…

En revanche, il faut aborder avec beaucoup de précautions la certification des modalités de vote électronique dans le contexte de l'évolution de la menace cyber. S'agissant des INE et de la manipulation de l'information, le problème réside moins dans les narratifs hostiles à des fins de propagande que dans l'objectif stratégique consistant à faire croire au citoyen que son vote est inutile.

M. Marc-Antoine Brillant. S'agissant de la question sur les élections municipales, comme l'a dit le secrétaire général, le but des acteurs étrangers malveillants est de casser le lien de confiance. C'est valable pour l'ensemble de la menace informationnelle et c'est particulièrement vrai en période électorale. On vise alors le lien de confiance avec les institutions, le vote et la mécanique de l'élection – et, *in fine*, la confiance des citoyens les uns vis-à-vis des autres.

Nous avons pu observer et entraver une opération intéressante pendant les élections municipales. Menée par Storm-1516, elle consistait à créer des faux sites de médias d'information locale, ce qui est assez facile. Dans le cas observé, ils l'ont été par John Mark Dougan, un citoyen américain réfugié en Russie, et son réseau CopyCop, dont le *business model* repose sur de faux sites alimentés par des contenus générés par IA. Depuis environ

deux ans, il a créé des centaines de faux sites d'informations locales, dont près de 120 en France depuis l'été dernier. Pour être honnête, ils ne sont pas très bien faits, mais ils peuvent tromper l'internaute, car ils comprennent principalement des contenus locaux anodins. Toutefois, ils permettent de glisser des éléments de critique de la politique du gouvernement, voire de celle du maire. Leur objectif est de briser la confiance et de générer de la confusion.

Comme ces sites suspects avaient un nom de domaine en .fr, nous les avons signalés à l'AFNIC. Elle a contacté les gens qui étaient censés les avoir créés pour qu'ils confirment leur identité et, dans 99 % des cas, n'a reçu aucune réponse à ses courriels. Les sites ont donc été suspendus. Voilà un moyen d'entrave pour les sites en .fr qui a très bien fonctionné. Cela prend environ six jours, ce qui est assez rapide. Nous sommes très attachés au partenariat avec l'AFNIC.

S'agissant de la prévention et de l'éducation, nous visons trois types d'audience : les enfants, les adultes et les médias.

Nous travaillons depuis deux ans avec la direction générale de l'enseignement scolaire pour intégrer dans les programmes, de la sixième à la terminale, des éléments d'information et de sensibilisation sur l'ingérence numérique étrangère, uniquement sous le prisme des procédés techniques. On y explique ce qu'est un bot ou un troll et comment fonctionne l'IA générative. Nous avons également réalisé une série de huit podcasts explicatifs avec un opérateur de l'éducation nationale, le CLEMI (Centre de liaison de l'enseignement et des médias d'information).

Par ailleurs, certains éditeurs – de mémoire, Belin et Hatier – nous ont proposé de créer une page ludique de sensibilisation dans les manuels d'histoire, de géographie et d'enseignement moral et civique de quatrième. Nous l'avons validée et nous avons trouvé que c'était une très bonne approche, qui permettait de toucher du doigt des éléments techniques.

Enfin, nous avons mis en place un partenariat avec le magazine d'actualité scientifique *L'Éléphant junior*, destiné aux 9-13 ans. Nous avons réalisé avec eux des doubles pages l'an dernier et cette année.

Notre objectif, en lien avec l'éducation nationale, les éditeurs et les médias, est de rendre les jeunes plus vigilants et de leur enseigner le réflexe de vérifier lorsqu'ils voient des choses qui les étonnent.

En ce qui concerne les adultes, nous avons beaucoup travaillé avec la PQR (presse quotidienne régionale), notamment avec le groupe CMA-CGM, propriétaire de *La Provence*, ainsi qu'avec *Ouest-France*. L'idée est, encore une fois, de donner des éléments de compréhension de la menace, en amont d'élections mais pas seulement.

Nous avons publié des kits ressemblant à des cahiers de vacances, qui sont plutôt destinés aux entreprises afin qu'elles organisent des ateliers de formation en interne. La semaine dernière, nous avons ouvert notre première chaîne YouTube. Elle offre des contenus de sensibilisation, dont une vidéo qui concerne les bots. Plusieurs autres arriveront dans les prochaines semaines, l'idée étant d'avoir un nouveau vecteur de communication pour toucher un public plus large.

Enfin, les médias constituent un relais important pour informer. Nous avons mis en place avec certains médias un programme pour former les journalistes et pour produire des

contenus pédagogiques. Nous avons noué un partenariat avec France Télévisions afin d'accompagner ses journalistes dans le domaine de l'investigation numérique sur les sources ouvertes. Nous faisons de même avec l'école de journalisme de Sciences Po.

Toutes ces actions seront complétées cette année par la création au sein de Viginum de l'académie de la lutte contre les manipulations de l'information.

M. le président Alexandre Portier. Nous en venons aux questions des autres députés.

M. Guillaume Bigot (RN). Monsieur Brillant, la stratégie nationale de lutte contre les manipulations de l'information prévoit d'inscrire Viginum au cœur du DSA européen pour protéger nos processus électoraux.

Il serait utile que vous nous indiquiez comment le fonctionnement de ce bouclier démocratique à l'échelle continentale s'articule avec le respect de notre souveraineté nationale. Pourriez-vous notamment préciser les modalités opérationnelles de coopération avec le Centre européen pour la résilience démocratique ? Quelles sont les garanties prévues pour assurer l'indépendance de l'évaluation française par rapport aux priorités définies par la Commission européenne ?

Quelle est la nature exacte de votre contribution au mécanisme de réaction rapide de la Commission européenne ?

Enfin, quel type d'informations vous sont transmises au titre de l'article 35 du DSA par les grandes plateformes sur leurs risques systémiques ? Disposez-vous d'un accès direct à ces informations ou s'agit-il simplement de rapports déclaratifs transmis par les plateformes ?

M. Paul Vannier (LFI-NFP). Je souhaite vous interroger sur les sondages, dont on sait qu'ils peuvent avoir un impact lors des campagnes électorales, notamment dans l'espace numérique.

Prenons l'exemple du sondage de l'IFOP publié le 18 novembre dernier, dont l'un des volets portait sur les Frères musulmans. Il a été commandé par la revue *Écran de veille*, éditée par Global Watch Analysis, un groupe dont les journaux *Mediapart* et *Le Monde* ont documenté les liens financiers avec les services de renseignement des Émirats arabes unis. Le rédacteur en chef et fondateur de la revue *Écran de veille*, M. Tazaghart, est décrit dans un article du journal *Le Monde* du 3 décembre 2025 comme un « *espion* » et « *l'un des principaux rouages des opérations d'influence orchestrées […] au profit des Émirats* ».

Ce sondage a donné lieu à une grande polémique dans l'espace médiatique français. L'avez-vous identifié comme le fruit d'une opération d'ingérence ? Comment réagiriez-vous dans l'hypothèse où un sondage du même type serait publié lors d'une campagne électorale ?

Mme Virginie Duby-Muller (DR). Les ingérences numériques étrangères dans nos processus électoraux reposent sur des infrastructures de plus en plus sophistiquées – réseaux de faux comptes, amplification algorithmique, *deepfakes* –, souvent hébergées hors du territoire européen, ce qui complique toute action juridique ou technique.

Viginum dispose-t-il de capacités juridiques et techniques suffisantes pour agir en temps réel, ou votre action consiste-t-elle essentiellement à documenter *a posteriori* ? Face à des acteurs étatiques – je pense notamment à l'opération russe Doppelgänger –, quelle est la

doctrine française en matière de réponse ? Se limite-t-elle à exposer publiquement les faits et à recourir à la contre-narration ? Ou bien existe-t-il des capacités de perturbation des infrastructures de manipulation ? Si oui, quelle est l'autorité qui décide de les utiliser ?

Je suggère à mes collègues de lire les ouvrages de Giuliano da Empoli, notamment *Les Ingénieurs du chaos* et *Le Mage du Kremlin*. Je rappelle que vous avez noué un partenariat avec France Télévisions pour organiser la projection à certains députés du film *Le Mage du Kremlin*, réalisé par Olivier Assayas. Je pense que c'est un bon outil de sensibilisation aux enjeux dont nous parlons.

Mme Ayda Hadizadeh (SOC). Comment évaluez-vous le fait qu'une ingérence ait pu fausser une élection ? Vous avez déjà partiellement répondu, mais pouvez-vous aller plus loin ? Si j'ai bien compris, en effet, nous disposons de tous les outils permettant de savoir s'il y a eu ingérence, mais nous serions très faibles pour ce qui est de la sanctionner et de provoquer une nouvelle élection.

Par ailleurs, serait-il possible de « watermarker » des vidéos réalisées au moyen de l'intelligence artificielle – comme on le fait pour les billets de banque, afin que nos concitoyens puissent rapidement savoir si elles sont vraies ou fausses ? De telles technologies pourraient-elles être développées pour que, sur les réseaux sociaux, qui sont le lieu principal où se partagent ces vidéos, un bouton nous permette de scanner les vidéos pour savoir lesquelles sont vraies et lesquelles sont fausses ?

M. Lionel Vuibert (NI). Vous avez souligné que l'essentiel du débat numérique français se déroule sur des plateformes étrangères soumises à des droits étrangers et dont les règles de modération sont fixées par des acteurs privés selon leurs propres intérêts. Tant que cette réalité prévaudra, nous devrons surveiller des opérations d'ingérence sur une infrastructure que nous ne maîtrisons pas, ce qui revient, en quelque sorte, à garder une maison dont nous n'avons pas les clés.

Dans ce cadre structurel, quelles sont concrètement les marges d'action dont vous disposez et pensez-vous que, sans une véritable souveraineté numérique européenne, nos efforts resteront nécessairement limités ?

M. Nicolas Roche. Vous avez raison, monsieur le député : la question des ingérences ne se limite pas aux ingérences numériques étrangères et aux manipulations de l'information ; elle les précède, les accompagne et les suivra probablement. Dans le cas que vous évoquez, la question est fondamentalement du ressort de la DGSI (direction générale de la sécurité intérieure), du ministère de l'intérieur, et relève, au bout du compte, de la judiciarisation. Elle est donc complètement hors du champ de Viginum et même de mes fonctions de coordination interministérielle : elle relève essentiellement des services enquêteurs qui qualifieront l'ingérence. Celle-ci est pénalement répréhensible en tant que telle. Généralement, c'est la DGSI qui est chargée de cette lutte, historiquement dérivée du contre-espionnage : la contre-ingérence est, avec le contre-terrorisme, l'une de ses missions fondamentales dans le périmètre du ministère de l'intérieur et dans sa double fonction de service de renseignement et d'enquête judiciaire au service des magistrats. Les gens susceptibles de répondre à votre question sont donc plutôt ceux qui sont informés de la procédure judiciaire dans ce domaine. Dans notre modèle démocratique, la justice est séparée de l'administration, mais nous essayons de comprendre l'environnement dans lequel se déroulent les ingérences numériques étrangères sur lesquelles nous opérons.

Deuxièmement, nous devons être beaucoup plus confiants dans nos capacités d'action que ne le laissent penser certaines des questions posées, car ces capacités sont assez importantes. Nous pouvons ainsi mettre en œuvre tout un volet d'information et de prévention. En effet – c'est la raison pour laquelle la première partie de la stratégie LMI porte sur la résilience –, la meilleure défense contre les ingérences numériques étrangères et les manipulations de l'information consiste à faire en sorte qu'elles n'aient plus d'efficacité dans le débat numérique national. Il n'est certes pas naturel, pour un service comme le SGDSN et pour des agences chargées de la défense et la sécurité nationale, de dire que leur première mission est la transparence, la publication, l'information et l'éducation ; c'est pourtant bien le cas.

En outre, même s'il n'y a pas d'obligation juridique de suppression des comptes inauthentiques sur les plateformes, je constate que, dans le rapport de force, celles-ci n'aiment pas être clouées au pilori, que l'on dise publiquement qu'elles ne coopèrent pas et qu'elles sont en retard, surtout dans la gestion d'un processus électoral. Lorsqu'on voit des plateformes supprimer aussi vite, et pour la première fois presque volontairement, des comptes inauthentiques, je ne peux pas m'empêcher de penser que c'est aussi parce qu'on leur a dit que l'information allait être publiée et parce qu'on était en période électorale. En matière d'entrave technique, c'est-à-dire de fermeture des infrastructures numériques utilisées par nos adversaires pour mener des opérations d'ingérence numérique étrangère, nous ne sommes absolument pas nus devant la menace.

Troisièmement, nous avons de très nombreux outils judiciaires. Certes, le temps de la justice n'est pas celui de l'élection. Mais cela ne signifie pas que le recours à l'article 40 du code de procédure pénale ou à une procédure en référé – on peut obtenir une décision en référé en quarante-huit heures devant le juge judiciaire, ce qui est rapide – n'ait pas d'impact.

Enfin, la publication et l'exposition ont de l'effet. On en revient toujours à la base : ce que cherchent nos adversaires, c'est faire du clandestin, s'immiscer sans être détectés dans un processus de débat ou d'élection, notamment pour le délégitimer. Le dévoilement, l'exposition publique sont donc un instrument très puissant.

Ces nombreux instruments, il ne dépend que de nous de les utiliser pleinement, comme nous l'avons fait pendant les élections municipales. Cela ne signifie pas que n'ayons pas des choses à faire au titre du DSA – Marc-Antoine Brillant y reviendra –, notamment sur le plan juridique ou pour durcir de notre dispositif.

Les plateformes concernées sont certes étrangères, mais elles sont soumises au droit européen : le DSA, son article 35 existent…

M. Jérémie Iordanoff (EcoS). Il n'est pas appliqué !

M. Nicolas Roche. Il commence à l'être. Cela ne dépend que de nous et de la Commission européenne. Les premières enquêtes ont été engagées, même si je suis plus frustré encore que vous, car nous pensons que c'est trop peu et trop tard, et l'avons d'ailleurs dit publiquement et en privé. Nous pensons en effet qu'il faut être beaucoup plus agressifs dans la mise en œuvre du DSA et nous avons plein d'idées, sur le plan technique, pour que la Commission fasse tout ce que le droit européen lui permet – et Dieu sait qu'il y a encore des marges de manœuvre à utiliser ! Nous allons donc pousser dans cette direction.

Enfin, pour ce qui est de savoir si une élection est faussée, madame la députée, en termes juridiques, la définition de l'altération manifeste de la sincérité du scrutin relève de la compétence du juge *a posteriori*. En effet, dans la jurisprudence électorale française, le juge de l'élection ne mesure pas simplement s'il y a eu une fraude, une ingérence, une ingérence numérique ou quelque facteur qui a pesé sur le déroulement du scrutin, mais il en évalue aussi l'impact sur le déroulement du scrutin à la lumière de l'écart électoral, ce qui ne peut se faire *a priori*. Savoir si une ingérence numérique étrangère altère manifestement la sincérité du scrutin relève donc du juge *a posteriori*.

M. Jean-Paul Lecoq (GDR). Uniquement s'il est saisi.

Mme Ayda Hadizadeh (SOC). Pourrait-on imaginer, en cas d'ingérence, une deuxième élection présidentielle en 2027 ?

M. Nicolas Roche. C'est ce que nous cherchons à prévenir, et c'est la deuxième partie de ma réponse à votre question.

Nous essayons d'être très précis techniquement : en France, cette question relève exclusivement du juge électoral *a posteriori* et je ne vois pas dans quel univers cela ne continuerait pas à être le cas.

En revanche, pour appeler un chat un chat, dans l'ensemble du RCPE que nous avons construit avec vous, nous avons commencé à ramener dans la conduite de la campagne électorale des municipales toute une série de prérogatives de la puissance publique consistant à surveiller le déroulement effectif des opérations électorales et à nous doter des moyens permettant de limiter au maximum l'impact potentiel d'une opération d'ingérence numérique étrangère. Nous n'allons pas toucher au principe fondamental de la jurisprudence électorale qui confie à un juge indépendant le soin de vérifier la sincérité de l'élection et ou son altération manifeste. En revanche, tout ce que nous avons fait dans le RCPE et tout ce à quoi nous sommes en train de réfléchir pour 2027 consiste à nous donner, dans le temps de la campagne électorale et dans le plein respect des principes républicains et démocratiques qui sont au cœur de ce que nous cherchons à protéger, des moyens durcis et plus efficaces d'action pour entraver des opérations d'ingérence numérique étrangère.

M. Jean-Paul Lecoq (GDR). Vous avez dit que votre temps de travail pouvait être plus long que le délai de recours devant le juge électoral.

M. Nicolas Roche. Pour les municipales, nous avons publié tout de suite les éléments concernant les opérations d'ingérence numérique étrangère que nous avons détectées pendant la campagne. Ce que j'ai dit, c'est que nous avions publié avant d'avoir finalisé toutes les investigations. Nous n'avons pas gardé les poches pleines : nous avons tout mis sur la table – dans les bulletins et, bientôt, dans le rapport final du RCPE. En revanche, il n'est pas nécessairement possible de faire tous les pivots techniques que mentionnait Marc-Antoine Brillant pour remonter en source ouverte au plus près de la primo-diffusion, donc du primo-responsable. Mais cela n'empêchera pas l'exercice des délais de recours.

M. Marc-Antoine Brillant. Pour ce qui est du DSA et du bouclier démocratique, lorsqu'est apparue l'idée de créer un centre européen de résilience démocratique dans le cadre du projet de bouclier, la position de la France – sur ce point, nous étions parfaitement en accord avec le ministère de l'Europe et des affaires étrangères – était très claire : il ne fallait pas que cette entité ait une capacité opérationnelle. En effet, ce centre ne doit pas avoir pour

vocation d'assurer une veille sur les débats publics des États membres, car il y va d'enjeux de souveraineté qui relèvent du champ de la sécurité nationale. Le centre n'a donc pas ce mandat – nous avons veillé à ce que ce soit très clair, en lien avec la Commission européenne, le secrétariat général des affaires européennes et, donc, avec le Quai d'Orsay. Sa vocation est plutôt de permettre l'interopérabilité. Viginum est assez unique : il n'existe pas, hormis en Suède, d'entité équivalente. L'idée, avec ce centre européen, est d'amener nos partenaires à prendre en compte notre définition de l'ingérence numérique étrangère afin qu'ils n'adoptent pas de mesures liées aux contenus, mais aux comportements, et qu'il existe à terme des entités homologues assez proches.

Pour ce qui est de l'article 35 du DSA, les plateformes ne nous laissent pas d'accès à leurs API. Pour les deux seules plateformes qui l'ont fait, cet accès se situe au niveau de la régie publicitaire, ce qui nous a permis de voir des choses ; il s'agissait de TikTok et de Google YouTube. Pour les autres, c'est difficile et nous nous heurtons à une lenteur volontaire. Nous faisons autre chose mais, je le répète, nous n'avons pas cet accès.

Quant au *watermarking*, c'est une question technique qui n'est pas simple. La labellisation d'un contenu est effectuée soit par l'outil d'intelligence artificielle – votre prompt génère une vidéo sur laquelle ChatGPT ou une autre IA posera automatiquement un label –, soit par la plateforme même sur laquelle vous diffusez. Concrètement, ce n'est pas fait – au point que certains médias envisagent de labelliser plutôt le contenu authentique : c'est prendre le problème à l'envers. Il s'agit là d'un vrai problème technique, qui fait l'objet de nombreuses discussions.

Avec le PEREN, nous nous sommes appliqués à créer un métadétecteur de *deepfakes* et en avons publié en mars 2025 le code source – imparfait, pour être franc, mais au moins, nous avons essayé. Il s'agit d'un moteur de recherche qui, une fois saisie l'URL (*uniform resource locator*) d'une vidéo que vous voulez voir, sollicite une demi-douzaine d'outils en source ouverte qui procèdent à ces détections et fait remonter un pourcentage de probabilité qu'elle soit authentique ou inauthentique. Cet outil a été récupéré notamment par des entités en Corée du Sud, qui l'ont amélioré. Voilà l'optique dans laquelle nous essayons de nous situer.

M. le président Alexandre Portier. Merci beaucoup.

***

La séance est levée à 18 h 50.

———

Membres présents ou excusés

Présents. - M. Guillaume Bigot, Mme Cendrine Chazé, M. Alain David, Mme Alix Fruchon, M. Bruno Fuchs, Mme Pascale Got, Mme Carole Guillerm, M. Stéphane Hablot, M. Michel Herbillon, Mme Sylvie Josserand, M. Arnaud Le Gall, Mme Constance Le Grip, M. Jean-Paul Lecoq, Mme Charlotte Parmentier-Lecocq, Mme Laetitia Saint-Paul, M. Lionel Vuibert

Excusés. - Mme Nadège Abomangoli, M. Pieyre-Alexandre Anglade, M. Gabriel Attal, M. Bertrand Bouyx, M. Pierre-Yves Cadalen, M. Sébastien Chenu, Mme Christelle D'Intorni, M. Olivier Faure, M. Marc Fesneau, M. Perceval Gaillard, Mme Clémence Guetté, M. Michel Guiniot, Mme Marine Hamelet, Mme Brigitte Klinkert, Mme Amélia Lakrafi, Mme Marine Le Pen, M. Laurent Mazaury, Mme Mathilde Panot, M. Davy Rimane, Mme Sabrina Sebaihi, Mme Michèle Tabarot, Mme Liliana Tanguy, M. Christopher Weissberg, Mme Estelle Youssouffa

Assistaient également à la réunion. - M. Erwan Balanant, Mme Soumya Bourouaha, M. Fabrice Brun, Mme Céline Calvez, Mme Julie Delpech, Mme Virginie Duby-Muller, M. Christian Girard, Mme Ayda Hadizadeh, M. Jérémie Iordanoff, Mme Florence Joubert, Mme Fatiha Keloua Hachi, Mme Graziella Melchior, Mme Frédérique Meunier, M. Alexandre Portier, Mme Anne Sicard, M. Thierry Sother, M. Paul Vannier