ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

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

Mercredi
25 mars 2026
Séance de 15 heures

Compte rendu n° 9

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à quinze heures cinq.

La commission entend, lors de sa table ronde réunissant des associations sur le thème de la protection des données personnelles :

– La Quadrature du net : M. Bastien Le Querrec, juriste ;

– Amnesty International : Mme Katia Roux, chargée de plaidoyer ;

– Ligue des droits de l'homme : Mme Maryse Artiguelong, coresponsable du groupe de travail « Libertés et technologies de l'information et de la communication » et M. Pierrick Clément, avocat.

M. le président Philippe Latombe. Nous réunissons aujourd'hui, sous forme de table ronde, des associations particulièrement investies dans la protection des données personnelles. Notre commission examine les vulnérabilités de l'économie européenne, et française en particulier, liées à l'utilisation de solutions numériques extra-européennes. Selon vous, dans quelle mesure l'économie de la donnée mise en place par les grandes plateformes constitue-t-elle une menace pour la préservation de la confidentialité des utilisateurs ?

Je vous remercie, dans un premier temps, de nous déclarer tout autre intérêt public ou privé de nature à influencer vos déclarations. Auparavant, 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 serment de dire la vérité, toute la vérité, rien que la vérité. Je vais donc vous inviter chacun à lever la main droite et à dire « Je le jure ».

(*M. Bastien Le Querrec, Mme Katia Roux, Mme Maryse Artiguelong et M. Pierrick Clément prêtent serment*.)

M. Bastien Le Querrec, juriste, La Quadrature du net. La Quadrature du Net est une association créée en 2008, initialement centrée sur les sujets de liberté sur internet, d'où notre nom. Au fil des années, nos activités ont évolué, et nous consacrons aujourd'hui une grande partie de notre travail à la surveillance par le numérique de manière générale et aux libertés à l'ère du numérique. La question des libertés sur internet conserve néanmoins une place très importante dans notre activité, et nous travaillons notamment sur la question des *Big Tech*. Il y a quelques années, j'aurais parlé des Gafam, l'acronyme pour Google, Apple, Facebook, Amazon, Microsoft. Aujourd'hui, force est de constater que cet acronyme n'est plus d'actualité puisque d'autres acteurs sont apparus, y compris des non américains. Nous préférons donc désormais le terme de *Big Tech*, qui est repris du terme utilisé dans le milieu anglo-saxon.

Dans mes propos liminaires, je souhaiterais mettre l'accent sur une dimension qui n'est peut-être pas suffisamment prise en considération lorsque l'on évoque la souveraineté, à savoir la souveraineté informationnelle. Si la notion de souveraineté financière ou politique est désormais bien identifiée, et si la question de l'utilisation de services en ligne, de solutions d'hébergement ou de logiciels entretenant un lien direct avec des pays étrangers est régulièrement soulevée, celle de la souveraineté informationnelle me paraît, pour sa part, devoir faire l'objet d'une attention particulière aujourd'hui. Il s'agit de s'interroger, indépendamment de l'origine ou du contrôle des capitaux, sur les effets produits en matière d'information et de

représentation du réel par l'usage des outils numériques. Tel est notamment le cas des réseaux sociaux qui, à travers leurs mécanismes de hiérarchisation algorithmique des contenus, sont susceptibles de déformer la réalité ou de proposer une vision particulière de la société et du monde qui nous entoure. Cette problématique est particulièrement manifeste s'agissant de X, réseau social dont les dérives en matière de manipulation algorithmique sont désormais largement documentées, mais elle concerne, plus largement, l'ensemble des plateformes sociales commerciales.

Au sein de La Quadrature du Net, nous abordons avec une certaine réserve la notion même de souveraineté, dans la mesure où celle-ci ne saurait se réduire à une simple substitution de capitaux américains ou chinois par des capitaux européens ou français. C'est en réalité le modèle sous-jacent qu'il convient de repenser et cette refondation est essentielle, car, en définitive, les dispositifs de surveillance ou les atteintes aux libertés fondamentales produisent les mêmes effets pour les citoyens, qu'ils émanent d'États étrangers, de l'Union européenne ou de la France.

Le lien que j'établis avec la question des réseaux sociaux tient au fait qu'aujourd'hui, lorsqu'il s'agit de les réguler, la tendance consiste à vouloir faire émerger des géants du numérique européens ou français, sans pour autant interroger le modèle sous-jacent. Or parallèlement à la nécessaire réinvention de ce modèle, des évolutions législatives s'imposent également. Dans le questionnaire que vous nous avez adressé, vous avez notamment insisté sur l'omnibus numérique, réforme particulièrement préoccupante portée par la Commission, qui ne vise pas à promouvoir un modèle alternatif, à la différence de ce qu'avait pu représenter le règlement général sur la protection des données (RGPD). Lors de sa présentation, ce dernier avait suscité de vives critiques de la part des milieux économiques, qui y voyaient un texte susceptible d'entraver l'innovation et l'initiative économique en Europe, et force est de constater que ces craintes ne se sont pas confirmées. Néanmoins, le modèle qu'il incarnait tend aujourd'hui à être fragilisé par cet omnibus. À La Quadrature du Net, nous défendons au contraire l'idée d'un renforcement de l'application des règles. Dans son principe, le RGPD constitue un dispositif pertinent et, s'il était effectivement mis en œuvre, il serait de nature à remettre en cause l'hégémonie de certaines grandes entreprises technologiques, américaines mais aussi chinoises. Même si les sanctions prévues, pouvant atteindre 4 % du chiffre d'affaires mondial, sont en elles-mêmes dissuasives, le règlement souffre toutefois d'un défaut d'application. Il y a dix jours, la justice luxembourgeoise a ainsi annulé une sanction prononcée à l'encontre d'Amazon, qui avait été condamnée à plus de 740 millions d'euros pour non-respect du RGPD. Tout en reconnaissant les manquements de l'entreprise, la juridiction a estimé qu'un vice de procédure faisait obstacle à ce que cette amende soit directement infligée.

Nous sommes donc confrontés à une difficulté d'effectivité du RGPD. En 2018, La Quadrature du Net a engagé une série de plaintes sur le fondement du RGPD afin de mettre à l'épreuve le nouveau mécanisme des actions collectives, en réunissant 10 000 personnes. À ce jour, Microsoft a été condamné, et Amazon l'a également été, sous réserve de l'annulation intervenue devant la justice luxembourgeoise. Les autres plaintes demeurent toutefois sans suite, dans la mesure où elles ont été transmises à l'Irlande, où existe un problème structurel affectant l'autorité de protection des données.

Tout cela conduit à considérer que le modèle permettant d'atteindre une véritable souveraineté informationnelle ne saurait reposer sur un affaiblissement des protections juridiques. Il suppose, au contraire, non seulement un renforcement de l'effectivité du droit existant, mais également une remise en question du modèle économique des plateformes. Aujourd'hui, dès lors que l'on aborde la question des réseaux sociaux, on constate que les

algorithmes de mise en avant des contenus posent un problème. Cette réalité n'est pas nouvelle, puisqu'il est solidement établi depuis plusieurs années que les réseaux sociaux ont un intérêt économique à promouvoir des contenus problématiques, qu'il s'agisse de contenus haineux, sans être nécessairement illégaux, de contenus violents ou encore de contenus suscitant de fortes réactions. En effet, plus les internautes réagissent, plus ils demeurent sur la plateforme, continuent d'être exposés à de la publicité ciblée et contribuent ainsi à l'augmentation des revenus de ces acteurs. Ces mécanismes de hiérarchisation algorithmique se trouvent donc au cœur des difficultés posées par les réseaux sociaux commerciaux.

Une alternative existe toutefois, qui mériterait d'être encouragée, notamment par le droit : l'interopérabilité des réseaux sociaux. Elle consiste à mettre fin au monopole exercé par les plateformes commerciales sur leurs communautés, afin d'en restituer le contrôle aux utilisateurs eux-mêmes. En effet, lorsqu'un utilisateur envisage de quitter X ou Meta, il est souvent dissuadé par la perspective de perdre l'accès à ses contacts. On ne saurait reprocher à une étudiante arrivant dans une nouvelle ville de rejoindre un groupe WhatsApp regroupant les étudiants locaux, ni à des militants de se tourner vers Facebook en raison des communautés qui s'y sont constituées. Cet effet de réseau incite les individus à rester sur ces plateformes, en dépit des difficultés bien connues liées à leurs algorithmes, et c'est précisément à ce stade que l'interopérabilité trouve toute sa pertinence. À l'instar des courriels, où il est possible de disposer d'une adresse en @assemblee-nationale.fr et d'échanger avec des utilisateurs de Gmail grâce à des protocoles techniques communs, une telle interopérabilité pourrait être envisagée pour les réseaux sociaux. Or elle demeure aujourd'hui inexistante car les *Big Tech*, en particulier américaines, n'ont aucun intérêt commercial à la mettre en œuvre, dans la mesure où le contrôle de ces communautés constitue la principale source de valeur pour leurs véritables clients, à savoir les annonceurs, et non les utilisateurs.

C'est la raison pour laquelle l'interopérabilité des réseaux sociaux, un temps envisagée dans le cadre du règlement sur les services numériques (Digital Services Act, DSA) et du règlement sur les marchés numériques (Digital Markets Act, DMA) avant d'être écartée de la version finale de ces textes, nous paraît constituer le modèle à réinventer. En offrant aux utilisateurs la possibilité de quitter les réseaux sociaux commerciaux, elle leur permettrait en effet de se tourner vers des alternatives européennes et françaises qui, surtout, proposeraient un modèle renouvelé. Il existe d'ores et déjà un écosystème du Fediverse, au sein duquel s'inscrit notamment le réseau social Mastodon. Les plateformes interopérables actuellement disponibles reposent sur un modèle qui ne privilégie pas la mise en avant algorithmique des contenus dans la mesure où leurs intérêts économiques diffèrent, les utilisateurs évoluant sur des services qui ne recourent pas au ciblage publicitaire et ne promeuvent pas de contenus pour des motifs économiques ou idéologiques.

Ce modèle apparaît, à nos yeux, comme une voie pertinente pour atteindre la souveraineté informationnelle. En face, se conjuguent non seulement des intérêts économiques incitant à promouvoir certains contenus afin d'accroître la rentabilité des plateformes, mais également des enjeux diplomatiques et de représentation du réel. Il n'est pas nécessaire de rappeler que le réseau X fait actuellement l'objet d'une enquête en raison de la mise en avant algorithmique de contenus d'extrême droite. Nous ne sommes donc plus uniquement confrontés à des logiques économiques, mais bien à des stratégies relevant du champ diplomatique et du *soft power*. C'est dans ce contexte que doit s'inventer un nouveau modèle informationnel, fondé notamment sur l'interopérabilité des réseaux sociaux, qui doit être soutenue par le droit, car les plateformes commerciales ne l'adopteront pas de leur plein gré.

Mme Katia Roux, chargée de plaidoyer, Amnesty International. Dans ce propos liminaire et au nom d'Amnesty International France, je poserai d'abord quelques constats assez connus aujourd'hui, avant de dire quelques mots de l'omnibus numérique.

Le premier constat, bien connu, est qu'une poignée d'entreprises de la tech, essentiellement américaines mais pas uniquement, exerce une influence extraordinaire sur les infrastructures, les services et les normes qui façonnent notre vie en ligne. Ce pouvoir, qui reste largement incontrôlé dans divers secteurs du numérique, fait peser de graves risques pour les droits humains, qui constituent le référentiel d'Amnesty International. Je pense notamment au droit à la vie privée, à la liberté d'opinion, au droit à la non-discrimination ou encore à l'accès à l'information, comme cela a déjà été évoqué. Le deuxième constat est que, dans certains pays, ces plateformes numériques ont un monopole tel et sont si ancrées dans la vie quotidienne que la participation à la société dépend en réalité de l'accès à leurs services. Cela leur confère un pouvoir énorme pour à la fois influencer le discours public et contrôler les flux d'information.

Depuis plusieurs années, Amnesty International conduit des travaux de recherche consacrés à l'impact du fonctionnement des grandes plateformes numériques sur les droits humains, en particulier s'agissant des réseaux sociaux. Dès 2018, une première étude a été menée sur Twitter, devenu depuis X, portant notamment sur les attaques en ligne visant les femmes. Par la suite, une analyse a été consacrée au modèle économique de Google et de Facebook, fondé sur la surveillance et la collecte massive de données personnelles. L'organisation a ensuite approfondi ses recherches dans des contextes spécifiques, notamment en lien avec des situations de violence ethnique. À ce titre, des travaux ont été réalisés sur le rôle de Facebook dans les atrocités commises à l'encontre des Rohingyas au Myanmar, ainsi que contre la population tigréenne en Éthiopie. Parallèlement, des analyses ont porté sur X et la diffusion de contenus haineux, qu'il s'agisse de propos dirigés contre la communauté LGBTI en Pologne ou de discours racistes au Royaume-Uni. Plus récemment, Amnesty International s'est intéressée au modèle économique de TikTok et à ses effets sur la santé mentale des jeunes, notamment en France, dans le cadre d'une recherche publiée à la fin de l'année dernière.

L'ensemble de ces recherches met en évidence l'existence d'un modèle économique commun, fondé sur un profilage intrusif, une collecte massive de données personnelles et le recours à la publicité ciblée, qui constitue le moteur du fonctionnement de ces plateformes. Ce schéma se retrouve de manière constante puisque les plateformes cherchent en permanence à accroître la quantité de données collectées afin d'élaborer des profils toujours plus précis, destinés à être commercialisés auprès des annonceurs, tandis qu'elles recourent, dans le même temps, à des algorithmes sophistiqués pour déduire des centres d'intérêt, voire des indicateurs de bien-être, comme c'est le cas de TikTok. L'objectif poursuivi consiste à personnaliser les contenus, à maintenir les utilisateurs en ligne le plus longtemps possible et à remporter cette guerre de l'attention, souvent au détriment des droits humains. Je serai naturellement en mesure de répondre à vos questions concernant la méthodologie et les conclusions de ces enquêtes, en particulier celle consacrée à TikTok, dans le cadre de laquelle nous avons déposé plainte pour manquement aux articles 34 et 35 du DSA, relatifs à la prise en compte des risques systémiques et à l'adoption de mesures destinées à y répondre. Très récemment, la Commission européenne, dans ses conclusions préliminaires, a d'ailleurs confirmé notre analyse en constatant également des manquements de la part de TikTok au regard du DSA, s'agissant notamment de la dimension addictive de sa conception et de ses choix de design.

J'en viens à mon deuxième point, relatif à l'omnibus numérique, qui suscite également de vives inquiétudes au sein d'Amnesty International. Au regard des menaces que font peser ces plateformes sur les droits humains, les réglementations adoptées à l'échelle de l'Union

européenne, bien qu'imparfaites, constituent à ce jour les meilleures garanties dont nous disposons. Même si nous avons, à plusieurs reprises, mis en évidence certaines lacunes du DSA ou du règlement sur l'intelligence artificielle, l'AI Act, en matière de protection des droits fondamentaux, ces textes demeurent néanmoins des instruments essentiels pour la défense des droits humains en ligne. Or ces protections se trouvent aujourd'hui fragilisées par le train de mesures de l'omnibus numérique, dont la mise en œuvre pourrait ouvrir la voie à des pratiques de surveillance illégale et à des formes de profilage discriminatoire, notamment dans les domaines de la protection sociale ou du maintien de l'ordre, tout en privant les individus de leur droit à contrôler leurs données ou à s'opposer à des décisions automatisées. À terme, si le DSA devait être concerné, notamment dans le cadre du Digital Fairness Act, cela pourrait conduire à sa révision et favoriser, de ce fait, la diffusion de contenus problématiques en ligne, ce qui suscite une vive inquiétude. Certaines de ces législations ne sont pas encore pleinement mises en œuvre (je pense en particulier à certaines dispositions de l'AI Act), mais l'Union européenne semble d'ores et déjà orienter l'équilibre en faveur des entreprises plutôt que de la protection des personnes. Une telle évolution reviendrait, à nos yeux, à céder aux intérêts des grandes entreprises technologiques, guidées par des logiques de profit qui s'exercent fréquemment au détriment des droits humains.

Je souhaite enfin évoquer le Digital Fitness Check, qui appelle également notre vigilance. Si son périmètre et sa portée demeurent encore incertains, le fait que le DSA ou le DMA puissent être concernés par cette procédure serait de nature à affaiblir les protections indispensables à la garantie d'un environnement numérique sûr et respectueux des droits.

En conclusion, si l'Union européenne entend véritablement assurer une mise en œuvre cohérente et efficace de ses réglementations numériques, elle doit en renforcer l'ambition et en garantir une application stricte et effective, plutôt que de les affaiblir, comme semble l'indiquer la trajectoire actuelle. Ces cadres juridiques ne sont certes pas exempts d'imperfections, mais ils constituent néanmoins les meilleures protections dont nous disposons aujourd'hui pour la défense des utilisateurs en ligne.

Mme Maryse Artiguelong, Ligue des droits de l'homme. Je ne sais pas si vous en avez eu connaissance mais la Ligue des droits de l'homme avait, en 2018, à la veille d'un Conseil européen du numérique, adressé au président de la République un courrier l'invitant à œuvrer en faveur de l'instauration d'une véritable souveraineté numérique européenne. La réponse qui nous avait été apportée mettait en avant le RGPD, en soutenant que la pénalité pouvant atteindre 4 % du chiffre d'affaires mondial permettrait de résoudre l'ensemble des difficultés.

Sans revenir sur la question des plateformes, je me limiterai à remonter dans le temps jusqu'à 2021. À cette période, à la suite de la crise sanitaire du covid et dans le cadre de la politique vaccinale, nous avons contesté le recours à Doctolib ou, plus précisément la décision du ministre de la santé de lui confier la gestion des prises de rendez-vous. Nous estimions en effet qu'il existait un risque pour les données personnelles, y compris des données sensibles de santé, dans la mesure où Doctolib recourt à Amazon Web Services pour leur hébergement. Bien que l'entreprise ait affirmé que cet hébergement était localisé en Europe, nous faisions valoir que le Privacy Shield n'assurait pas une protection suffisante des données des patients. Bien que le Conseil d'État ne nous ait pas donné raison, Doctolib a depuis considérablement évolué, collectant un volume important de données de santé et proposant de nombreux services, touchant environ 50 millions de Français, les données demeurant hébergées par Amazon Web Services.

En décembre 2021, nous avons saisi le tribunal administratif de Nancy afin de contester l'utilisation de Teams par un centre hospitalier régional, au motif que cet outil, fourni par Microsoft, était susceptible de mettre en péril les données des patients. Bien que le tribunal ne nous ait pas suivis, le centre hospitalier a finalement décidé de renoncer à l'usage de Teams, ce qui constitue, à nos yeux, un motif de satisfaction.

En juin 2023, nous avons également contesté l'hébergement du Health Data Hub par Microsoft. Sans revenir en détail sur ces procédures, qui n'ont pas abouti, j'ai pris connaissance de l'audition de M. Vilbœuf devant votre commission, au cours de laquelle il a reconnu l'existence d'un risque d'accès par une autorité étrangère aux données contenues dans cette plateforme. Nous avons par ailleurs introduit un recours devant le Conseil d'État concernant le projet Darwin, qui devrait toutefois devenir sans objet dans la mesure où il est associé au Health Data Hub, dont la migration vers des entreprises françaises a été actée, ce qui nous apporte un certain apaisement.

Au-delà de ces cas, nous avons régulièrement critiqué les choix opérés par les gouvernements successifs, qu'il s'agisse du recours à Microsoft pour l'éducation nationale, à Palantir pour la DGSI ou encore à Starlink par Air France pour l'accès au wifi à bord, alors même qu'Eutelsat serait en mesure de fournir des services équivalents. Ces orientations nous paraissent à la fois regrettables et porteuses de risques. Nous avons également observé que, lorsque des outils sont développés en France, comme Tchap destiné à remplacer WhatsApp au sein des administrations, il s'avère particulièrement difficile de modifier les usages. De même, un outil tel que Visio, conçu pour se substituer à Zoom, ne semble pas être utilisé à la hauteur de ses capacités.

On peut également évoquer l'usage répandu de messageries telles que Gmail ou Microsoft, très largement utilisées en France. Plus de 5 000 communes françaises disposent ainsi d'adresses électroniques Microsoft, alors même que les risques associés ont déjà été exposés par mes collègues. Le fait que des personnalités telles que le président de la Cour pénale internationale ou un magistrat français de cette juridiction puissent se voir couper l'accès à leur messagerie illustre, me semble-t-il, l'ampleur des enjeux et la nécessité d'agir.

Je souhaiterais enfin m'associer pleinement aux propos tenus par M. David Chavalarias. La Ligue des droits de l'homme partage entièrement ses analyses, notamment s'agissant de X et de l'influence des réseaux sociaux sur la formation des opinions, sujet qui a été rappelé au cours de cette audition.

Pour conclure, compte tenu des actions menées par MM. Trump et Poutine et de leur influence sur l'Union européenne, il me paraît nécessaire de s'appuyer plus fréquemment sur le Conseil de l'Europe car, bien qu'il ne dispose pas de la même portée que l'Union européenne, le recours à la Convention 108, qui a valeur de traité, constituerait un levier utile.

M. Pierrick Clément, avocat, Ligue des droits de l'homme. La Ligue des droits de l'homme aimerait rappeler, puisque nous parlons de vulnérabilité, que cette dernière passe aussi par les atteintes et les influences sur les textes qui protègent nos valeurs. Vous nous avez posé des questions écrites sur l'omnibus, et il est pertinent de revenir sur le contexte dans lequel ce texte a été proposé.

Premièrement, ce projet répond à la crainte d'une surrèglementation européenne susceptible d'entraver l'innovation et la compétitivité. Le rapport sous-jacent ne remet pas en cause la réglementation en tant que telle, mais cible des points précis, parmi lesquels la

surtransposition par les États membres, l'impact jugé disproportionné sur les PME et, surtout, la fréquence des modifications législatives. Sur ce dernier aspect, il faut souligner que la révision d'ensemble de la législation européenne (à travers pas moins de sept omnibus) produit un effet contre-productif et engendre une insécurité juridique préoccupante. À cet égard, la modification de l'AI Act, alors même que celui-ci n'est pas encore pleinement entré en vigueur, apparaît particulièrement révélatrice.

S'agissant de la souveraineté, la proposition d'omnibus procède également, et de manière significative, de pressions extérieures, au premier rang desquelles celles émanant des États-Unis. L'administration Trump considérait en effet que ces textes visaient de manière injustifiée ses entreprises, en raison de leur prétendue portée extraterritoriale et de leur caractère supposément censorial. Or l'application de la réglementation européenne ne saurait être assimilée à une forme de censure, puisqu'elle participe de la lutte contre les discours de haine, les discriminations et les violences numériques. Ainsi, interdire à une intelligence artificielle conversationnelle de tenir des propos négationnistes (comme cela a été le cas de Grok, ce qui a conduit la Ligue des droits de l'homme à déposer plainte) relève non pas de la censure, mais de la protection des droits fondamentaux. Par ailleurs, l'application de cette réglementation ne présente pas de caractère extraterritorial, dans la mesure où elle concerne des entreprises opérant sur le territoire européen ou s'adressant à des citoyens européens.

Ces critiques américaines, que nous estimons infondées, ne se limitent pas aux textes eux-mêmes, mais visent également des personnes. Si la figure de Thierry Breton a été largement évoquée, il convient de rappeler que quatre défenseurs et défenseuses des droits humains sont également concernés : Imran Ahmed, Clare Melford, Anna-Lena von Hodenberg et Josephine Ballon.

Ce contexte d'influence doit également être appréhendé à l'aune du rôle des lobbys américains à Bruxelles. Les 700 organisations représentant le secteur du numérique qui y sont enregistrées ont consacré 113 millions d'euros à leurs activités en 2023, et les projections pour 2025 s'élèvent à 150 millions d'euros. Parmi les principaux contributeurs figurent les entreprises américaines Meta, Microsoft, Amazon, Google qui, à elles seules, ont dépensé plus que les dix premières entreprises des secteurs pharmaceutique, financier et automobile réunies. Meta, à elle seule, a augmenté ses dépenses de plus de 10 millions d'euros pour 2025. Or cette influence se répercute inévitablement sur le contenu des textes. Les ONG LobbyControl et Corporate Europe Observatory ont ainsi recensé un certain nombre de modifications proposées par les lobbys américains et directement reprises dans l'omnibus numérique : la redéfinition de la notion de données personnelles est portée par Microsoft, la limitation du droit d'accès aux données est issue de Google, l'utilisation des données personnelles à des fins d'entraînement des systèmes d'intelligence artificielle est soutenue par Meta, Google et X tandis que l'affaiblissement du principe *human in the loop* résulte d'une action conjointe de plusieurs acteurs.

Ces lobbys entretiennent, en outre, des relations de plus en plus étroites avec certains eurodéputés d'extrême droite, le cordon sanitaire qui prévalait à Bruxelles tendant ainsi à disparaître. Meta a notamment rencontré à plus de 38 reprises des membres des groupes ECR et l'Europe des nations souveraines, au sein desquels siègent notamment les eurodéputés allemands de l'AfD, publiquement soutenus par M. Trump. C'est dans ce contexte que la proposition d'omnibus a émergé. L'offensive dirigée contre les textes européens constitue, en réalité, une remise en cause des valeurs que nous défendons depuis des années, à savoir la protection des données personnelles et la lutte contre les discriminations.

L'Union européenne et la France exercent également une forme de puissance à travers les valeurs qu'elles portent et diffusent à l'échelle internationale. Cet « effet Bruxelles », désormais bien identifié, participe de la puissance normative de l'Union et de la France, dans la mesure où les standards qu'elles élaborent, notamment en matière de protection des libertés fondamentales, influencent les législations de nombreux États tiers. Le RGPD en constitue une illustration particulièrement marquante. À l'inverse, simplifier les textes en les dérégulant revient à affaiblir cette capacité d'influence normative.

La notion même de simplification apparaît, à cet égard, trompeuse et doit être qualifiée pour ce qu'elle est réellement, à savoir une démarche de dérégulation. La simplification, en tant que mécanisme juridique, consiste à faciliter l'application des normes par une clarification des définitions, une harmonisation des procédures ou une réduction des redondances. En revanche, redéfinir des concepts juridiques et étendre les dérogations aux garanties fondamentales ne relève pas de la simplification, mais bien d'un choix de dérégulation, qui traduit une décision politique. Les modifications introduites par l'omnibus numérique traduisent ainsi des arbitrages quant au niveau acceptable d'atteinte aux droits fondamentaux. Elles portent sur des données personnelles particulièrement sensibles, relatives notamment aux opinions politiques, aux convictions religieuses ou à l'orientation sexuelle, et concernent des systèmes d'intelligence artificielle appelés à être déployés dans des domaines aussi essentiels que la justice, la police, l'éducation ou encore le travail.

Je conclurai en indiquant que nous nous tenons à votre disposition pour revenir plus en détail sur les évolutions qui, à nos yeux comme à ceux d'organisations spécialisées telles que le réseau EDRi (European Digital Rights) ou Noyb, ainsi que des autorités administratives indépendantes comme le Comité européen de la protection des données (CEPD), soulèvent des difficultés particulières. Parmi les points les plus préoccupants figurent l'exclusion des données pseudonymisées du champ des données personnelles, l'autorisation du traitement de ces données par des systèmes d'intelligence artificielle, l'élargissement des dérogations en matière de recherche scientifique, la facilitation du recours à des décisions automatisées et, en particulier, la restriction du droit d'accès consacré par le RGPD.

M. le président Philippe Latombe. Ma première question prolonge vos développements sur l'interopérabilité : comment appréciez-vous la création du consortium européen pour une infrastructure numérique (Edic) ainsi que la notion de « communs numériques » ? Ces instruments pourraient-ils constituer l'une des voies de solution et, dans cette perspective, la France, qui a pris part à la création de l'Edic, devrait-elle s'engager plus résolument encore dans cette direction, à l'instar de l'Allemagne tout récemment ?

Ma deuxième question, qui fait suite aux différentes procédures engagées, s'adresse à l'ensemble des intervenants. Constatez-vous, de la part de la Commission européenne, une forme de tropisme dans l'application du DSA et du DMA, se traduisant par un traitement différencié entre les procédures visant des entreprises d'origine chinoise et celles concernant des entreprises américaines ? Certaines procédures dirigées contre des entreprises américaines ont été abandonnées tandis que, comme vous l'avez indiqué, madame Roux, celles que vous avez engagées contre TikTok semblent, pour leur part, progresser, selon des rythmes d'avancement distincts. Maître Clément, s'agissant plus particulièrement de la question du lobbying, avez-vous le sentiment que, sur le terrain de l'applicabilité des textes, celui-ci conduit à une différence de traitement selon la nationalité des entreprises en cause ?

M. Bastien Le Querrec. Je commencerai par répondre à votre question relative à l'interopérabilité. Lorsqu'il est question de souveraineté numérique, l'enjeu premier réside dans la maîtrise de l'ensemble de la chaîne, depuis l'infrastructure et le logiciel jusqu'au cheminement du paquet internet, depuis son émission jusqu'à sa réception par l'administration ou les entreprises. Dès lors que des intermédiaires, qu'ils soient extraterritoriaux ou nationaux, exercent un contrôle sur cette chaîne, une difficulté se pose. C'est précisément dans ce cadre que la question des communs numériques, ainsi que les initiatives visant à reprendre la maîtrise des infrastructures, revêtent une importance particulière. À cet égard, l'Éducation nationale en France mène un travail significatif avec Apps.education, ensemble de logiciels mis à disposition de ses agents. Elle veille non seulement à maîtriser le code source, en privilégiant le recours au logiciel libre, mais également l'infrastructure et les modalités d'hébergement. Ce type d'initiative mérite d'être développé et soutenu afin de devenir la norme, même s'il convient de relever que l'existence d'un contrat avec Microsoft, déjà évoqué, entre en tension avec cet objectif de souveraineté.

Appliquée aux réseaux sociaux, l'interopérabilité repose aujourd'hui sur un modèle encore très marginal. Certaines administrations, aussi bien européennes que françaises, ont fait le choix de recourir à des réseaux sociaux interopérables, sur lesquels elles conservent la maîtrise de leur infrastructure. L'intégration à de tels réseaux permet de créer ce que l'on appelle une instance, c'est-à-dire une entité autonome interconnectée avec d'autres instances pour former un ensemble cohérent. Il n'est pas nécessaire, pour l'État, d'assurer lui-même l'hébergement intégral de ces infrastructures puisqu'il peut également s'appuyer sur des initiatives, souvent portées par des structures associatives ou à but non lucratif, dont l'objectif n'est pas la recherche de profit. Si l'engagement de l'État peut naturellement contribuer au développement de ces infrastructures, il ne constitue pas une condition préalable à leur émergence. À titre d'exemple, en France, la bibliothèque universitaire de Nanterre, La Contemporaine, dispose d'un compte sur Mastodon, reposant sur l'instance du développeur initial du logiciel. Il serait souhaitable que l'État soutienne davantage ce type d'initiatives en mettant à disposition des infrastructures adaptées, même si une telle intervention n'est pas indispensable pour engager une première dynamique.

En l'état, l'interopérabilité des réseaux sociaux repose essentiellement sur la volonté des administrations et des acteurs qui contribuent à la construction de ces infrastructures. Il n'existe pas, à ce jour, de dispositif équivalent à l'Edic permettant d'accompagner ce mouvement vers une souveraineté informationnelle, par exemple en mettant fin à l'usage de réseaux comme X pour des communications diplomatiques. Il est à cet égard regrettable que la France continue d'y recourir, certaines annonces diplomatiques y étant même diffusées en priorité. Le risque n'est pas théorique puisque, dans l'hypothèse où le gouvernement américain demanderait à X de suspendre les comptes du ministère des affaires étrangères français, une telle situation pourrait se produire. À ce stade, aucune initiative structurée ne vise à accompagner les administrations dans une migration vers des solutions alternatives. Sans même évoquer une évolution législative imposant l'interopérabilité des réseaux sociaux, il conviendrait au moins de donner l'exemple. Nous en sommes encore éloignés car, même si des initiatives existent, elles demeurent ponctuelles et gagneraient à être soutenues et amplifiées.

Mme Katia Roux. S'agissant de la question d'un éventuel tropisme ou d'un traitement différencié à l'égard des entreprises américaines ou chinoises, Amnesty International n'a pas spécifiquement documenté cet aspect mais il demeure indéniable, comme en attestent les chiffres évoqués, qu'un lobby particulièrement puissant des entreprises américaines est à l'œuvre.

Il convient, à cet égard, d'apporter quelques précisions sur la plainte que nous avons introduite contre TikTok dans le cadre du DSA, dont le traitement a été particulièrement long. En réalité, la Commission européenne avait ouvert une enquête depuis un certain temps déjà et, constatant que celle-ci n'avançait pas à un rythme que nous jugions satisfaisant, nous avons décidé d'apporter des éléments de preuve complémentaires. Notre organisation avait en effet conduit, dès 2023 au niveau international, une première enquête sur TikTok, peu après l'entrée en vigueur du DSA pour les très grandes plateformes. L'année suivante, nous avons engagé une recherche spécifiquement centrée sur la France, dès lors que ce règlement est censé y produire pleinement ses effets, ce qui nous a conduits à constater que, malgré les mesures annoncées par l'entreprise, des contenus problématiques continuaient d'être promus. C'est dans ce contexte que nous avons saisi, à la fin de l'année dernière, le mécanisme de plainte prévu par le DSA, en rappelant qu'une enquête était en cours depuis près de deux ans et que nous en attendions toujours les conclusions. Il a toutefois fallu attendre le mois de février de cette année pour que soient publiées les premières conclusions préliminaires, qui ne portent que sur une partie de l'enquête, à savoir la question de la conception addictive et qui, comme je l'indiquais, convergent avec les éléments de preuve issus de notre propre enquête.

Nous constatons donc, sans pouvoir apprécier s'il existe une différence de traitement, que les procédures se caractérisent par leur lenteur et leur longueur, ce qui n'est pas sans conséquence pour les personnes concernées, notamment lorsqu'il s'agit de familles ayant été confrontées à des drames, la propagation de la haine en ligne étant susceptible d'avoir des effets particulièrement graves dans la vie réelle. Or, alors même que les preuves sont largement documentées et qu'il ne nous a fallu que quelques semaines pour conduire une enquête technique et produire des éléments probants, bien que cela suppose des moyens, une équipe de la Commission est spécifiquement chargée d'enquêter sur TikTok si bien que, même s'agissant de cette entreprise chinoise, la procédure a pris du temps et demeure, à ce jour, inachevée.

Les nombreuses autres procédures engagées dans le cadre du DSA, notamment à l'encontre d'entreprises américaines, se révèlent elles aussi particulièrement longues. Ainsi, conjugués à cette dynamique de dérégulation (car l'omnibus représente bien, comme cela a été indiqué, une démarche de dérégulation et non de simplification), ces délais procéduraux suscitent une vive inquiétude. Une telle situation n'envoie pas un signal positif de nature à inciter ces entreprises à davantage de responsabilité, mais tend plutôt à leur laisser un champ d'action élargi. Dès lors, sans pouvoir me prononcer sur l'existence d'un éventuel tropisme, je peux néanmoins préciser que la procédure engagée à l'encontre de TikTok n'a été ni automatique ni rapide, en tout cas pas à la hauteur de ce que nous estimions nécessaire.

M. Pierrick Clément. La LDH ne dispose pas non plus d'éléments particuliers permettant d'établir une distinction opérée par la Commission européenne selon le pays d'origine des entreprises, d'autant que la plupart de ces sanctions font l'objet de procédures juridictionnelles et que nous continuons, sur ces questions, à faire confiance à la Cour de justice de l'Union européenne.

On peut toutefois regretter que l'évolution rapide de la situation aux États-Unis, et notamment ce glissement vers une forme d'autoritarisme, ne soit peut-être pas davantage prise en compte par la Cour de justice. La décision rendue en 2025 dans l'arrêt Latombe, relative à l'autorisation de transférer des données vers les États-Unis, en offre une illustration. Le RGPD impose que les pays tiers présentent des garanties « *adéquates* ». Or le Tribunal de l'Union européenne a considéré, dans cette affaire, que les garanties apportées par les États-Unis répondaient à cette exigence. Nous émettons de sérieux doutes sur cette appréciation, au regard de la situation actuelle de l'administration américaine.

En effet, le Data Protection Review Court, censé constituer un organe indépendant et impartial chargé d'assurer la protection des données, voit ses membres nommés par un autre organe, le Privacy and Civil Liberties Oversight Board. Or trois membres démocrates de cet organe ont été poussés à la démission par Donald Trump. Dans ces conditions, on peut s'interroger sur l'existence réelle d'une instance indépendante garantissant la protection des données personnelles aux États-Unis et, par conséquent, sur la possibilité, pour les Européens, de transférer leurs données vers ce pays. L'évolution rapide et préoccupante de la situation américaine devrait donc, à mon sens, être mieux prise en compte par la Commission comme par la Cour de justice.

M. le président Philippe Latombe. Ce n'est pas moi qui vais vous contredire sur la dernière partie de votre propos, et nous en parlerons d'ailleurs devant la Cour de justice de l'Union dans quelques semaines.

Mme Cyrielle Chatelain, rapporteure de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. Ma première question porte sur le modèle économique, que vous avez beaucoup mentionné. Pourriez-vous, avec des exemples précis, clarifier ce mécanisme ? Comment nos données sont-elles à la base de ce modèle et en quoi la modification des algorithmes le sert-elle ?

Il me semble par ailleurs, au vu de vos interventions, que ce modèle économique fonctionne en contradiction avérée avec la réglementation européenne. Les procédures sont longues et les condamnations n'aboutissent pas toujours. Quels sont les points de blocage que vous avez identifiés ? Vous avez mentionné le lobbying, mais il en existe peut-être d'autres. Pourriez-vous revenir en particulier sur la question de l'Irlande et sur le principe du pays d'origine, qui semble être l'un de ces points de blocage ?

Ma dernière question concerne la plateforme X. Au-delà de la fermeture de comptes, avons-nous aujourd'hui la garantie qu'un opérateur de X ne peut pas usurper un compte et, par exemple, publier un tweet à la place de la diplomatie française ou du président de la République ? Lorsqu'un opérateur devient un acteur politique, avons-nous des garanties techniques qu'il ne puisse pas s'exprimer à la place de quelqu'un d'autre ?

M. Bastien Le Querrec. Le modèle économique des plateformes commerciales repose sur la publicité ciblée : leurs véritables clients ne sont pas les internautes, mais les annonceurs, auxquels elles permettent d'insérer des messages publicitaires entre deux contenus. Ce fonctionnement suppose une collecte massive de données personnelles afin d'établir, pour chaque utilisateur, un profil toujours plus précis. Dans ce contexte, le RGPD aurait pu constituer un frein, dans la mesure où ce profilage publicitaire relève d'un traitement de données nécessitant une base légale, comme le consentement. Or ce consentement doit être libre et éclairé ce qui, dès 2018, nous paraissait contestable puisque l'accès même à la plateforme était conditionné à l'acceptation du traitement des données. C'est dans ces conditions que La Quadrature du Net avait déposé cinq plaintes en 2018, aujourd'hui presque toutes restées lettres mortes en Irlande.

Ce modèle, qui repose donc sur une violation du RGPD à des fins publicitaires, repose également sur la mise en avant algorithmique de contenus afin de maintenir les utilisateurs sur la plateforme : plus les réactions sont nombreuses, qu'il s'agisse de contester une vidéo ou d'exprimer un soutien à un tweet haineux, plus le temps passé augmente, et avec lui l'exposition à la publicité. Il s'agit, en somme, d'une version contemporaine du « *temps de cerveau disponible* » de TF1.

Il existe toutefois un autre modèle, celui des plateformes non marchandes, que La Quadrature du Net promeut. Dès lors que l'on s'écarte d'une logique de recherche maximale de profit, d'autres formes d'équilibre économique peuvent émerger, fondées notamment sur le don ou l'abonnement, avec des effets concrets sur la conception même des plateformes. Mastodon en constitue une illustration. Ce logiciel de micro-blogging, conçu en réaction aux contenus de haine visant la communauté LGBTQIA+ sur Twitter, intègre en effet des mécanismes limitant la viralité et ne recourt pas à des algorithmes de recommandation, le choix ayant été fait, dès l'origine, de ne pas chercher à retenir les utilisateurs le plus longtemps possible.

S'agissant des obstacles à l'application du RGPD, ils sont nombreux. Le premier tient à sa non-application par certains États membres, en particulier l'Irlande, puisque l'autorité irlandaise de protection des données, la DPC, apparaît notoirement incapable de faire face aux *Big Tech*. Pour des raisons fiscales, ces entreprises s'y sont implantées et relèvent ainsi d'une autorité marquée par des phénomènes de pantouflage et un turnover élevé, qui entravent le traitement des plaintes et les investigations. Les plaintes déposées en 2018, portant sur la notion juridique de consentement, ne nécessitaient pourtant pas d'enquête approfondie, puisqu'il suffisait de constater l'absence de caractère libre et éclairé du consentement dans les conditions générales d'utilisation. Malgré cela, en 2026, Apple n'a toujours pas été sanctionnée.

L'autre point problématique, qui n'est pas du tout envisagé dans l'omnibus, est que les plaignants ne sont pas parties à la procédure. Le cas d'Amazon est symptomatique. Nous avons déposé une plainte en 2018 et avons appris par la presse qu'un projet de sanction était en cours, puis que la sanction finale avait été prononcée par l'autorité luxembourgeoise, la CNPD. La Commission nationale de l'informatique et des libertés (Cnil), notre interlocutrice, nous l'a confirmé après la presse. À ce jour, nous n'avons toujours pas pu obtenir une copie de cette sanction, sous des prétextes variés comme le caractère non définitif de la décision ou le risque d'atteinte à l'image d'Amazon. Même la demande effectuée auprès de la Commission d'accès aux documents administratifs (Cada) a été refusée. Nous n'avons donc pas accès à la sanction prononcée à la suite de notre propre plainte.

Enfin, sur votre question concernant l'usurpation de comptes sur X, c'est effectivement un risque qui existe dès lors que l'on ne maîtrise pas l'infrastructure. Là encore, l'interopérabilité est une réponse. Mediapart, par exemple, a sa propre instance Mastodon pour ses journalistes. Comme le média maîtrise cette infrastructure, il peut garantir que les comptes de ses journalistes sont authentiques, ce qui est une protection contre l'usurpation dont ils sont régulièrement victimes. Cette garantie est impossible quand une entreprise tierce détient l'infrastructure et, même si nous n'avons pas vu ce cas d'usurpation se produire, le risque est bien réel.

Mme Katia Roux. Je souhaite simplement ajouter que la publicité ciblée repose sur une extraction continue de données, dans la mesure où l'ensemble de nos activités en ligne fait l'objet d'un suivi. La réussite majeure de ces entreprises tient précisément au fait d'avoir imposé ce modèle comme l'unique horizon possible, freinant ainsi l'émergence d'alternatives plus respectueuses des droits humains. J'insiste également sur la puissance des algorithmes de recommandation, à l'image du fil « Pour toi » de TikTok, désormais reproduit par l'ensemble des plateformes, ainsi que sur les difficultés persistantes à obtenir de la transparence quant à leur fonctionnement.

S'agissant des points de blocage, j'ajoute le déni quasi total de responsabilité des entreprises, en particulier en ce qui concerne la prise en compte des risques systémiques induits par leurs choix de conception. Deux exemples permettent de l'illustrer. Le premier concerne

nos travaux sur la responsabilité de Facebook, devenu ensuite Meta, dans les atrocités commises au Myanmar à l'encontre de la population rohingya en 2017 : nous avions mis en cause la plateforme et un groupe de réfugiés sollicitait une réparation sous la forme d'un projet éducatif d'un montant d'un million de dollars. Facebook a opposé une fin de non-recevoir, en indiquant que l'entreprise ne menait pas d'activités philanthropiques, ce qui éclaire sa conception de ses obligations au regard du droit international.

Le second exemple, plus récent, est lié à notre enquête sur TikTok en France, qui s'appuyait sur le DSA et sur les mesures d'atténuation des risques mises en avant par l'entreprise, comme les outils de « bien-être » ou les dispositifs de déconnexion de la plateforme, dont la pertinence apparaît discutable. Lorsque nous avons rendu publiques nos conclusions, TikTok a contesté notre méthodologie, soutenant que le recours à des comptes-tests ne reflétait pas la réalité des usages. Or, si nous avions mobilisé des utilisateurs réels, les résultats auraient sans doute été encore plus accablants. Nous nous sommes ainsi heurtés à un déni complet de responsabilité, qui constitue un obstacle majeur. C'est la raison pour laquelle nous nous appuyons fortement sur les articles 34 et 35 du DSA relatifs aux risques systémiques mais, à ce stade, les rapports d'évaluation que les entreprises sont tenues de publier se révèlent très décevants.

Mme Maryse Artiguelong. Les contenus addictifs ne se limitent pas à la haine ou à la publicité ciblée. En Asie, sur TikTok, existent ainsi des dispositifs de vente flash permettant d'acquérir des produits de grande valeur à des prix très bas, à condition d'être connecté au moment opportun, ce qui incite les utilisateurs à demeurer en permanence sur ces réseaux.

Quant à la question du guichet unique, elle ne concerne pas uniquement l'Irlande. La LDH accompagne notamment une action de groupe engagée par des chauffeurs Uber qui ne parviennent pas à obtenir leurs données de travail, ce qui les empêche de vérifier leurs revenus et, le cas échéant, de faire reconnaître un statut de salarié. La Cnil a transmis la plainte à l'autorité néerlandaise, compétente en raison de l'implantation du siège européen d'Uber aux Pays-Bas. Une condamnation a été prononcée, mais Uber a interjeté appel, de sorte que la procédure se prolonge depuis plus de quatre ans.

M. Éric Bothorel (EPR). Notre régulation numérique européenne repose aujourd'hui sur une logique simple qui consiste à publier puis à modérer a posteriori, les plateformes ayant toujours résisté à leur assimilation à un statut d'éditeur. Après avoir longtemps considéré que cette approche pouvait suffire, je m'interroge sur le fait que nous n'en atteignions pas aujourd'hui les limites, notamment face à l'émergence des intelligences artificielles génératives. L'exemple de Grok sur X en offre une illustration éclairante : au début de cette année, les utilisateurs ont généré environ 3 millions d'images sexualisées en onze jours, dont plus de 23 000 impliquaient des mineurs, dans le cadre de cette tendance dite du « *mets-la-moi en bikini* » ou du déshabillage par intelligence artificielle, alors même que ces contenus n'existaient pas auparavant. Dans ce contexte, on demande à l'entreprise de modérer ces productions tandis que, dans le même temps, des équipes de développeurs conçoivent des outils capables de générer des contenus totalement illicites.

La question se pose dès lors de savoir si cette modération réactive, qui poursuit un flux quasi infini, n'atteint pas ses limites et s'il ne serait pas temps de faire évoluer la doctrine en encadrant les capacités de certains outils d'intelligence artificielle générative avant qu'ils ne produisent des millions de contenus illicites. Je suis curieux de connaître vos recommandations pour permettre une protection plus efficace des consommateurs et des usagers.

M. Émeric Salmon (RN). Ma question relève moins d'une incompréhension que d'un besoin de précision sur ce que vous entendez par « *ciblage* ». Lorsque je réfléchis à cette notion, je comprends que vous mettez en cause le ciblage personnalisé des internautes par la récupération de leurs données. Cependant, ce modèle économique, que vous semblez juger très néfaste, est utilisé dans de nombreux autres domaines. Par exemple, lorsque l'on regarde « Télématin » sur France 2, la publicité n'est pas la même que celle diffusée l'après-midi sur la même chaîne pendant Roland-Garros, car le public n'est pas identique. France Télévisions, qui n'est pourtant pas un acteur des Gafam, sait que les téléspectateurs du matin et de l'après-midi sont différents et adapte donc sa publicité en conséquence.

Je suis d'ailleurs persuadé que si, un jour, un opérateur internet parvenait à diffuser des flux en direct différenciés pour chaque foyer, les chaînes, y compris France Télévisions, cibleraient rapidement ces téléspectateurs pour leur adresser la publicité la plus pertinente. J'ai donc du mal à concevoir la distinction entre ce qui constituerait un bon et un mauvais ciblage.

Mme Laure Miller (EPR). Je souhaitais vous interroger sur la comparaison que l'on peut établir entre l'industrie de la tech et l'industrie du tabac. Cette dernière a opéré pendant des décennies une stratégie consistant à investir et orienter la recherche afin de faire subsister le doute dans l'opinion publique sur la réalité scientifique du caractère nocif du tabac. Ne retrouve-t-on pas aujourd'hui une stratégie similaire avec le numérique, et plus précisément les réseaux sociaux ? On observe en effet que des scientifiques, dont les laboratoires sont en partie financés par ces entreprises, occupent une place massive dans les médias pour instiller cette même théorie du doute. N'y a-t-il pas là une question de transparence et la nécessité de démonter cette stratégie, qui n'est pas véritablement exposée dans le débat public à l'heure actuelle ?

M. Pierrick Clément. Je répondrai brièvement à la question du profilage, afin de déterminer s'il en existe de bons et de mauvais, notamment lorsqu'il porte sur des données personnelles. Si je m'en tenais à ma conviction personnelle, tous les profilages seraient mauvais. Toutefois, la position que nous devons adopter consiste à reconnaître que l'intégration de données personnelles dans un système algorithmique ne se limite pas à créer des risques de discrimination, mais en amplifie considérablement les effets potentiels, ce qui est désormais parfaitement établi.

C'est pourquoi le cadre européen impose de raisonner selon une approche en trois temps, dite du triple test, selon laquelle tout traitement de données doit être à la fois légitime, nécessaire et équilibré, seule méthode permettant d'en apprécier la validité. À défaut, le risque de discriminations devient concret, comme l'illustrent plusieurs exemples. Lorsque Meta a déployé des algorithmes pour diffuser des offres d'emploi sur ses réseaux sociaux, il est apparu rapidement que ces offres étaient présentées différemment selon le genre. L'algorithme avait en effet observé une présence plus importante de femmes dans le secteur de la petite enfance, ce qui a conduit à orienter 93 % des offres correspondantes vers des femmes. À l'inverse, 74 % des offres de pilotes de ligne étaient diffusées vers des hommes. Ces biais discriminatoires apparaissent dès lors que des données personnelles sont mobilisées dans des outils algorithmiques.

Mme Maryse Artiguelong. Sur la comparaison avec l'industrie du tabac, je pense malheureusement qu'elle n'est pas la seule à recourir à de telles pratiques, que l'on retrouve également, par exemple, dans l'industrie du sucre. S'il est difficile d'établir une équivalence stricte avec les *Big Tech*, on peut néanmoins faire un parallèle avec les pratiques de lobbying évoquées précédemment qui, bien que sans doute moins dissimulées, produisent des effets largement comparables. Il ne s'agit donc pas, à mon sens, d'un phénomène propre au seul secteur du numérique.

Mme Katia Roux. La question de la place des plateformes en tant qu'éditeurs s'est effectivement posée, dans la mesure où le développement des algorithmes de recommandation conduit à une forme d'éditorialisation accrue des contenus, qui les éloigne de leur statut de simples hébergeurs. Les plateformes ont longtemps soutenu qu'elles ne faisaient qu'héberger des contenus promus par les utilisateurs eux-mêmes, ce qui renvoie la question de la modération à la nécessité de retirer les contenus illicites tout en préservant l'équilibre avec la liberté d'expression. Toutefois, de notre point de vue, la modération ne constitue qu'un correctif insuffisant puisque, dès lors que les algorithmes recommandent des contenus problématiques, une modération, de surcroît de plus en plus fondée sur l'intelligence artificielle, ne saurait résoudre ces difficultés. C'est pourquoi nous portons davantage notre attention sur les choix de conception et sur les systèmes algorithmiques eux-mêmes.

S'agissant de l'IA générative, un travail est en cours et il ne m'est pas encore possible de formuler des recommandations, même s'il apparaît d'ores et déjà nécessaire d'anticiper et d'encadrer en amont ce type de contenus. Les plateformes ne peuvent se retrancher derrière un simple statut d'hébergeur et il convient d'appréhender les systèmes algorithmiques et, le cas échéant, les systèmes d'IA générative comme des sources potentielles d'atteintes aux droits humains.

Sur la question des données personnelles et du ciblage publicitaire, je rejoins pleinement les analyses précédentes. À cet égard, l'analogie avec la télévision trouve rapidement ses limites puisque, sur les réseaux sociaux, l'utilisateur peut être entraîné dans ce que l'on désigne comme des *rabbit holes*, c'est-à-dire des enchaînements de contenus potentiellement toxiques qui tendent à l'enfermer. Il ne s'agit pas du même phénomène que la publicité télévisée, qui ne repose pas sur des inférences relatives à nos centres d'intérêt, à notre niveau de bien-être ou à nos comportements potentiels. Le ciblage publicitaire sur les réseaux sociaux se révèle ainsi bien plus intrusif et peut, dans certains cas, mobiliser des données sensibles, ce qui soulève des interrogations juridiques au regard du test en trois étapes précédemment évoqué.

S'agissant enfin de la comparaison avec l'industrie du tabac, la question du financement de la recherche n'a pas été spécifiquement étudiée, mais elle constitue très probablement un enjeu majeur. Elle renvoie à la dichotomie fréquemment avancée entre innovation et régulation : d'un côté, un discours promeut l'investissement dans des systèmes d'intelligence artificielle présentés comme intrinsèquement vertueux et porteurs de progrès social, en considérant la régulation comme un frein et, de l'autre, des moyens considérables, notamment financiers, sont sans doute mobilisés, sans que nous ayons, à ce stade, mené d'investigations sur ce point. Dans ce contexte, la régulation demeure aujourd'hui l'un des principaux leviers pour exiger des plateformes davantage de transparence et le respect de leurs obligations. Il importe ainsi de tirer les enseignements de ce qui a pu être observé dans d'autres secteurs, le numérique n'étant nullement exempt de telles problématiques, qui doivent dès lors être approfondies.

M. Bastien Le Querrec. Pour répondre à votre question, monsieur Bothorel, le DSA a amorcé une remise en cause de ce modèle tout en maintenant le principe de la modération *a posteriori* ainsi que la distinction entre hébergeur et éditeur, mais il a introduit, pour les très grandes plateformes, de nombreuses obligations destinées notamment à lutter contre les risques systémiques, assorties de sanctions. Ce dispositif s'apparente toutefois à une réponse partielle à un problème plus large et, comme vous l'indiquez, il semble aujourd'hui atteindre ses limites. Si tel est le cas, c'est, selon La Quadrature du Net, en raison de l'hypercentralisation des contenus au sein de plateformes de très grande taille, qui concentrent un pouvoir considérable,

disproportionné et dangereux pour nos démocraties, et du fait que leur modèle économique demeure largement remis en cause. C'est pourquoi nous revenons à la nécessité de faire émerger un nouveau modèle, qui passe notamment par l'interopérabilité des réseaux sociaux. Une telle évolution affecterait profondément ces grandes plateformes, en remettant en cause leur modèle économique et en les contraignant à s'adapter. Elle explique donc également l'intensité des efforts qu'elles déploient en matière de lobbying et de financement d'initiatives, afin de préserver leur monopole sur leurs communautés. À l'inverse, l'ouverture de ces communautés permettrait l'émergence d'alternatives décentralisées, constituées de plateformes plus petites, dotées de règles de modération différentes, plus légitimes, plus proches des utilisateurs et mieux contrôlées par eux. C'est ce modèle qu'il convient d'inventer et de promouvoir afin de dépasser l'opposition binaire entre, d'une part, l'acceptation des limites de la modération et, d'autre part, l'instauration d'une modération *a priori* aux conséquences potentiellement graves pour la liberté d'expression. Cet équilibre passe, selon nous, par une obligation d'interopérabilité.

Pour répondre à votre question, madame Miller, je partage votre constat selon lequel l'industrie de la tech finance de nombreuses initiatives. Il y a quelques années, La Quadrature du Net a ainsi travaillé sur un lobby dénommé TechAgainstTerrorism et sur son initiative européenne, qui soutient de nombreuses recherches relatives à la régulation des contenus terroristes en ligne. Cette organisation promeut notamment des systèmes destinés à détecter et bloquer a priori ces contenus, qui se retrouvent aujourd'hui intégrés dans le règlement européen sur les contenus terroristes (TCO). Notre enquête a débuté à la suite de la découverte d'un rapport universitaire qui semblait être le seul à défendre ce type de dispositif, alors même que de nombreuses ONG, dont la nôtre, y étaient fortement opposées. En poursuivant cette analyse, nous avons mis en évidence que TechAgainstTerrorism et sa branche européenne, financées par différents intermédiaires, dépendaient pour moitié de l'industrie technologique américaine et pour moitié de certaines polices, notamment canadiennes, révélant ainsi des liens entre l'industrie, certaines autorités publiques et le milieu de la recherche. Sans préjuger de la qualité du rapport de recherche en question, il apparaît donc que ces investissements existent.

Un autre exemple concerne l'interopérabilité des réseaux sociaux. Nous avions été auditionnés par le Conseil national du numérique, alors en charge d'un travail sur ce sujet, et cette audition s'était particulièrement mal déroulée. Le Conseil a ensuite rendu, en juillet 2020, un rapport très critique à l'égard de cette idée, présenté aux côtés de Facebook et de Snapchat. Sans affirmer qu'il y aurait eu une intervention directe de ces entreprises, cette proximité, au moins dans ses apparences, est documentée et doit nous interroger.

Ces entreprises poursuivent donc à la fois des intérêts économiques et idéologiques. Un rapport préoccupant de la Chambre des représentants des États-Unis, publié début février, met en cause la position de la Commission européenne dans l'application du DSA, en l'accusant de censure. Il insiste également sur le rôle d'« ONG censeures » (*censorious NGOs*) qui collaboreraient avec la Commission pour contraindre les entreprises américaines. Il existe ainsi un travail idéologique mené par ces entreprises, notamment en lien avec l'administration Trump. Une association, AccessNow, est explicitement citée, tandis que d'autres sont évoquées de manière implicite, à l'image de Bits of Freedom, organisation néerlandaise qui a publiquement dénoncé ce rapport en estimant être visée. Dans ce contexte, il existe un risque que les États-Unis prennent, à l'avenir, pour cible d'autres acteurs français ou européens dans une démarche idéologique visant à contester la réglementation européenne. Il s'agit là d'un point d'alerte que je souhaitais souligner.

Mme Cyrielle Chatelain, rapporteure. Dans cette série de questions, je souhaite poursuivre sur le modèle économique et revenir sur la proposition omnibus.

Premièrement, concernant la modération, vous avez bien expliqué la contradiction entre des algorithmes qui valorisent des contenus néfastes et la volonté de les modérer. Or certaines plateformes hébergent des contenus qui sont illégaux au regard du droit français, comme des images pédopornographiques. Avons-nous aujourd'hui la capacité, ou serait-il souhaitable, dans le cadre d'un rapport de force entre les États et ces plateformes, de pouvoir bloquer, ne serait-ce que temporairement, la diffusion d'une plateforme au titre de ces publications illégales ? Est-ce une mesure possible et souhaitable, au-delà des contraintes financières ?

Deuxièmement, sur le modèle économique, nous avons beaucoup parlé des Gafam et de leur cercle fermé, mais une enquête parue dans *Le Monde* a mis en lumière l'autre acteur que sont les courtiers en données. Des applications comme Leboncoin ou Vinted captent des données, notamment de géolocalisation, et les vendent à ces courtiers. Avez-vous étudié le modèle économique de ces derniers et l'impact de ces pratiques ? Relèvent-elles du RGPD ?

Ma troisième question porte sur l'omnibus, qui, dans le discours officiel, est présenté comme une démarche de simplification. Nous avons compris que tel n'était pas votre point de vue, et je le partage. Plus précisément, ces mesures sont-elles de nature à simplifier la vie des petites et moyennes entreprises, ou bien s'agit-il d'un texte qui ne modifie pas leur situation mais qui allège, en réalité, les contraintes pesant sur les grands groupes ? Par ailleurs, s'agissant de questions telles que la définition des données personnelles ou l'utilisation de données pour l'entraînement des systèmes d'intelligence artificielle, quelles sont les craintes concrètes que font naître ces nouvelles mesures ? Enfin, si le droit européen venait à être affaibli, disposons-nous d'outils juridiques français qui pourraient être utilisés ou renforcés ?

M. Bastien Le Querrec. Sur la modération, La Quadrature du Net se demande régulièrement s'il faudrait aller jusqu'à demander ouvertement le blocage de X, puisque le DSA le permet en dernier recours à l'égard d'une plateforme qui manquerait de manière systémique à ses obligations. Notre position a longtemps consisté à considérer qu'une telle censure devait demeurer exceptionnelle, judiciaire et proportionnée, et toute la question est donc de savoir si le blocage de X serait proportionné au regard de l'ensemble de ses utilisateurs. Nous n'avons pas de réponse définitive à ce stade, mais certains éléments plaident dans un sens comme dans l'autre. Il faut également relever que, selon une étude de Médiamétrie, X a perdu de nombreux internautes. La portée de sa nuisance pourrait donc diminuer sans qu'il soit nécessaire de recourir à une mesure de blocage, simplement si les pouvoirs publics, les élus et les collectivités cessaient de communiquer exclusivement sur cette plateforme. Cela amorcerait une évolution qui pourrait nous éviter d'en arriver à une telle extrémité.

S'agissant des courtiers en données, je vous renvoie à la note d'EDRi sur la proposition omnibus, qui relevait que l'une des modifications envisagées consistait à réviser la directive e-Privacy, qui encadre notamment les cookies. En transférant la question du dépôt de cookies de la directive e-Privacy vers le RGPD, la Commission ouvrirait des possibilités beaucoup plus larges de recourir au pistage, notamment par le biais de l'intérêt légitime. On passerait ainsi du consentement comme base légale à d'autres fondements dans lesquels l'internaute n'aurait plus son mot à dire. EDRi estimait que cette évolution contribuerait à légaliser les pratiques de ces courtiers en données, les *data brokers*, alors même qu'elles ne sont pas tenues pour légales aujourd'hui. Ces acteurs prospèrent en exploitant les failles du RGPD et le défaut d'application effective de ce règlement par les autorités. En France, Criteo, qui relève de cette catégorie d'entreprises, a été sanctionnée par la Cnil à hauteur de 50 millions d'euros, si mon souvenir est exact. Cette sanction n'est toutefois intervenue qu'après des années d'activité et, pour une entreprise condamnée, combien d'autres poursuivent encore leurs pratiques en toute impunité ?

Sur le projet d'omnibus, je partage votre analyse qui consiste à affirmer qu'il allège les contraintes pesant sur les grandes entreprises sans apporter de réelle simplification. La note d'EDRi est, sur ce point, très complète. Pour aller plus loin, la modification de la notion de données personnelles constitue une réaction directe à l'arrêt IAB Europe rendu par la Cour de justice en 2024. La Cour a considéré que des données devaient être regardées comme personnelles alors même qu'elles ne permettent pas, à elles seules, d'identifier une personne, dès lors que des tiers sont en mesure de le faire en les utilisant. Cet arrêt a constitué une défaite pour l'industrie de la publicité ciblée et la proposition de la Commission en est la réponse directe.

S'agissant enfin des outils français, ils sont malheureusement peu nombreux, mais il ne faut pas pour autant déduire que la France devrait agir seule. Elle a, au contraire, un rôle à jouer au sein de l'Union européenne pour défendre un modèle aujourd'hui en voie de détricotage. Cela suppose d'en réaffirmer le soutien et de le renforcer, notamment à l'occasion d'une éventuelle révision du DSA ou du DMA sur la question de l'interopérabilité, plutôt que de considérer que le combat est perdu d'avance. Le Conseil d'État a, certes, dégagé dans l'arrêt French Data Network un mécanisme lui permettant de réinterpréter le droit de l'Union lorsque les exigences constitutionnelles diffèrent, mais ce mécanisme soulève des difficultés au regard de l'état de droit et de l'intégration européenne. Il ne me paraît pas souhaitable d'aller jusqu'à cette extrémité, qui poserait la question de l'intégration de la France dans une Union européenne demeurant, par ailleurs, très protectrice des libertés fondamentales.

Mme Katia Roux. S'agissant tout d'abord de la suspension, le DSA en prévoit la possibilité en dernier recours. La question est donc de savoir jusqu'à quel point cette mesure peut être différée et quelle mise en conformité peut être obtenue dans l'intervalle. C'est la raison pour laquelle Amnesty International insiste sur la nécessité de transformations systémiques du modèle économique, dans la mesure où une suspension, en l'absence de tels changements, ne garantirait pas nécessairement une amélioration de la sûreté des plateformes. Elle demeure néanmoins une option, au même titre que l'amende.

Sur la question des courtiers en données, nous n'avons pas conduit de travaux spécifiques.

S'agissant en revanche de la proposition d'omnibus et de l'objectif de simplification, notre analyse converge malheureusement vers l'idée qu'elle vise avant tout à desserrer les contraintes pesant sur les grands groupes. À titre d'exemple, si l'on examine les obligations prévues par l'AI Act pour les systèmes à haut risque, notamment dans les domaines de l'emploi ou de l'éducation, le texte initial présentait déjà des insuffisances, en ce qu'il comportait une faille permettant aux fournisseurs de s'auto-évaluer et de déterminer eux-mêmes si leur système relevait de cette catégorie, ce qui les conduisait à s'exonérer de leurs obligations de transparence. Or les propositions de la Commission repousseraient à la fin de l'année 2027 des obligations qui devaient initialement entrer en vigueur en août de cette année, en y ajoutant une clause d'antériorité, de sorte que les fournisseurs ayant déjà déployé leurs systèmes n'y seraient pas soumis. Ce délai supplémentaire leur offrirait ainsi la possibilité de développer rapidement leurs solutions afin d'échapper à ces nouvelles obligations.

De la même manière, le recours à des données personnelles, y compris sensibles, pour entraîner les systèmes d'intelligence artificielle suscite des inquiétudes quant aux risques de discrimination, d'autant que ces systèmes sont susceptibles de reproduire et d'amplifier des biais existants. Ces évolutions, loin de constituer une véritable simplification, apparaissent surtout comme un allègement des contraintes au bénéfice des grands groupes, avec un

accroissement corrélatif des risques en matière de droits humains. Enfin, la nouvelle définition des données personnelles, qui introduit une forme de subjectivité, ne va pas non plus dans le bon sens, alors même que le cadre existant, bien qu'imparfait, constituait l'outil le plus protecteur dont nous disposions.

Mme Maryse Artiguelong. S'agissant des outils juridiques hors Union européenne, des dispositifs techniques, tels que les systèmes de hachage utilisés dans la lutte contre le terrorisme, peuvent également être mobilisés pour d'autres types de contenus illicites, notamment les contenus pornographiques.

Au risque de paraître insistant, je souhaite revenir sur la Convention 108 du Conseil de l'Europe, qui revêt une valeur conventionnelle et dont le champ d'application ne se limite pas aux seuls États membres du Conseil de l'Europe. Son adhésion est subordonnée à la démonstration, par les États candidats, du respect des principes de protection des données personnelles. Par ailleurs, le Conseil de l'Europe a également élaboré une convention relative à l'intelligence artificielle.

M. Pierrick Clément. S'agissant de la simplification et de la proposition d'omnibus, celle-ci a été élaborée dans un délai très court et avec une volonté prioritaire de dérégulation, ce qui a conduit la Commission à se heurter à une contrainte : la nécessité de respecter la jurisprudence de la Cour de justice de l'Union européenne. Elle a ainsi supprimé un certain nombre de règles, tout en leur associant des critères destinés à en assurer la conformité, ce qui, dans certains cas, aboutit paradoxalement à une complexification notable. L'exemple du droit à l'information, prévu à l'article 13 du RGPD, l'illustre clairement. La Commission a envisagé d'exclure cette obligation lorsque l'entité qui collecte les données n'en fait pas un usage intensif et qu'il existe des motifs raisonnables de considérer que la personne concernée est déjà informée, ce qui devrait viser la grande majorité des PME et des TPE. Toutefois, afin de se conformer à la jurisprudence, cette dispense d'information est désormais subordonnée au respect de sept critères distincts que chaque entreprise doit vérifier. Là où il suffisait auparavant de délivrer une information, il convient désormais de satisfaire à sept conditions pour s'assurer de pouvoir s'en exonérer. Je ne suis pas certain que l'on puisse, dans ces conditions, parler de simplification.

Mme Cyrielle Chatelain, rapporteure. Serait-il, selon vous, pertinent de renforcer les compétences du CEPD ? Ensuite, vous avez beaucoup mentionné un nouveau modèle décentralisé. Pourriez-vous dire quelques mots sur ce que pourrait être un modèle qui ne soit pas lié à la concentration des grands groupes ? Vous avez parlé d'infrastructures, et nous avons un grand débat en France sur l'installation des centres de données. Cela répond-il à cet enjeu de maîtrise ? Enfin, sur l'interopérabilité, comment envisagez-vous de surmonter la complexité du changement d'habitude pour les utilisateurs et la peur de manquer quelque chose, le fameux « FOMO » (*fear of missing out*) ?

M. Bastien Le Querrec. Je commencerai par les compétences du CEPD, qu'il convient à mon sens, en effet, de renforcer. La collégialité ainsi que la diversité des points de vue nationaux et culturels constituent, en effet, des atouts, comme l'illustre le fait que le CEPD se soit opposé à plusieurs reprises à l'autorité irlandaise de protection des données.

S'agissant du nouveau modèle que La Quadrature du Net appelle de ses vœux, il vise à redonner aux internautes la maîtrise de leurs usages en mettant fin au monopole des grandes plateformes sur leurs communautés. L'interopérabilité consiste concrètement à permettre, par exemple, aux utilisateurs de Facebook de communiquer avec des utilisateurs d'autres

plateformes, ce qui ne signifie pas que tous quitteraient Facebook, mais que ceux qui le souhaitent pourraient le faire sans perdre le lien avec leurs contacts. Un tel cadre favoriserait l'émergence d'alternatives, notamment de start-up françaises et européennes, qui pourraient, au sein de cet écosystème de réseaux sociaux interopérables appelé Fediverse, proposer des algorithmes plus vertueux, voire s'en passer, ou encore développer des modèles économiques fondés sur l'abonnement et assortis d'engagements en matière de confidentialité. Les internautes disposeraient ainsi d'un véritable choix et pourraient participer à la définition des règles de modération. Aujourd'hui, dans le milieu des réseaux sociaux interopérables, les règles varient selon les instances : l'instance mamot.fr, gérée par La Quadrature du Net, applique par exemple des règles qui peuvent être moins strictes que celles d'instances se présentant comme des *safe spaces* pour la communauté LGBTQIA+. Il n'existe pas de modèle unique de modération et les règles sont déterminées par les internautes eux-mêmes au sein de chaque instance et, en cas d'insatisfaction, il leur est possible d'en changer sans perdre leurs contenus.

Dans cette perspective, la question du FOMO se trouve résolue puisqu'il serait possible, demain, de quitter Instagram pour rejoindre Mastodon tout en continuant à suivre des comptes restés sur Instagram. La différence tiendrait à l'absence d'un algorithme imposant des contenus jugés néfastes et, inversement, ceux qui s'en satisfont pourraient choisir de rester sur Instagram tout en accédant à des contenus issus d'autres plateformes.

Mme Maryse Artiguelong. Simplement, je suis d'accord sur le maintien et le renforcement du CEPD, qui me paraît très important.

Mme Katia Roux. Je rejoins mes collègues s'agissant du CEPD : son maintien et son renforcement vont dans le bon sens. S'agissant des nouveaux modèles, nos travaux se sont principalement concentrés sur les entreprises de réseaux sociaux, ce qui conduit notamment à envisager l'interdiction de la publicité ciblée. Le DSA a d'ailleurs déjà proscrit la publicité fondée sur les données personnelles des mineurs, ce qui démontre que ce mode de fonctionnement est possible et pourrait être étendu à l'ensemble des utilisateurs. D'autres approches existent également, telles que des mécanismes d'adhésion volontaire (*opt-in*) au partage des données, en lieu et place de dispositifs de retrait (*opt-out*). La publicité ciblée se situe au cœur du problème et il est dès lors possible d'envisager des formes alternatives, notamment contextuelles, qui ne reposent pas sur une exploitation prédatrice des données.

M. Pierrick Clément. Madame la rapporteure, en tant qu'écologiste, vous êtes particulièrement sensible aux enjeux liés au développement des centres de données. Or à l'horizon 2027, la consommation annuelle d'eau imputable à l'essor de l'intelligence artificielle devrait dépasser celle du Danemark. Nous atteignons ainsi un niveau particulièrement préoccupant, notamment en raison des coûts énergétiques associés à ces infrastructures. Si la poursuite d'une stratégie de souveraineté technologique peut être envisagée, il n'est pas certain qu'elle puisse l'être à n'importe quel prix.

M. le président Philippe Latombe. Ce sera le mot de la fin. Je vous remercie de vous être rendus disponibles.

La séance s'achève à seize heures cinquante-cinq.

———

Membres présents ou excusés

Présents. – M. Éric Bothorel, Mme Cyrielle Chatelain, M. Philippe Latombe, Mme Laure Miller, M. Stéphane Rambaud, M. Alexandre Sabatou, M. Emeric Salmon, M. Hervé Saulignac

Excusé. – M. Philippe Gosselin