N° 444

SÉNAT

SESSION ORDINAIRE DE 2024-2025

Enregistré à la Présidence du Sénat le 13 mars 2025

RAPPORT

FAIT

au nom de la commission des affaires européennes (1) sur la proposition de résolution européenne en application de l'article 73 quinquies *du Règlement, visant à l'***application stricte** *du* **cadre réglementaire numérique** *de l'***Union européenne** *et appelant au* **renforcement** *des* **conditions** *d'une* **réelle souveraineté numérique européenne***,*

Par Mmes Catherine MORIN-DESAILLY et Florence BLATRIX CONTAT,

Sénatrices

(1) Cette commission est composée de : M. Jean-François Rapin*, président ;* MM. Alain Cadec, Cyril Pellevat, André Reichardt, Mme Gisèle Jourda, MM. Didier Marie, Claude Kern, Mme Catherine Morin-Desailly, M. Georges Patient, Mme Cathy Apourceau-Poly, M. Louis Vogel, Mme Mathilde Ollivier, M. Ahmed Laouedj*, vice-présidents ;* Mme Marta de Cidrac, M. Daniel Gremillet, Mmes Florence Blatrix Contat, Amel Gacquerre*, secrétaires ;* MM. Pascal Allizard, Jean-Michel Arnaud, François Bonneau, Mmes Valérie Boyer, Sophie Briante Guillemont, M. Pierre Cuypers, Mmes Karine Daniel, Brigitte Devésa, MM. Jacques Fernique, Christophe-André Frassa, Mmes Pascale Gruny, Nadège Havet, MM. Olivier Henno, Bernard Jomier, Mme Christine Lavarde, MM. Dominique de Legge, Ronan Le Gleut, Mme Audrey Linkenheld, MM. Vincent Louault, Louis-Jean de Nicolaÿ, Teva Rohfritsch, Mmes Elsa Schalck, Silvana Silvani, M. Michaël Weber.

Voir les numéros :

Sénat : **351** et **445** (2024-2025)

SOMMAIRE

Pages

AVANT-PROPOS

« Le numérique défie l'Europe : il ébranle la puissance économique traditionnelle en captant la valeur et en bouleversant secteurs et marchés ; il se joue de l'impôt et exploite la concurrence fiscale entre États membres de l'Union européenne ; il défie les règles de droit et fait advenir dans le cyberespace des règles concurrentes aux règles étatiques. »

En 2013, dans son rapport d'information intitulé « l'Union européenne, colonie du monde numérique ? »[1], la commission des affaires européennes du Sénat se faisait « lanceuse d'alerte » sur les risques induits par la numérisation des sociétés et des économies européennes, qui, selon elle, menaçaient la capacité des États membres de l'Union européenne à maîtriser leurs données, posaient la question de « la survie de l'esprit européen » et même de « l'avenir de la civilisation européenne ».

Douze ans plus tard, où en est l'Europe numérique ?

Après une prise de conscience tardive, l'Union européenne et les États membres ont fini par bâtir un cadre normatif inédit à l'échelle mondiale pour réguler le numérique et garantir un usage des données personnelles, incarné par le Règlement général sur la protection des données (RGPD). Puis, le règlement européen sur les marchés numériques (ou *Digital Market Act* – DMA), entré en vigueur le 6 mars 2024, vise à maintenir une concurrence équitable entre plateformes en ligne sur le marché intérieur, alors que le règlement européen sur les services numériques (ou *Digital Services Act* – DSA), entré en vigueur le 17 février 2024, tend à inciter les plateformes en ligne à suivre des règles de transparence, de modération des contenus et de lutte contre les contenus illicites.

Cependant, force est de constater que les très grandes plateformes en ligne et les principaux moteurs de recherche, devenus oligopolistiques, dominant le marché européen sont américains et chinois.

Ainsi, la moitié de la population mondiale se connecte au moins une fois par mois à un service de Meta (Facebook, Instagram, WhatsApp, etc.). Le système d'exploitation Windows de Microsoft représente 68,5 % des systèmes installés et son moteur de recherche, Bing, est le deuxième le plus utilisé dans le monde après Google, qui malgré une baisse récente au niveau mondial, est utilisé par les citoyens européens dans 90 % des cas. Le chiffre d'affaires 2023 d'Amazon, leader mondial du commerce en ligne, était de 574,8 milliards de dollars et Apple représente 22 % des ventes de téléphonie mobile dans l'Union européenne.

---

[1] *Rapport d'information n° 443 (2012-2013) sur l'Union européenne, « colonie du monde numérique ? », de Mme Catherine Morin-Desailly au nom de la commission des affaires européennes du Sénat, en date du 20 mars 2013.*

La dépendance des États membres et des citoyens de l'Union européenne à l'égard de leurs services est donc réelle. Elle ne fait que s'accroître au fur et à mesure de la numérisation des économies européennes et du développement des usages.

Or, le modèle économique de ces acteurs, qui recherche le profit absolu, est fondé sur le « clic rémunérateur » et la captation de l'attention des utilisateurs.

Les conséquences de ce modèle toxique sont désormais bien documentées : diffusion de fausses nouvelles, mise en exergue de contenus violents sexualisés et extrêmes, réelle porosité aux actions de manipulation de l'information et aux ingérences étrangères, et atteinte à la santé mentale des jeunes…

Sur ce point, lors de son audition au Sénat, la « lanceuse d'alerte » Frances Haugen, ancienne ingénieure chez Facebook, expliquait que les plateformes en ligne privilégient toujours l'optimisation du profit à la sécurité des enfants.

Pour certains observateurs, comme Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique, « les données sont un outil de contrôle des populations ». Ce faisant, leur influence sur les systèmes démocratiques est grandissante.

À titre d'exemple, le réseau social TikTok, dont les pratiques et les liens avec le régime chinois avaient été dénoncés par la commission d'enquête du Sénat[1], a ainsi été accusé de faciliter les tentatives d'ingérences étrangères dans le premier tour de l'élection présidentielle en Roumanie par la Cour constitutionnelle du pays, qui a, en conséquence, annulé ce scrutin.

En outre, ces acteurs en viennent parfois à contester publiquement les règles européennes. Ainsi, Mark Zuckerberg, fondateur de Meta, a critiqué avec virulence la réglementation européenne sur le numérique, le 7 janvier 2025, annonçant vouloir « travailler avec le Président Trump pour faire pression sur les gouvernements du monde entier qui s'en prennent aux entreprises américaines » et estimant que « l'Europe a un nombre croissant de lois qui institutionnalisent la censure et empêchent l'innovation ». Cela prend une tournure plus grave depuis que ces critiques ont été reprises par le nouveau président des États-Unis.

Voilà pourquoi la proposition de résolution européenne précitée appelle à une application stricte et rapide des pouvoirs d'enquête et de sanction prévus par le DSA, afin que les très grandes plateformes en ligne qui souhaitent bénéficier du marché intérieur en respectent les règles. Dans le même temps, l'Union européenne n'a pas manifesté de réelle volonté politique

[1] *Rapport n° 831 (2022-2023) de la commission d'enquête sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence*

pour construire son autonomie stratégique numérique, en assumant une politique industrielle globale et ambitieuse. Cette menace, qui a été maintes fois dénoncée par le Sénat, est parfaitement identifiée par le « rapport sur l'avenir de la compétitivité européenne », remis par Mario Draghi à la Commission européenne le 9 septembre 2024, qui appelle l'Union européenne à un « choc de compétitivité ». Dans ce dernier, l'ancien Président de la Banque centrale européenne (BCE) et Président du Conseil des ministres italien constate que l'essor de la technologie numérique est la principale cause de l'écart de compétitivité entre l'Union européenne et les États-Unis. Il souligne l'impératif, pour l'Europe, d'accélérer l'innovation, en particulier dans le numérique, en concentrant les programmes de recherche sur un plus petit nombre de priorités, en procédant à une évaluation de la réglementation numérique, en réduisant le coût de déploiement de l'intelligence artificielle (IA), ou encore, en promouvant le partage des données.

La proposition de résolution européenne n° 351 (2024-2025) déposée par le groupe Socialiste, Écologiste et Républicain du Sénat, dans le même esprit, appelle de ses vœux une stratégie numérique européenne renouvelée qui doit permettre la mise en place d'une politique industrielle volontariste, d'une politique de recherche ambitieuse et d'un écosystème numérique démocratique robuste afin d'instaurer des plateformes européennes souveraines et un *cloud* souverain européen, ceci devant en outre permettre à l'Union européenne de jouer un rôle dans le développement de l'intelligence artificielle (IA) et des technologies quantiques.

I. L'UNION EUROPÉENNE DISPOSE D'UN CADRE DE RÉGULATION DU NUMÉRIQUE AMBITIEUX AUJOURD'HUI MIS AU DÉFI

A. LA RECHERCHE D'UN DÉVELOPPEMENT DU NUMÉRIQUE CONFORME AUX PRINCIPES DES DÉMOCRATIES EUROPÉENNES PAR DES TEXTES NOVATEURS DONT L'AMBITION A ÉTÉ SOUTENUE PAR LE SÉNAT

Depuis 2016, l'Union européenne s'est dotée d'un cadre normatif pionnier dans le domaine du numérique, qui tente de concilier protection et valorisation sécurisée des données, concurrence équitable, retrait des contenus illicites et transparence.

1. Le règlement général sur la protection des données (RGPD) garantit les droits des citoyens sur leurs données personnelles

a) Les données, « matière première » de l'économie numérique et enjeu stratégique

Les données sont au cœur de l'économie numérique, elles en sont même « la matière première ». Mais à la différence du pétrole, et aux autres ressources physiques nouvelles qui avaient accompagné les précédentes révolutions industrielles et technologiques, les données sont illimitées. La numérisation des économies et des sociétés a pour conséquence première la production et la mise à disposition de nouvelles données, du fait de l'activité des personnes (ex : achat en ligne, démarches administratives dématérialisées, conduite d'un véhicule assisté par un ordinateur de bord, etc.).

Dès lors qu'elles sont captées et recueillies pour faire l'objet d'un traitement de données, ce dernier peut servir à de multiples bénéficiaires. De plus, une donnée peut faire l'objet de plusieurs traitements par divers acteurs.

« La valorisation des données résulte essentiellement de leur traitement et de leur mise en relation : agrégation, rapprochement de jeux de données de sources diverses, analyses, extrapolations. Prise isolément, une donnée ne génère en effet généralement que très peu de valeur. » [1]

Or, les grands acteurs du numérique disposent désormais de technologies leur permettant de traiter des données en masse *(big data)*, en particulier avec l'intelligence artificielle (IA).

Économiquement, cette valorisation des données permet aux entreprises du numérique de créer de nouveaux services numériques (avec des coûts décroissants) et de les personnaliser en « ciblant » les goûts, habitudes et préférences des individus. Elle leur confère également des positions dominantes qui leur permettent de mettre des « barrières à l'entrée » pour décourager d'éventuels concurrents.

---

[1] *Rapport n°7 (2019-2020) de la commission d'enquête du Sénat sur la souveraineté numérique, p 55.*

Politiquement et géopolitiquement, la détention et le contrôle des données est devenu un enjeu stratégique majeur. Il permet de tout connaître des habitudes et des goûts des individus et, dans les régimes autoritaires, de les surveiller. Dans nos sociétés, il facilite également la possibilité d'influencer leurs décisions, leurs votes…

Or, les services numériques dans l'Union européenne sont très largement assurés par des entreprises extra-européennes.

Ainsi, le moteur de recherche Google est utilisé pour 90 % des recherches en ligne dans l'Union européenne.

Concernant l'utilisation des réseaux sociaux, en novembre 2024, 269 millions de personnes utilisaient Instagram dans l'Union européenne, 261 faisaient de même avec Facebook, 160 avec TikTok et 105 millions étaient actives sur X.

Enfin, trois entreprises américaines[1] se partageaient 72 % du marché européen fin 2022 et 66 % du marché mondial du *cloud* fin 2023 (Amazon web services : 31 % ; Microsoft Azure : 24 % ; Google cloud : 11%).

b) Le règlement général sur la protection des données (RGDPD) permet à chacun de garder la maîtrise de ses données

Face à cette tendance à la marchandisation et à la manipulation des données, sous l'influence de la législation pionnière de la France dite « Informatique et libertés » du 6 janvier 1978, l'Union européenne a reconnu les droits d'une personne à garder la maîtrise de ses données en adoptant le règlement général sur la protection des données (RGPD)[2].

Brève présentation du RGPD

Adopté le 27 avril 2016 et entré en vigueur, le 25 mai 2018, le RGPD est un texte majeur de protection des droits des personnes physiques à l'ère numérique et de contrôle de l'utilisation de leurs données personnelles par des entreprises et organisations.

Les « données à caractère personnel » y sont définies comme « toute information se rapportant à une personne physique identifiée ou identifiable ».

Elles doivent être traitées de manière licite, loyale et transparente et collectées pour des finalités déterminées, explicites et légitimes.

[1] *Amazon web services (AWS) ; Microsoft Azure ; Google cloud. Études du synergy research group.*
[2] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*

Les droits des personnes physiques :

Toute personne dont les données personnelles font l'objet d'un traitement dispose de droits sur ces données :

- elle doit consentir clairement à ce traitement de données, après avoir été correctement informée de ses modalités et de son objet. Mais elle peut aussi s'opposer à ce traitement ;

- elle bénéficie d'un accès facilité à ses données et peut en obtenir la rectification, l'effacement et l'oubli ;

- elle jouit d'un droit à la portabilité de ses données, d'un prestataire de services à un autre.

Les entreprises et organisations responsables d'un traitement de données, ont aussi l'obligation de notifier les violations de données à caractère personnel et de désigner en leur sein, un délégué à la protection des données.

Les modalités de contrôle du RGPD :

Chaque État membre doit mettre en place une autorité de contrôle indépendante (la CNIL en France). Afin d'assurer la cohérence de leurs décisions, ces autorités nationales siègent au sein d'un comité européen de la protection des données.

Chaque personne concernée par un traitement de données personnelles peut introduire une réclamation contre ce dernier auprès d'une autorité de contrôle, mais aussi de contester la décision de cette dernière et d'obtenir, le cas échéant, une indemnisation.

Les responsables d'un traitement de données ayant violé le RGPD (ou leurs sous-traitants) peuvent faire l'objet d'amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % de leur chiffre d'affaires mondial.

À titre d'exemple, le 22 juillet dernier, l'autorité néerlandaise de protection des données, en coopération avec la CNIL, a infligé une amende de 290 millions d'euros à la société Uber pour avoir transféré les données personnelles des chauffeurs travaillant pour elle vers les États-Unis, sans respecter le RGPD.

En outre, les États membres peuvent prévoir des sanctions pénales. Ainsi, en France, l'article 226-21 du code pénal prévoit une sanction en cas de **détournement de la finalité** lors du traitement des **données personnelles** pouvant aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende.

Ce règlement est d'autant plus protecteur que sa portée est extraterritoriale. Il s'applique en effet à tout traitement de données personnelles, automatisé ou non, « effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union [européenne], que le traitement ait lieu ou non dans l'Union ». Ses dispositions sont applicables indépendamment du lieu de traitement effectif des données.

Ce faisant, les transferts de données personnelles vers des pays tiers doivent aussi respecter les garanties du RGPD. Le règlement prévoit une liste d'éléments qui, cumulés, permettent à la Commission européenne d'évaluer le caractère adéquat du niveau de protection des données du pays tiers (législation interne du pays, existence d'une ou de plusieurs autorités de contrôle indépendantes en matière de protection des données, engagements internationaux pris par le pays, etc.).

Puis si l'examen de ces éléments est probant, la Commission adopte alors une décision d'adéquation[1], qui établit qu'un pays tiers (c'est-à-dire un pays non lié par le RGPD) ou une organisation internationale assure un niveau de protection adéquat des données personnelles. Une telle décision d'adéquation a pour effet de permettre le transfert, sans exigences supplémentaires, de données personnelles depuis les États membres soumis au RGPD vers le pays tiers ou l'organisation concerné.

En pratique, ces règles ont conduit la Cour de justice de l'Union européenne (CJUE) à annuler le dispositif *Privacy shield* (ou bouclier de la protection des données), validé par la Commission européenne et signé entre l'Union européenne et les États-Unis avant l'entrée en vigueur du RGPD, le 1er août 2016. Dans un arrêt « Schrems II »[2], la Cour a, en effet considéré que le *Privacy shield* :

- ne fournissait pas les garanties nécessaires pour limiter l'accès des autorités publiques américaines aux données personnelles concernées dans l'Union européenne, compte tenu des lois américaines[3] sur la surveillance ;

- n'assurait ni une protection judiciaire efficace contre les programmes de surveillance américains, ni le droit à un recours effectif pour les personnes localisées sur le territoire d'un État membre de l'Union européenne devant un organisme offrant des garanties substantiellement équivalentes à celles exigées par le droit de l'Union européenne.

---

[1] *Une telle décision peut être prise sur la base de l'article 45 du RGPD.*

[2] *CJUE, 16 juillet 2020,* Data Protection Commissioner*/Maximillian Schrems et Facebook Ireland, aff. C-311-18.*

[3] *Ainsi, le* Cloud Act *(pour* Clarifying Lawful Overseas Use of Data Act*), adopté en mars 2018, après le RGPD européen, prévoit que toute société dont le siège est aux États-Unis, ainsi que les sociétés contrôlées par elle, doit communiquer aux autorités américaines, sur leur demande, les données de communication placées sous son contrôle, sans considération du lieu de stockage de ces données. Cette loi permet aux autorités américaines de s'affranchir des procédures classiques de demandes d'entraide entre États et de coopération judiciaire internationale. Et sa portée est explicitement extraterritoriale puisqu'elle vise les « communications, données et informations localisées à l'intérieur comme en dehors des États-Unis ».*
En outre, le Foreign Intelligence Surveillance Act *(FISA) autorise les agences de renseignement américaines à collecter des données de citoyens et d'entreprises, en dehors du territoire des États-Unis.*

À la suite de cette annulation, les transferts de données personnelles entre les États membres de l'Union européenne et les États-Unis n'étaient plus juridiquement sécurisés et l'efficacité du RGPD a été démontrée pour « contrer », en partie au moins, la portée extraterritoriale des lois américaines.

En effet, sans remettre en cause la possibilité pour les services de renseignement américains de « piocher » dans les données personnelles des entreprises nationales ayant des activités en Europe, le président Joe Biden a adopté, le 7 octobre 2022, un décret présidentiel (*executive order*) qui soumet ces collectes de données aux principes de nécessité et de proportionnalité, et instaure une nouvelle procédure de recours auprès d'une cour de contrôle de la protection des données. Cette cour a le pouvoir d'enquêter sur les plaintes des citoyens européens et de prendre des décisions correctives contraignantes.

En conséquence, le 10 juillet 2023, la Commission européenne a pris une nouvelle décision d'adéquation pour les transferts de données entre l'Union européenne et les États-Unis. Elle en modifie peu les conditions de transfert qui restent d'une grande fragilité.

Ce faisant, l'Union européenne dispose d'un cadre protecteur qui s'impose comme un levier d'influence juridique.

c) L'encouragement au partage sécurisé des données

Une fois ce cadre protecteur mis en œuvre, l'Union européenne a adopté plusieurs textes précisant les modalités sécurisées de partage des données, afin de ne pas rester à l'écart de « l'économie de la donnée » :

- le règlement sur la gouvernance européenne des données (*Data Governance Act*)[1], adopté en mai 2022 et entré en vigueur en septembre 2023, tend à faciliter la réutilisation de données protégées du secteur public (données personnelles, informations commerciales, propriété intellectuelle) et a donné un statut aux fournisseurs de services d'intermédiation de données (certification obligatoire) ;

- le règlement sur les données (ou *Data Act*)[2], adopté en décembre 2023 et entré en vigueur en janvier 2024, a pour objectif d'assurer une meilleure répartition de la valeur issue de l'utilisation des données personnelles et non personnelles entre les acteurs économiques (en particulier *via* des objets connectés). Il facilite donc le partage des données entre entreprises et avec le consommateur ainsi que le changement de fournisseur de services de traitement de données, permet l'utilisation des données détenues par les entreprises, par les organismes publics des États membres et de l'Union européenne, sous réserve que ceux-ci justifient d'un besoin

[1] *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).*

[2] *Règlement (UE) 2023/ du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données).*

exceptionnel, prévoit des règles d'interopérabilité pour les données, et met en place des garanties contre les accès illicites des gouvernements des pays tiers aux données non personnelles contenues dans le *cloud*.

Ainsi, les États membres et l'Union européenne ont établi un cadre normatif unique au monde qui permet d'exploiter et de valoriser les données, tout en assurant un niveau élevé de protection des données personnelles et de la vie privée de leurs détenteurs.

Mais alors que le rapport Draghi précité a attiré l'attention sur le risque de chevauchement réglementaire et d'incohérences entre le règlement européen sur l'intelligence artificielle et le RGPD, et a préconisé l'élaboration de règles simplifiées ainsi qu'une mise en œuvre harmonisée du RGPD, la Commission européenne a annoncé vouloir présenter une nouvelle stratégie sur l'utilisation des données, afin d'en assouplir de nouveau le partage et l'utilisation.

C'est pourquoi la commission des affaires européennes du Sénat, qui est favorable par principe aux efforts de simplification du cadre normatif européen, veillera toutefois à la préservation du RGPD et du rôle des autorités nationales de protection des données qui ont prouvé leur efficacité pour protéger les citoyens sans décourager l'innovation.

2. Le règlement européen sur les marchés numériques (*Digital Markets Act* – DMA) et le règlement européen sur les services numériques (*Digital Services Act* – DSA)

Pour faire face à la fragmentation juridique qui caractérisait le marché numérique en Europe, la Commission européenne a présenté le 15 décembre 2020 une proposition de règlement relatif à un marché intérieur des services numériques (« règlement sur les services numériques », ou DSA, qui renforce et actualise les règles horizontales définissant les responsabilités et obligations des prestataires de services numériques dans l'Union), conjointement à sa proposition de règlement relatif aux marchés numériques (*Digital Markets Act* ou DMA, visant à assurer une concurrence plus équitable entre les acteurs du numérique).

a) Deux propositions relativement ambitieuses visant à mettre fin au « Far West » *numérique*[1]

Publiés en décembre 2020 et déposés sur le bureau des assemblées parlementaires françaises le 4 février 2021, ces deux textes sont des maillons essentiels du marché unique du numérique.

---

[1] *Expression usuelle de l'ancien commissaire européen en charge du numérique, Thierry Breton, qui a exposé sa vision des enjeux actuels devant la commission des affaires européennes du Sénat le 29 janvier 2025 : https://www.senat.fr/compte-rendu-commissions/20250127/euro.html#toc2.*

Le DSA est un règlement européen dont le but est de freiner la diffusion de contenus illégaux et d'instaurer plus de transparence entre les plateformes en ligne et leurs utilisateurs. Pour cela, le DSA distingue les petites plateformes en ligne, les « très grandes plateformes en ligne » et les « très grands moteurs de recherche ». Le DSA détermine un seuil de 45 millions d'utilisateurs par mois pour être désigné très grande plateforme ou très grand moteur de recherche. Sont ainsi concernés les « fournisseurs de services intermédiaires en ligne », c'est-à-dire les hébergeurs, les réseaux sociaux, les moteurs de recherche, les plateformes de voyage et d'hébergement, ou encore les sites de vente. Le DSA n'est pas un outil de gestion de crises mais de gestion des risques.

Le DMA vise à mieux encadrer les activités économiques des plus grandes plateformes, qualifiées de « contrôleurs d'accès » par la Commission européenne dans la mesure où les plus petites entreprises et les consommateurs sont dépendants de leurs services et où la concurrence des autres sociétés se trouve freinée. Sont donc concernées les grandes plateformes ayant un poids important sur le marché intérieur, fournissant un service essentiel qui constitue un point d'accès majeur et bénéficiant d'une position solide et durable.

Pour être désignée contrôleur d'accès, une plateforme doit remplir plusieurs critères cumulatifs :

– une position économique forte, c'est-à-dire au moins 7,5 milliards d'euros de chiffre d'affaires réalisés dans l'Espace économique européen ou une capitalisation boursière d'au moins 75 milliards d'euros avec une activité dans au moins trois États membres ;

– le contrôle d'un service de plateforme essentiel (moteur de recherche, réseau social, messagerie, place de marché en ligne, etc.) utilisé par au moins 45 millions d'Européens par mois et au moins 10 000 professionnels par an dans l'Union ;

– et une position durable sur le marché, attestée par le dépassement, au cours des trois années précédentes, des seuils énumérés aux deux premiers critères.

Toute société remplissant ces critères a l'obligation d'en informer la Commission dans les deux mois. En retour, cette dernière dispose à son tour de deux mois pour la désigner contrôleur d'accès. Ensuite, les plateformes disposent d'un délai maximum de six mois pour se conformer aux obligations prévues par le DMA.

La Commission européenne pourra aussi désigner comme contrôleur d'accès une entreprise qui n'atteindrait pas tous les seuils mais serait considérée comme trop dominante, en fonction de certains critères (taille de la plateforme, y compris le chiffre d'affaires et la valeur boursière, nombre d'entreprises utilisatrices et d'utilisateurs finaux, effets de réseau et avantages tirés des données ou capacité d'analyse de celles-ci, effets d'échelle et de

gamme, y compris en ce qui concerne les données et, le cas échéant, les activités en dehors de l'Union, captivité des entreprises utilisatrices ou des utilisateurs finaux, structure conglomérale). Les entreprises concernées pourront contester leur désignation.

b) Des obligations découlant des statuts de plateforme en ligne ou de contrôleur d'accès

Le DSA et le DMA imposent diverses exigences pour les plateformes en lignes et contrôleurs d'accès.

Ainsi, aux termes du DSA, les plateformes ont l'obligation :

– de veiller à rédiger leurs conditions générales de façon compréhensible, c'est-à-dire **simple, intelligible, aisément accessible et sans ambiguïté**, y compris les informations relatives aux possibilités de recours pour l'utilisateur ;

– d'informer leurs utilisateurs de toute modification importante de leurs conditions générales ;

– d'établir des **rapports de transparence** portant sur leurs systèmes internes de traitement des réclamations et leurs activités de modération des contenus ;

– **de suspendre**, pendant une période raisonnable et après avertissement, la fourniture de leurs services aux utilisateurs **diffusant fréquemment des contenus manifestement illicites** ;

– et de prendre des mesures appropriées et proportionnées afin de garantir un niveau élevé de protection de la **vie privée**, de la **sûreté** et de la **sécurité des mineurs**.

Le DMA, quant à lui, vise à limiter les avantages grâce auxquels les contrôleurs d'accès peuvent conserver une **position dominante sur le marché,** prévoyant ainsi :

– l'interdiction pour un contrôleur d'accès de favoriser ses propres services et produits par rapport à ceux des entreprises qui les utilisent, ou d'exploiter les données de ces dernières pour les concurrencer. Il **ne peut pas non plus imposer les logiciels les plus importants** (comme les navigateurs ou les moteurs de recherche) par défaut à l'installation de son système d'exploitation ;

– la possibilité pour une entreprise utilisatrice de **promouvoir son offre hors d'une plateforme à laquelle elle est liée**, ainsi que de conclure des contrats avec ses clients ou proposer ses propres services aux consommateurs indépendamment de cette dernière ;

– l'accès pour toute entreprise **aux données générées par ses activités** et aux informations liées aux annonces publicitaires qu'elle finance sur une plateforme ;

– la nécessité d'un consentement explicite d'un utilisateur pour l'utilisation de ses données personnelles à des fins de publicité ciblée ;

– la garantie d'une interopérabilité des principaux **services de messagerie** (tels que WhatsApp ou Facebook Messenger) avec leurs concurrents plus petits ;

– l'information de la Commission en cas d'**acquisitions et de fusions**.

c) Des possibilités d'enquête et de sanctions associées, dont la Commission européenne

(1) Les sanctions prévues au titre du DSA

En vertu du DSA, si, sur la base d'informations obtenues au cours de sa surveillance ou de sources fiables, en cas de manquement, la Commission soupçonne une infraction, elle peut décider d'ouvrir une enquête. Si la Commission continue de soupçonner une infraction à la législation sur les services numériques à la suite de l'enquête, elle peut ouvrir une procédure. Toutefois, avant d'adopter toute décision de sanction, elle doit entendre les responsables de la plateforme concernée. Si la violation est confirmée, alors la Commission peut lui infliger une **amende dans la limite de 6 % de son chiffre d'affaires mondial annuel** au cours de l'exercice précédent, ainsi que lui ordonner de prendre des mesures pour remédier au manquement dans un délai fixé.

En outre, si la plateforme ne respecte pas les mesures visant à remédier au manquement, elle peut se voir appliquer des **astreintes** allant **jusqu'à 5** % de son chiffre d'affaires quotidien moyen mondial **par jour** de retard.

Enfin, en dernier recours, en cas de manquements graves et répétés, la Commission européenne peut demander la **suspension temporaire du service**, sous réserve que : (i) elle ait invité les parties intéressées à présenter des observations écrites dans un délai qui ne peut être inférieur à 14 jours ouvrables, en décrivant les mesures qu'elle entend demander et en identifiant le ou les destinataires visés, (ii) elle ait demandé au coordinateur pour les services numériques de l'État membre d'établissement de demander à l'autorité judiciaire compétente une injonction de restreindre temporairement l'accès au service concerné par l'infraction et (iii) ledit coordinateur demande l'ordonnance. Cette dernière doit être rendue par un juge de l'État membre d'établissement de la plateforme.

Les très grandes plateformes et moteurs de recherche sous la surveillance de la Commission européenne et leur pays coordinateur

AliExpress (Pays-Bas)	Meta Instagram (Irlande)
Amazon (Luxembourg)	Bing Microsoft (Irlande)
Apple (Irlande)	XNXX (République Tchèque)
Pornhub (Chypre)	Pinterest (Irlande)
Booking (Pays-Bas)	Snapchat (Pays-Bas)
Google recherche (Irlande)	Stripchat (Chypre)
Google Play (Irlande)	TikTok (Irlande)
Google maps (Irlande)	X (Irlande)
Google shopping (Irlande)	Temu (Irlande)
YouTube (Irlande)	XVideos (République Tchèque)
Shein (Irlande)	Wikipédia (Pays-Bas)
LinkedIn (Irlande)	Zalando (Allemagne)
Meta Facebook (Irlande)	

Depuis l'entrée en vigueur du DSA, dix procédures ont été ouvertes par la Commission européenne : une contre X, trois contre TikTok, une contre AliExpress, deux contre Meta (Facebook et Instagram) et une contre Temu. À ce jour, des conclusions préliminaires ont été adoptées s'agissant de l'enquête contre X, et un dossier a été clôturé, celui contre TikTok et de son programme « Lite Rewards », auquel la plateforme a finalement renoncé.

(2) Les sanctions prévues par le DMA

Au titre du DMA, la Commission peut décider de procéder à des **enquêtes de marché**, soit en vue de désigner un contrôleur d'accès, soit en cas de non-respect systématique d'une ou plusieurs obligations par un contrôleur d'accès. Elle est dotée à cet effet de pouvoirs d'investigation (recueil de renseignements, auditions, inspections, accès aux systèmes informatiques, audits et expertises) et peut ordonner des mesures provisoires.

En cas de violation établie d'obligations, la Commission peut infliger à l'entreprise des **amendes à concurrence de 10 % du chiffre d'affaires mondial total** (jusqu'à 20 % en cas de récidive). Elle peut aussi prononcer des **astreintes jusqu'à 5 %** du chiffre d'affaires quotidien mondial total. Si l'entreprise enfreint la législation européenne de façon répétée (au moins trois violations en l'espace de huit ans), la Commission peut ouvrir une enquête de marché, voire imposer des **mesures correctives comportementales ou structurelles**, par exemple obliger l'entreprise à céder une activité (vente d'unités, d'actifs, de droits de propriété intellectuelle ou de marques) ou lui

interdire d'acquérir des entreprises qui fournissent des services dans le numérique ou des services de collecte de données.

Les autorités nationales de concurrence peuvent être chargées d'enquêter ou prendre l'initiative de procéder à des enquêtes ; elles transmettent alors leurs conclusions à la Commission. En outre, leurs agents doivent prêter assistance aux enquêteurs de la Commission pour les inspections, en requérant au besoin la force publique. Une coopération (échanges d'informations et mise en œuvre des mesures d'exécution) est par ailleurs rendue possible dans le cadre du Réseau européen de la concurrence (REC).

Les contrôleurs d'accès (*gatekeepers*) désignés au titre du DMA

- Alphabet (Google, YouTube, Android)
- Amazon
- Apple
- Booking
- ByteDance (TikTok)
- Meta (Facebook, Instagram, WhatsApp, Messenger)
- Microsoft (LinkedIn, Windows)

Des enquêtes sont actuellement en cours, au titre du DMA, contre Apple, Google ou encore Meta. Cinq des enquêtes ont été ouvertes le 25 mars 2024, deux semaines après l'entrée en vigueur du règlement. Considérant que le DMA laisse un délai de douze mois à la Commission pour clore son enquête, les premières enquêtes ouvertes sont encore en cours. Dès que la Commission aura rédigé ses conclusions préliminaires, elle devra les transmettre au contrôleur d'accès concerné, qui aura la possibilité de les contester, avant que la décision finale ne soit rendue. Cette dernière est susceptible de recours devant la Cour de justice de l'Union européenne (CJUE).

d) Des exigences européennes adaptées en droit français par la loi « SREN »

Promulguée le 21 mai 2024, la loi n° 2024-449 visant à sécuriser et à réguler l'espace numérique (SREN) a bénéficié d'apports importants du Sénat. Parmi ses nombreuses dispositions[1], plusieurs tendent à faciliter la mise en œuvre du DMA et du DSA.

[1] *Ce projet de loi renforce la protection des mineurs en ligne et celle des citoyens dans l'environnement numérique. Elle vise également à lutter contre les pratiques déloyales entre entreprises sur le marché de l'informatique en nuage et à mieux assurer leur interopérabilité, ainsi qu'à assurer la protection des données sensibles ou stratégiques. Il a été examiné au Sénat par une commission spéciale présidée par Mme Catherine Morin-Desailly et dont les rapporteurs étaient M. Patrick Chaize et M. Loïc Hervé.*

Ainsi :

– **au titre du DMA**, la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et l'Autorité de la concurrence, en coopération avec la Commission européenne dans le cadre du « Réseau européenne concurrence », sont désignées comme autorités compétentes. Des pouvoirs d'inspection et d'enquête leur sont reconnus et des juridictions spécialisées sont chargées de traiter des litiges résultant de ce règlement ;

– de plus, le ministre chargé de l'économie ou son représentant est habilité à adresser à la Commission européenne, conjointement avec au moins trois autres États membres, une demande d'ouverture d'enquête de marché lorsqu'il existe des motifs raisonnables de soupçonner qu'une entreprise est « contrôleur d'accès » ;

– **au titre du DSA**, l'ARCOM est désignée comme coordinateur des services numériques en France. Mais la Commission nationale de l'informatique et des libertés (CNIL) est chargée de vérifier le respect par les plateformes des limitations posées en matière de profilage publicitaire. Quant à la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), elle est compétente pour contrôler le respect des obligations des fournisseurs de places de marché. Conformément au DSA, leurs pouvoirs d'enquête, d'exécution et de sanction sont également précisés ;

- la loi instaure également un réseau national de coordination de la régulation des services numériques[1] ;

- les procédures et sanctions de la loi pour la confiance en l'économie numérique[2], de la loi relative à la liberté de communication[3] et du code électoral sont mises en conformité avec le DSA.

[1] *Outre l'ARCOM et la CNIL, ce réseau comprend l'Arcep (autorité de régulation des communications électroniques, des postes et de la distribution de la presse), désignée comme « gendarme du* cloud *», la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et la plateforme de signalement des contenus illicites sur Internet, PHAROS.*

[2] *Loi n°2004-475 du 21 juin 2004.*

[3] *Lois n°86-1067 du 30 septembre 1986.*

B. LA RÉGULATION EUROPÉENNE DU NUMÉRIQUE MISE AU DÉFI

1. La régulation européenne garantit la liberté d'expression et protège les autres droits et libertés des citoyens

a) Comme l'a souligné le Sénat à plusieurs reprises, la régulation mise en place en France et par l'Union européenne permet de garantir la liberté d'expression et d'en sanctionner les abus

La liberté d'expression est un « principe à double face » puisqu'à la liberté des émetteurs répond le droit des destinataires à en bénéficier, de sorte que « l'une comme l'autre doivent être défendues ». En outre, elle est d'autant plus importante qu'elle garantit l'exercice d'autres libertés fondamentales[1].

La France lui a conféré une existence juridique en 1789, dans l'article 11 de la Déclaration de l'homme et du citoyen du 26 août 1789. Cet article souligne aussi d'emblée que cette liberté doit être conciliée avec d'autres droits fondamentaux : ainsi, « la libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme ». Par la suite, la valeur cardinale de cette liberté a été confirmée par l'article 10 de la Convention européenne des droits de l'homme et des libertés fondamentales du 4 novembre 1950[2] et par l'article 11 de la Charte européenne des droits fondamentaux.

Dans un arrêt important, « Handyside contre Royaume-Uni », la Cour européenne des droits de l'Homme (CEDH) a précisé que la liberté d'expression constituait « l'un des fondements essentiels [d'une société démocratique], l'une des conditions primordiales de son progrès et de l'épanouissement de chacun »[3].

En conséquence de cette reconnaissance, en France, la liberté de la presse et, plus largement, la liberté de communication sont reconnues (par les lois du 29 juillet 1881 et du 30 septembre 1986). Le respect de ces libertés est valable dans la sphère numérique : en France, le Conseil constitutionnel a affirmé que le droit de s'exprimer et de communiquer librement impliquait la liberté d'accéder à Internet dans sa décision n° 2009-580 DC en date du 10 juin 2009. Au niveau européen, sous l'impulsion de la CEDH, le rôle d'Internet dans l'exercice de la liberté d'expression a été rapidement reconnu[4].

---

[1] « Les interdits et la liberté d'expression », Guy Carcassonne, professeur de droit à l'université Paris Ouest-Nanterre – La Défense, Nouveaux cahiers du Conseil Constitutionnel n°36 (juin 2012).

[2] 1. » Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. »

[3] CEDH, 7 décembre 1976, Handyside contre Royaume-Uni, aff. n° 5493/72.

[4] Voir CEDH, 10 mars 2009, Times Newspapers Ltd. Contre Royaume-Uni, aff. n° 3002/03 et 23676/03 et 10 janvier 2013, Ashby Donalds et autres contre France, aff. n° 36769/08.

La liberté d'expression n'est toutefois pas absolue. Elle doit être conciliée avec d'autres droits et libertés. De plus, elle ne doit pas permettre d'exprimer des propos contraires à la dignité humaine ou à l'ordre public.

Cet équilibre était déjà présent dans l'article 11 précité de la Déclaration des droits de l'homme et du citoyen, qui soulignait que « tout citoyen peut donc parler, écrire, imprimer librement sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ».

Il a été confirmé par l'article 10 précité de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, selon lequel l'exercice de cette liberté peut être soumis « à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

Cependant, Internet pose des défis spécifiques quant au respect de cet équilibre, à la fois du fait de la possibilité, pour chacun, d'élaborer et de publier des contenus en ligne, de la multiplication des sources d'information disponibles, de l'usage répandu de l'anonymat, et de la rapidité de la publication des informations et messages. Ce faisant, comme le rappelait le rapport de la commission des affaires européennes du Sénat sur le DSA[1], « l'usage généralisé des services numériques est aussi devenu une source de risques : la prolifération, sur Internet, de propos haineux, de contenus de désinformation, de produits contrefaits ou dangereux, et d'activités illicites en tout genre, est susceptible d'affecter gravement les individus, mais aussi de fragiliser les sociétés dans leur ensemble ».

C'est pourquoi, en France, quel que soit leur format de diffusion, les propos ou écrits alléguant ou imputant un fait précis portant atteinte à l'honneur ou à la considération d'une personne constituent une diffamation[2] et sont pénalement condamnables. Il en va de même pour les personnes ayant provoqué un crime ou un délit portant atteinte aux intérêts fondamentaux de la nation[3].

---

[1] Rapport n°274 (2021-2022) de Mmes Florence Blatrix Contat et Catherine Morin-Desailly au nom de la commission des affaires européennes du Sénat, sur la proposition de législation européenne sur les services numériques (DSA), en date du 8 décembre 2021.

[2] La diffamation publique est passible d'une amende de 12 000 euros. Si elle a un caractère racial ou discriminatoire, elle est passible d'une peine d'un an d'emprisonnement et de 45 000 euros d'amende.

[3] Cette « provocation » peut être punie d'une peine allant jusqu'à cinq ans d'emprisonnement et 45 000 euros d'amende.

En outre, en 2020, un observatoire de la haine en ligne a été créé auprès de l'ARCOM pour assurer le suivi des contenus haineux. Et, en 2022[1], l'ARCOM a été chargée de veiller au respect des dispositions de la loi du 24 août 2021 prévoyant de nouvelles obligations de modération et de signalement des contenus illicites. En vertu de la loi « SREN », ces dispositions ont, depuis, été remplacées par celles du règlement européen DSA.

Enfin, les contenus illicites[2] hébergés sur le web peuvent être signalés à la plateforme PHAROS[3], composée de policiers et de gendarmes, qui va les examiner. Si cet examen confirme le caractère illicite du contenu, le signalement est transmis au procureur de la République pour ouverture d'une enquête pénale, enclenchant une demande de retrait du contenu visé au fournisseur concerné. L'accès aux contenus terroristes ou pédopornographiques signalés doit être bloqué sans délai par le fournisseur et ces contenus doivent être retirés dans les 24 heures[4]. Un dispositif similaire a été institué en Allemagne par la loi NetzDG du 1er octobre 2017[5].

Au niveau européen, la Cour de justice de l'Union européenne (CJUE) a reconnu, sous conditions, un droit à l'oubli numérique des individus demandant la suppression de liens obsolètes et préjudiciables les concernant. Elle a alors effectué un contrôle de proportionnalité entre liberté d'expression et respect de la vie privée[6].

Puis, depuis le 17 février 2024, le DSA a harmonisé les réglementations nationales des 27 États membres pour réguler les actions des fournisseurs de services en ligne afin d'assurer un environnement en ligne sûr. Ce faisant, il a facilité l'activité économique des fournisseurs de services en ligne souhaitant avoir accès au marché intérieur. Ce texte établit un régime de responsabilité limitée des hébergeurs au terme duquel un hébergeur ne peut être tenu pour responsable des contenus illicites présents sur ses services dès lors qu'il n'avait pas eu connaissance de leur présence ou de leur caractère illicite ou que, ayant eu connaissance de tels contenus, il a « agi promptement » pour les retirer ou les rendre inaccessibles.

---

[1] Décret d'application de l'article 42 de la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

[2] Pédophilie et pédopornographie ; expression du racisme, de l'antisémitisme et de la xénophobie ; incitation à la haine raciale, ethnique et religieuse ; terrorisme et apologie du terrorisme ; escroqueries et arnaques financières utilisant Internet.

[3] Pour le seul second semestre 2023, PHAROS a reçu 120 322 signalements, dont 35 250 pour escroqueries et extorsions, 17 067 pour discrimination, 16 473 pour atteintes sur mineurs, 13 281 pour terrorisme, ou encore 8 289 pour menaces. En parallèle, PHAROS a demandé aux opérateurs le retrait de 67 295 contenus d'atteintes sexuelles sur mineurs, de 2 549 contenus terroristes et a notifié 1 137 contenus divers (discriminatoires pour l'essentiel) aux hébergeurs afin qu'ils les retirent.

[4] Article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique modifié par l'article n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN).

[5] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken.

[6] CJUE, 13 mai 2014, Google Spain, aff. C-131/12.

En résumé, en Europe, la liberté d'expression est bien le principe, et ses limites sont liées à la sanction de propos ou écrits mettant en cause la dignité humaine ou troublant gravement l'ordre public.

b) Les règles européennes sont aujourd'hui attaquées comme contraires à la liberté d'expression

Au cours des derniers mois, certains dirigeants de pays tiers ou de très grandes plateformes en ligne ont critiqué le principe même des règles européennes du numérique, en les assimilant à de la censure.

Pour critiquer le DSA et le cadre normatif européen, ces dirigeants invoquent la conception absolue de la liberté d'expression, inscrite depuis 1791 dans la Constitution américaine. Le premier amendement de cette dernière affirme en effet que « le Congrès n'adoptera aucune loi […] pour limiter la liberté d'expression ».

Cette conception absolue du ***free speech*** a été « sanctuarisée » par la Cour suprême américaine, durant les années 1950-70, alors qu'elle était présidée par le juge Earl Warren, contre le souhait d'autorités locales ou du gouvernement fédéral de limiter la liberté de la presse. Ainsi, dans l'affaire dite des *Pentagon Papers*, déclenchée par la publication d'informations confidentielles sur la conduite de la guerre du Vietnam par le New-York Times, la Cour avait estimé que le gouvernement ne pouvait empêcher la divulgation d'informations sensibles, à moins qu'elle entraîne « à coup sûr des dommages directs, immédiats et irréparables à notre nation ou à son peuple »[1].

La Cour a étendu très loin cette notion de liberté d'expression puisqu'elle a estimé qu'un tribunal de l'Illinois ne pouvait interdire une manifestation de militants pro-nazis en uniforme[2], et qu'elle empêchait toute limitation des financements aux campagnes électorales des candidats à une élection par des entreprises car ces financements étaient la garantie de cette liberté d'expression[3].

Dans cet état d'esprit, en 2019, prononçant un discours à l'université de Georgetown, M. Zuckerberg s'inscrivait dans leurs pas pour effectuer un plaidoyer en faveur de la liberté d'expression (« Les citoyens qui ont la liberté de s'exprimer publiquement constituent une nouvelle force de notre monde – un cinquième pouvoir, qui vient s'ajouter aux autres structures de pouvoir de nos sociétés. »), manifestant alors sa méfiance à l'égard de toute régulation par l'État et lançant un avertissement : « en période d'agitation sociale, nous sommes souvent tentés de réduire la liberté d'expression ».

---

[1] *Le Monde, « Comment le* "free speech" *est devenu l'arme des conservateurs aux États-Unis », article de M. Gilles Paris, 17 janvier 2025.*

[2] *Décision «* National socialist party of America vs. village of Skokie », *432 U.S. 43 (1977).*

[3] *Décision «* Citizens united vs. FEC », *558 U.S. 310 (2010).*

Dans le même temps, les plateformes en ligne obtenaient une forme d'impunité sur les contenus qu'elles hébergent aux États-Unis. Tout d'abord, dans un contexte de dérégulation des télécoms, la « section 230 » du *Telecommunications Act* (1996) adoptée par le Congrès, les a exonérées de toute responsabilité pour les propos qui seraient tenus par des tiers sur leurs sites, forums, messageries, etc. Plus récemment, en 2024, la Cour suprême a reconnu le statut d'éditeur à ces plateformes tout en interdisant aux autorités publiques de réguler leurs contenus[1].

Néanmoins, comme le rappelait la commission d'enquête du Sénat sur la souveraineté numérique[2], « loin de l'utopie égalitaire et individualiste des débuts, le cyberespace est bien aujourd'hui le lieu où s'exercent les conflits d'intérêts, les luttes d'influence et des logiques économiques et sociales antagonistes, bref le retour sous des formes nouvelles de la très classique compétition pour la prise de pouvoir ».

Afin de bien comprendre ces attaques, il convient de rappeler brièvement que les grandes entreprises du secteur numérique :

- sont, pour certaines d'entre elles, liées au gouvernement américain. Les GAFAM (acronyme désignant les entreprises Google, Apple, Meta (Facebook), Amazon et Microsoft) garantissent aujourd'hui la mise en œuvre de la politique américaine de contrôle des données, « axe prioritaire tant du redéveloppement économique américain […] que de la stratégie américaine de sécurité »[3]. En outre, la frontière entre ces géants du numérique et l'État américain est « poreuse », certains chercheurs définissant ces imbrications structurelles comme constitutives d'un « complexe techno-étatique »[4] ;

- sont pour d'autres, des entreprises chinoises (surnommées « BAFX », pour désigner les entreprises Baidu, Alibaba, Tencent et Xiaomi auxquelles il faudrait ajouter Bytedance, entreprise « mère » du réseau social TikTok) qui ont des liens structurels avec le parti communiste chinois au pouvoir. La commission d'enquête du Sénat sur le réseau social TikTok a ainsi démontré, d'une part, que les technologies, brevets et ingénieurs de la société Bytedance étaient soumis au contrôle des autorités chinoises et à l'extraterritorialité du droit chinois, d'autre part, que le réseau social avait permis des actions d'espionnage, des campagnes de désinformation en faveur de la Chine et des transferts de données d'utilisateurs de TikTok vers la Chine[5].

---

[1] *Décision «* Moody vs. NetChoice », *LLC, 603, U.S. (2024).*

[2] *Rapport n° 7 (2019-2020) de la commission d'enquête sur la souveraineté numérique (p 14).*

[3] *Commission d'enquête du Sénat sur la souveraineté numérique (président : M. Franck Montaugé ; rapporteur : M. Gérard Longuet), rapport n° 7 (2019-2020) du 1er octobre 2019, p 18-19.*

[4] *« Les GAFAM mènent la danse stratégique », de M. Charles Thibout, site de l'IRIS ; 30 janvier 2019.*

[5] *Rapport n° 831 (2022-2023) du 4 juillet 2023 de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence (président : M. Mickaël Vallet ; rapporteur : M. Gérard Longuet).*

D'ailleurs, quelques exemples démontrent que l'attachement des GAFAM à la liberté d'expression varie selon les circonstances :

- entre 2015 et 2016, la société britannique Cambridge Analytica, spécialisée dans l'analyse de données à grande échelle, a collecté et analysé les données personnelles de 87 millions d'utilisateurs du réseau Facebook sans leur consentement, afin d'influencer l'élection présidentielle américaine de 2016 en faveur du candidat Donald Trump. Facebook avait dû payer une amende de 5 milliards de dollars (en 2019). En décembre 2022, l'entreprise a accepté de verser 725 millions de dollars pour clore les poursuites judiciaires ouvertes à son encontre par la justice américaine[1] ;

- en 2018, le projet « Dragonfly » de Google – finalement avorté – devait permettre de livrer aux autorités chinoises un moteur de recherche conforme aux exigences du parti communiste chinois en matière de censure ;

- en 2021, l'ingénieure américaine Frances Haugen, employée par Facebook entre 2019 et 2021, avait « lancé l'alerte » sur les pratiques de son employeur en transmettant plusieurs documents internes de Facebook au régulateur américain et au Congrès des États-Unis, qui prouvaient que Facebook rechignait à lutter contre les effets nuisibles de ses systèmes algorithmiques fondés sur la recherche du profit, en particulier en matière de contenus haineux et de désinformation.

Lucide sur les motivations des dirigeants des GAFAM, Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique, leur a demandé fermement d'arrêter « d'instrumentaliser la liberté d'expression » et a demandé à la Commission européenne d'appliquer strictement le DSA. « Nous ne sommes pas en train de demander aux États-Unis de réécrire le premier amendement de leur Constitution. Et ils n'ont pas à nous demander de repenser la manière dont nous garantissons la liberté d'expression en Europe et en France depuis deux siècles dans la Déclaration des droits de l'homme. »[2]

2. L'Union européenne face au modèle des réseaux sociaux

a) Les plateformes en ligne sont fondées sur « l'économie de l'attention » qui leur permet d'influencer les comportements de leurs utilisateurs

Depuis plusieurs années, la commission des affaires européennes du Sénat alerte les pouvoirs publics et l'Union européenne sur les « vices » du modèle économique qui fonde les grandes plateformes en ligne. En effet, ce modèle, basé sur « **l'économie de l'attention** », « repose sur l'exploitation par des algorithmes aussi puissants qu'opaques de très grandes quantités de données – en particulier de données à caractère personnel –, utilisées pour le

[1] *https://www.lemonde.fr/pixels/article/2022/12/23/affaire-cambridge-analytica-facebook-accepte-de-payer-725-millions-de-dollars_6155532_4408996.html*

[2] *Le Monde, 9 janvier 2025.*

ciblage des contenus et des publicités, en vue de maximiser le temps passé par l'utilisateur sur leurs services et donc son temps d'exposition à la publicité et, partant, les revenus des plateformes »[1].

Cette préoccupation faisait écho aux révélations de la lanceuse d'alerte Frances Haugen. Entendue au Sénat, elle avait affirmé, sur la base des document internes, que les dirigeants de l'entreprise savaient comment rendre Facebook et Instagram plus sûrs, mais refusaient de réaliser les changements nécessaires parce qu'ils faisaient passer leurs immenses bénéfices avant les personnes. « Les conséquences sont graves. La plateforme Facebook porte aujourd'hui atteinte à la santé et à la sécurité, menace nos communautés et l'intégrité de nos démocraties. »[2]

L'universitaire américaine Shoshana Zuboff a mis en évidence cette dérive de « l'économie de l'attention » qui aboutit à ce qu'elle appelle le « capitalisme de surveillance »[3] : dans ce dernier, les grandes plateformes en ligne collectent les données de leurs utilisateurs, non seulement pour mieux les connaître et leur proposer des publicités ciblées, « mais ils les exploitent pour modifier ou conditionner leurs comportements, non seulement économiques, mais aussi sociaux et politiques. Ce faisant, ils menacent le libre arbitre des individus et, indirectement, l'équilibre des démocraties. »[4]

b) Les grandes plateformes en ligne sont poreuses aux campagnes de manipulations de l'information et d'ingérences étrangères

La manipulation de l'information se définit comme une **opération de diffusion** d'informations falsifiées, déformées, associées à de vraies informations pour les rendre crédibles, ou encore, sorties de leur contexte ou partielles[5]. L'ingérence, quant à elle, est un procédé utilisant des moyens illégitimes et dissimulés, qui « passe principalement mais non uniquement par des **opérations de manipulation de l'information** »[6].

L'utilisation des réseaux sociaux pour essayer d'influencer les résultats d'un scrutin est un problème bien connu des dernières années. Déjà en 2016, les résultats du référendum sur la sortie du Royaume-Uni de l'Union européenne avaient démontré que les campagnes électorales sont désormais influencées par la désinformation et l'utilisation abusive de données.

---

[1] *Rapport d'information n° 274 (2021-2022) de Mmes Florence Blatrix Contat et Catherine Morin-Desailly du 8 décembre 2021 sur la législation européenne sur les services numériques (DSA), au nom de la commission des affaires européennes du Sénat, p 37-38.*

[2] *Audition du 10 novembre 2021 devant la commission des affaires européennes et la commission de la culture, de l'éducation et de la communication du Sénat.*

[3] *« L'âge du capitalisme de surveillance », éd. Profile, 2019 (EN) et ed. Zulam essais, 2020 (FR).*

[4] *Rapport d'information n° 274 (2021-2022) précité, p 37-38.*

[5] *https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/cyberdefense/lutte-contre-manipulation-de-linformation*

[6] *Sénat, commission d'enquête « Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide », rapport n° 739 (2023-2024). https://www.senat.fr/notice-rapport/2023/r23-739-2-notice.html*

En 2024, le service français de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a détecté des manœuvres informationnelles d'origine azerbaïdjanaise qui ont visé notre pays dans le contexte des émeutes en Nouvelle-Calédonie : en pratique, plusieurs montages vidéos trompeurs montrant des policiers français blesser ou tuer des manifestants indépendantistes en Nouvelle-Calédonie ont été diffusés massivement et de manière coordonnée sur les réseaux sociaux X et Facebook. Selon Viginum, ces contenus ont été initialement diffusés par des membres du parti politique présidentiel azerbaïdjanais et par une agence de l'État azerbaïdjanais[1].

Puis, au cours de l'année 2024, deux pays européens candidats à l'Union européenne, **la Moldavie et la Géorgie**, ont fait face à des ingérences fortes lors de scrutins nationaux[2]. En Moldavie, le 20 octobre 2024, à l'occasion du premier tour de l'élection présidentielle et du référendum portant sur l'adhésion à l'Union européenne, la présidente Maia Sandu a accusé des forces étrangères d'être intervenues pour influencer le résultat en déclarant que « Des groupes criminels, agissant de concert avec des forces étrangères hostiles à nos intérêts nationaux, ont attaqué notre pays à coups de dizaines de millions d'euros, de mensonges et de propagande. »[3]

Selon la sénatrice Gisèle Jourda, « la Moldavie est la cible privilégiée de multiples attaques hybrides. […] ces attaques ont fortement interféré avec la campagne électorale, dans les mois et semaines précédant le premier tour de l'élection, prenant la forme de diverses tentatives de manipulations et d'influences, d'achats massifs de voix, de campagnes de désinformation sur les réseaux sociaux, etc. […] c'est sur Instagram, Telegram et TikTok que se sont déroulées pour l'essentiel ces campagnes de désinformation. »[4]

En Géorgie, les élections législatives du 26 octobre 2024 ont donné lieu à des contestations massives, sur fond d'accusation de fraude électorale et d'ingérence étrangère. Le Parlement européen a ainsi adopté une résolution condamnant les élections législatives en Géorgie, considérant qu'elles n'ont été ni libres ni équitables. Le Parlement européen a ainsi condamné « fermement l'ingérence systématique de la Russie dans les processus démocratiques de la Géorgie, par le biais de la désinformation, comme la conspiration du "Parti de la guerre mondiale" qui prétend que l'opposition entraînerait le pays dans une guerre avec la Russie sur ordre de l'Occident »[5]. L'Assemblée parlementaire du Conseil de l'Europe (APCE) a également

---

[1] *Fiche technique du SGDSN en date du 17 mai 2024.*

[2] *Voir la communication des sénateurs Pascal Allizard et Gisèle Jourda, de retour de leurs missions d'observations électorales respectives en Géorgie et en Moldavie, devant la commission des affaires européennes du Sénat (27 novembre 2024).*

[3] *https://www.publicsenat.fr/actualites/international/moldavie-au-lendemain-du-referendum-sur-lunion-europeenne-la-marque-des-ingerences-etrangeres-sur-le-scrutin*

[4] *Voir la note de bas de page n° 2.*

[5] *https://www.europarl.europa.eu/doceo/document/TA-10-2024-0054_FR.html*

adopté une position très ferme, tenant compte d'une mission de suivi réalisée par le sénateur Claude Kern[1].

Fin novembre, c'est une tentative encore plus aboutie de manipulation du scrutin qui a eu lieu à l'intérieur même des frontières de l'Union européenne, en Roumanie, lors du premier tour de l'élection présidentielle, par l'intermédiaire du réseau social chinois TikTok. En effet, Călin Georgescu, candidat inconnu et tardivement déclaré, a remporté le premier tour de l'élection présidentielle roumaine en obtenant près de 23 % des suffrages.

Ainsi que l'indique Viginum dans son rapport *Manipulation d'algorithmes et instrumentalisation d'influenceurs : enseignements de l'élection présidentielle en Roumanie et risques pour la France*, « [p]eu connu du grand public avant l'élection présidentielle, il était crédité de moins de 1 % d'intentions de vote dans les sondages réalisés quatre semaines avant le scrutin, et de 10,6 % d'intentions de vote entre les 20 et 21 novembre 2024. À la suite de ces résultats, de nombreuses analyses ont pointé l'existence de **phénomènes numériques inauthentiques** visant à perturber le bon déroulé de l'élection. Les autorités roumaines ont notamment rendu publiques des notes de renseignement préalablement déclassifiées faisant état de manipulations observées sur la plateforme TikTok et du recours dissimulé à des influenceurs à des fins de propagande électorale, tout en suggérant l'implication d'un acteur étatique étranger. »[2]

La manipulation a ainsi combiné deux méthodes : d'une part, l'*astroturfing*, c'est-à-dire une forme de manipulation donnant l'illusion d'un mouvement d'opinion de masse, par l'utilisation de techniques de propagande, ici algorithmiques, par exemple avec une augmentation artificielle du nombre de likes sur les réseaux sociaux ; d'autre part le recrutement d'influenceurs rémunérés pour inciter les gens à se rendre aux urnes, sans pour autant appeler à voter en faveur d'un candidat particulier, mais dont les publications ou vidéos sur les réseaux sociaux ont permis à l'*astroturfing* décrit précédemment de prendre de l'ampleur.

---

[1] *Voir, pour illustrer cette position, le communiqué de presse du sénateur Claude Kern et de Mme Edite Estrela, co-rapporteurs de l'APCE pour le suivi de la Géorgie, intitulé « Les rapporteurs de l'APCE s'inquiètent de l'arrestation de dirigeants de l'opposition et des brutalités policières à l'encontre des journalistes et de manifestants pacifiques », en date du 10 décembre 2024 ainsi que le rapport d'observation de l'APCE https://pace.coe.int/fr/news/9746/georgie-des-elections-legislatives-marquees-par-une-forte-polarisation-des-conditions-de-concurrence-inegales-et-un-climat-generalise-d-intimidation*

[2] *https://www.sgdsn.gouv.fr/publications/manipulation-dalgorithmes-et-instrumentalisation-dinfluenceurs-enseignements-de*

Comme l'indique le rapport précité de Viginum[1], « TikTok a effectivement reconnu auprès des autorités roumaines qu'il s'agissait là de l'action de « bénévoles coordonnés », équivalente à une « campagne de guérilla politique de masse ».

Le rapport de Viginum précise également qu'» [i]l est enfin important de souligner que les phénomènes inauthentiques observés n'étaient pas limités à TikTok, d'autres modes opératoires ayant par exemple été identifiés sur les plateformes du groupe Meta (Facebook et Instagram). Ces manœuvres informationnelles ont également été accompagnées d'un nombre important de cyberattaques visant les systèmes informatiques liés au processus électoral, témoignant du déploiement d'un dispositif d'ampleur destiné à déstabiliser un grand rendez-vous démocratique. »

En réponse à cette manipulation d'envergure, **la Cour constitutionnelle roumaine a, de manière inédite, annulé, sur le fondement de l'article 146(f) de la Constitution, les résultats du premier tour**, au motif de « s'assurer de sa validité comme de sa légalité », *et a demandé à ce que* « l'intégralité du processus électoral » soit reportée. Depuis, la Roumanie connaît une crise politique. Parallèlement, la Commission européenne a lancé une enquête contre TikTok (voir *infra*).

Ingérence et élections en France : retour sur les scrutins de 2024

Interrogé par les rapporteures de la commission des affaires européennes, Viginum a indiqué que les élections européennes puis législatives organisées en France en 2024 avaient fait l'objet de 25 manœuvres visant à peser dans le débat public, 14 pour les élections européennes et 11 pour les élections législatives. Elles avaient pour objectifs la polarisation des débats autour de certains thèmes, la défiance envers les médias, l'exposition réputationnelle et des récriminations sur le processus électoral. La stratégie observée était celle d'une logique plutôt opportuniste, principalement par des acteurs pro-russes, opérant par la promotion et le dénigrement des candidats, la tromperie des internautes en les renvoyant vers des faux sites contenant du faux contenu, ainsi que l'amplification d'actions réalisées, à l'instar des mains rouges taguées sur le Mémorial de la Shoah. L'impact a cependant été quasi nul, aucune manœuvre n'a eu de visibilité ou d'impact.

Lors de son audition dans le cadre de la présente proposition de résolution le 12 février 2025, le chercheur David Colon préconisait, pour des réseaux sociaux intègres, d'élargir le champ de la responsabilité sociétale des entreprises[2] au champ démocratique, afin de garantir aux usagers qu'ils ne financent aucune campagne de désinformation. En octroyant un tel label,

[1] *Ibid., p. 5*

[2] *La responsabilité sociétale des entreprises correspond à leur responsabilité vis-à-vis des effets qu'elles exercent sur la société.*

M. Colon soulignait que cela pourrait représenter un signal fort dans la lutte contre les acteurs malveillants, étatiques comme non-étatiques.

3. Une réponse européenne qui doit être ferme et fidèle à ses principes

a) Une procédure ouverte quasi immédiatement suite aux évènements en Roumanie

Suite au premier tour de l'élection présidentielle roumaine, la Commission européenne a envoyé le 29 novembre 2024 à TikTok une demande d'informations au titre de la législation sur les services numériques. Elle a ainsi demandé à la plateforme de fournir des informations relatives à sa gestion des risques de manipulation de l'information, parmi lesquelles : (i) la façon dont elle a analysé et atténué le risque d'exploitation inauthentique ou automatisée de son service et les risques découlant de ses systèmes de recommandation, et (ii) des informations sur les efforts déployés par elle pour permettre à un plus grand nombre de tiers d'exercer un contrôle public et d'avoir accès à des données accessibles au public afin de détecter, d'identifier et de comprendre les risques systémiques liés aux processus électoraux[1].

Puis, le 17 décembre 2024, la Commission européenne a ouvert une procédure formelle à l'encontre de TikTok au titre du DSA pour les risques liés à l'intégrité des élections, en particulier l'obligation faite à la plateforme d'évaluer et d'atténuer correctement les risques systémiques liés à l'intégrité des élections, dans le contexte de l'élection présidentielle roumaine[2]. Cette procédure formelle devra déterminer si elle a mis en œuvre des outils d'atténuation des risques concernant ses systèmes de recommandation (risques liés à la coordination de comportements non authentiques ou à l'exploitation automatisée du service) ainsi que ses politiques en matière de publicités à caractère politique et de contenus politiques payants.

Plus précisément, comme l'indique le rapport de Viginum précité, « [a]u-delà des accusations de manipulation de l'information, il est notamment reproché à la plateforme de ne pas avoir été en mesure d'identifier que les vidéos publiées par le compte du candidat Călin Georgescu présentaient un caractère électoral. Celles-ci auraient dès lors bénéficié d'un traitement préférentiel par rapport aux publications des comptes des autres candidats, qui, en étant associées à la campagne électorale, ont été filtrées par l'algorithme de recommandation. Dès le 20 novembre, le Bureau Électoral Central a ainsi signalé à la plateforme des contenus de propagande électorale

---

[1] *La Commission adresse une demande d'informations supplémentaires à TikTok au titre de la législation sur les services numériques | Bâtir l'avenir numérique de l'Europe, https://digital-strategy.ec.europa.eu/fr/news/commission-sends-additional-request-information-tiktok-under-digital-services-act*

[2] *La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques, https://ec.europa.eu/commission/presscorner/detail/fr/ip_24_6487*

ne respectant pas les exigences légales roumaines, en particulier l'identification du mandataire fiscal. Bien que TikTok ait déclaré avoir bloqué ces contenus pour les audiences roumaines, les services de renseignement roumains ont affirmé que ces contenus étaient en réalité toujours accessibles sur la plateforme. »

L'enquête est toujours en cours, le DSA ne prévoyant pas de délai pour rendre les conclusions.

b) Une célérité moindre dans d'autres dossiers

Alors que la crise roumaine avait fait l'objet d'une réaction rapide de la part de l'Union européenne, sa « prudence » face à d'autres évènements suscitait l'étonnement, elle était même parfois suspectée de vouloir suspendre les enquêtes ouvertes contre les plateformes américaines[1].

Ainsi, interrogé sur France Inter le 8 janvier 2025 sur les provocations répétées de la part d'Elon Musk, Jean-Noël Barrot a appelé la Commission européenne « à se saisir de manière beaucoup plus vigoureuse des outils [qui] lui [ont été] donnés pour dissuader ces comportements ». « Soit la Commission européenne applique avec la plus grande fermeté les lois que nous nous sommes données pour protéger notre espace public, soit elle ne le fait pas et alors il faudra qu'elle consente à rendre aux États membres de l'UE, à rendre à la France, la capacité de le faire, » a déclaré M. Barrot.

Sous la pression de certains États membres, dont la France, et de parlementaires européens, la Commission européenne, a fini, le 17 janvier 2025, par annoncer l'approfondissement de son enquête sur X, sous la forme de trois mesures d'enquête technique supplémentaires concernant le système de recommandation de la plateforme. Ainsi, la Commission :

– a demandé à X de fournir une documentation interne sur ses systèmes de recommandation et toute modification récente qui y a été apportée, avant le 15 février 2025 ;

– lui a imposé, par l'intermédiaire d'une « injonction de conservation », de conserver les documents internes et les informations concernant les modifications futures apportées à la conception et au fonctionnement de ses algorithmes de recommandation, pour la période comprise entre le 17 janvier 2025 et le 31 décembre 2025, à moins que son enquête ne soit conclue avant cette date ;

– a demandé l'accès à certaines interfaces de programmation d'applications (API) commerciales de X, afin d'obtenir des informations directes sur la modération du contenu et la viralité des comptes.

[1] *https://www.lemonde.fr/international/article/2025/01/07/face-a-elon-musk-les-europeens-desunis_6486352_3210.html*

Malgré ces annonces, 12 ministres des affaires européennes des États membres, dont le ministre français, ont cosigné un courrier commun à la Commission européenne le 29 janvier 2025, dans lequel ils l'exhortaient « à mener la charge en exploitant pleinement les pouvoirs conférés par le règlement sur les services numériques (DSA) pour remédier à tous les risques et en accélérant les enquêtes en cours », avec en ligne de mire, les élections fédérales allemandes, fin février 2025, et l'élection présidentielle polonaise en mai-juin 2025.

En réponse, la Commission européenne a précisé qu'elle n'avait « pas d'intention d'accélérer ni de ralentir les enquêtes [du règlement sur les services numériques, DSA, face aux réseaux sociaux] », ajoutant que ces enquêtes étaient » menées en ce moment par les équipes responsables. Il faut respecter cette procédure, comme on l'a déjà dit plusieurs fois. »

La question des algorithmes, un sujet récurrent

Ainsi que le recommandaient les rapporteures de la commission des affaires européennes dans le rapport d'information n° 274 (2021-2022) précité, recommandation reprise dans rapport de la commission d'enquête sénatoriale n° 831 (2022-2023) *La tactique TikTok : opacité, addiction et ombres chinoises*, il serait primordial de s'assurer de la légalité et de la sécurité des algorithmes d'ordonnancement des contenus, de modération et d'adressage de la publicité utilisés par les plateformes en ligne en mettant en place, au niveau européen, des normes minimales en matière d'éthique et de respect des droits fondamentaux, obligatoires pour tous les algorithmes, dès leur création (sécurité et légalité par construction ou *safety and legacy by design*). La responsabilité des plateformes mettant en œuvre ces algorithmes devrait pouvoir être engagée dans le cas où leurs algorithmes ne respecteraient pas ces normes.

Dans le rapport de la commission d'enquête sénatoriale sur TikTok précité, il est en outre recommandé que des plateformes effectuant de la recommandation algorithmique de contenus soient assimilées à des éditeurs. L'idée d'une responsabilité renforcée des plateformes en ligne sur leurs contenus est défendue de longue date par le Sénat. Leur assimilation au statut d'éditeur de contenus a, par exemple, été préconisée, en mars 2021 par le sénateur Claude Malhuret, puis un an plus tard par la commission des affaires européennes du Sénat à l'occasion de l'examen de la proposition de résolution européenne sur le règlement sur les services numériques[1]. Une réforme du régime de responsabilité semble incontournable au niveau européen : en sélectionnant et en classant les contenus, puis en en déterminant la présentation et en augmentant la visibilité de certains d'entre eux au détriment d'autres, les plateformes, par le biais de leurs algorithmes, jouent bien un rôle actif qui peut s'apparenter à celui d'un éditeur.

[1] *Résolution européenne n° 70 (2021-2022) du 14 janvier 2022 sur la proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques - Digital Services Act - DSA) et modifiant la directive 2000/31/CE, COM(2020) 825 final.*

Auditionné le 12 février 2025 dans le cadre de l'examen de la présente proposition de résolution, l'historien David Colon expliquait qu'il serait plus approprié de parler de médias sociaux que de réseaux sociaux, dans la mesure où ils font plus qu'acheminer l'information : les algorithmes hiérarchisent les contenus à des fins qui ne sont pas neutres. Pour autant, selon lui, l'assimilation à un rôle d'éditeur devait être maniée avec précaution pour que cela ne se traduise ni par une baisse de la liberté d'expression, ni par une instrumentalisation au profit de la censure. Prenant l'exemple de la Chine et de la Russie, David Colon a expliqué qu'au-delà d'un certain seuil d'abonnés, les influenceurs étaient responsables même des commentaires postés sous leurs publications. De quoi faire facilement condamner des opposants en commentant leurs publications. Sous cette réserve importante, David Colon estimait pertinent de reconnaître une responsabilité des plateformes en ligne sur leurs protocoles algorithmiques.

La commission des affaires européennes du Sénat a conscience que les enquêtes menées au titre du DSA, tout comme celles menées au titre du DMA, sont des enquêtes au long cours qu'il convient de soigner, pour éviter toute déconvenue devant les juridictions compétentes. Aucune sanction n'a donc à ce jour été prononcée. Néanmoins, si un délai de douze mois est fixé par le DMA, aucun délai n'est prévu pour le DSA.

Ainsi, les nouvelles mesures d'enquête annoncées le 17 janvier 2025 contre X s'inscrivent dans le cadre d'une procédure existante contre la même plateforme ouverte le 18 décembre 2023. Quant à la nouvelle enquête, elle est prévue pour durer jusqu'à la fin de l'année 2025.

C. LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE, UNE NÉCESSITÉ EN DEVENIR

Pour contrer à moyen-terme la toute-puissance des plateformes extra européennes, l'Europe ne peut pas faire l'économie du développement de plateformes et d'infrastructures numériques européennes, afin d'offrir une alternative aux acteurs actuels. Cela passe également par une volonté politique forte et des mesures visant à privilégier l'usage de logiciels et de plateformes européens.

1. Un appel du Sénat depuis plusieurs années à construire un véritable projet européen de souveraineté numérique

a) Qu'est-ce que la souveraineté numérique européenne ?

En droit, les États membres demeurent les « maîtres des traités » (qui ne peuvent être modifiés sans leur accord unanime). Ils disposent à ce titre de la « compétence de la compétence et d'un droit de retrait qu'ils peuvent exercer de manière unilatérale »[1].

En France, « le principe de toute souveraineté réside essentiellement dans la Nation. Nul corps, nul individu ne peut exercer d'autorité qui n'en émane expressément. »[2]

Néanmoins, comme le rappelle le Conseil d'État dans sa dernière étude annuelle, consacrée au thème de la souveraineté[3], la « souveraineté européenne » est une « notion essentiellement politique qui connaît un succès certain ». Elle renvoie surtout au concept « d'autonomie stratégique »[4], qui trouve son origine dans le domaine militaire. Dans le contexte géopolitique, il s'agit, pour l'Union européenne et ses États membres, d'assurer leur défense, et, plus généralement, de pouvoir faire les choix garantissant la préservation de leurs intérêts vitaux. L'ancien Président du Conseil européen, M. Charles Michel, faisait de cette autonomie, « l'objectif d'une génération »[5].

C'est dans ce cadre que s'inscrit la recherche d'une souveraineté numérique européenne. Celle-ci a été définie par la commission d'enquête du Sénat sur cet enjeu majeur[6], avec deux dimensions :

« - la faculté d'exercer une souveraineté dans l'espace numérique, qui repose sur une capacité autonome d'appréciation, de décision et d'action dans le cyberespace – et qui correspond de fait à la cyberdéfense ;

« - et la capacité de garder ou restaurer la souveraineté de la France sur les outils numériques afin de pouvoir maîtriser nos données, nos réseaux et nos communications électroniques. »

---

[1] *Étude annuelle du Conseil d'État précitée (p 190).*
[2] *Article 3 de la Constitution.*
[3] *« La souveraineté », Étude annuelle 2024.*
[4] *Ce concept a été utilisé pour la première fois en France dans le Livre Blanc sur la défense en 1994.*
[5] *« L'autonomie stratégique européenne est l'objectif de notre génération », discours prononcé le 28 septembre 2020 devant le groupe de réflexion Bruegel (Bruxelles).*
[6] *Rapport n° 7 (2019-2020) de la commission d'enquête du Sénat sur la souveraineté numérique du 1er octobre 2019 (Président : M. Franck Montaugé ; rapporteur : M. Gérard Longuet).*

Des champions français et européens ? Oui !

Le numérique ne peut pas être résumé à un jeu qui se jouerait entre les États-Unis et la Chine, tandis que les États membres seraient réduits au rang de spectateurs. L'Europe, ainsi que la France à titre individuel, ont aussi des entreprises et des initiatives à promouvoir :

– s'agissant des moteurs de recherche, le français Qwant s'est associé avec l'allemand Ecosia pour essayer de développer un index de recherche et sortir ainsi de la dépendance aux grands moteurs américains. Baptisée *European Search Perspective*, cette coentreprise sera détenue à parts égales par les deux sociétés. Le Directeur Général d'*European Search Perspective* résume ainsi sa mission « développer une technologie démocratique et souveraine en Europe au moment même où l'IA Générative va redéfinir profondément l'expérience de la recherche en ligne ». Le moteur de recherche devrait être en ligne au cours de l'année 2025 ;

– en matière d'intelligence artificielle, l'entreprise française Mistral s'est alliée à l'entreprise allemande Helsing, annonçant le 10 février 2025 un partenariat ayant l'ambition de « révolutionner le secteur de la défense ». Les responsables des deux sociétés se déclarent soucieux des enjeux de souveraineté et estiment que « les Européens ont toutes leurs chances à condition de s'engager pleinement et d'être volontaristes ». La collaboration porte sur la création de modèles dits « *vision-language-action* », une forme d'IA qui permet d'interpréter des instructions complexes et d'agir en conséquence. Ce partenariat est la déclinaison européenne de la collaboration entre les groupes américains Anduril, spécialiste des technologies de défense, et OpenAI pour développer des solutions de lutte antidrones ;

– s'agissant du *cloud*, plusieurs plateformes françaises sont présentes sur le marché, notamment du *cloud* dit de confiance, c'est-à-dire respectueux des exigences strictes en matière de sécurité, de confidentialité et de protection juridique, ainsi que des législations française et européenne : NumSpot, OVHCloud, Scaleway ou encore Cloud Temple. Rappelons que la sécurisation des données sensibles est un enjeu clé, que les systèmes d'IA et de *cloud* sont interconnectés et qu'il n'y a pas d'IA de confiance sans *cloud* de confiance ;

– dans le domaine des technologies quantiques, les acteurs européens du secteur quantique ont publié en 2016 un « manifeste quantique », ce qui a conduit, en 2018, au lancement de l'initiative collaborative de recherche et d'innovation : l'initiative phare sur les technologies quantiques. Aujourd'hui, l'entreprise commune européenne pour le calcul à haute performance (EuroHPC) est une initiative conjointe de l'Union européenne, des pays européens et des partenaires privés, dont l'objectif est de développer un écosystème de supercalcul de classe mondiale en Europe. Huit supercalculateurs d'EuroHPC fonctionnent (dont deux qui se classent dans les dix premiers au monde selon le classement des 500 systèmes informatiques commerciaux les plus puissants connus[1]), d'autres sites d'hébergement devraient s'y ajouter. Côté français, plusieurs acteurs ont émergé ces dernières années, comme Pasqal, Alice&Bob, C12 ou Quobly. En outre, Quandela, leader français du calcul quantique photonique, a reçu fin janvier 2025 la visite de Benjamin Haddad, ministre délégué chargé de l'Europe. Ce dernier a ainsi indiqué « [a]vec ses solutions de calcul

[1] *https://www.top500.org/*

de pointe, Quandela place la France et l'Europe à l'avant-garde des technologies stratégiques. Les talents sont là. Le soutien à l'innovation est au cœur de notre autonomie stratégique. Investissement, simplification, union des marchés de capitaux : donnons les moyens à nos pépites européennes de conquérir le monde. »

La souveraineté numérique de la France et de l'Union européenne est donc toujours à établir. Elle suppose avant tout un changement d'état d'esprit des responsables publics européens et une détermination politique sans faille en particulier pour protéger les données des citoyens des États membres.

b) Prévenir tout risque de remplacement des États par les entreprises du numérique dans les missions régaliennes

En 2013, Eric Schmidt, alors patron de Google, estimait que les États étaient désormais trop lents et trop inefficaces pour faire face aux mutations technologiques en cours[1].

Il en résulte, de la part des très grandes plateformes en ligne, une tentation d'autonomisation, alors qu'elles soutiennent ou remplacent de plus en plus les États dans leurs missions régaliennes.

En écho à cette affirmation, lors de son audition devant le Sénat[2], Jean-Marie Cavada, ancien député européen et président de l'institut des droits fondamentaux numériques (iDFRights), soulignait que « les grands monopoles technologiques et l'intelligence artificielle générative sont aujourd'hui en mesure de tenir tête aux États et de ne plus leur obéir ».

Lors de la même audition, les propos de Bernard Benhamou, secrétaire général de l'Institut de la Souveraineté Numérique, étaient également teintés d'inquiétude : « les données sont un outil de contrôle des populations » et les réseaux sociaux sont des « mastodontes » qui « réunissent tellement d'informations, en savent tellement sur nous qu'ils peuvent nous manipuler d'une manière qui était totalement impensable dans les temps passés ».

Les États membres sont désormais souvent dépendants des solutions technologiques étrangères.

Peut être mentionné à cet égard le projet français de constitution d'une base nationale des données de santé (défini par l'anglicisme « *Health Data Hub* ») initié en 2019 et inscrit dans le cadre d'un projet européen plus vaste appelé EMC2. Ce projet tend à « accueillir les données [anonymisées] de 300 000 à 500 000 patients de différents hôpitaux par an et les comparer avec leurs données issues du système national des données de santé, géré par

[1] *« The new digital Age : transforming Nations, business, and our lives", Eric Schmidt et Jared Cohen, edition John Murray, 2014.*

[2] *Audition conjointe avec M. Bernard Benhamou, secrétaire général de l'Institut de la Souveraineté numérique, devant la commission des affaires européennes du Sénat, sur leur rapport « Intelligence artificielle : enjeux et perspectives pour les droits humains en Europe ».*

l'Assurance-maladie (et à terme par le *Health Data Hub*), pour permettre la réalisation de recherches, d'études et d'évaluations dans le domaine de la santé ».

Or, dès l'origine, la firme américaine Microsoft a été choisie pour mettre en place la plateforme technologique du projet. Aucun appel d'offres spécifiques n'a été publié, aucune entreprise française ou européenne n'ont été approchées, ce qu'elles ont déploré. Ainsi, ce choix a été attaqué, en vain, devant le Conseil d'État par des entreprises européennes et par des ONG du numérique qui soulignaient que Microsoft est soumise aux lois américaines permettant aux agences de renseignements américaines d'avoir accès aux données personnelles stockées. La CNIL, contrainte et forcée, a également validé ce projet. Sa décision a alors été justifiée par le besoin d'une mise en place rapide et par les insuffisances des réponses industrielles françaises et européennes. Dans l'entrefaite, le premier ministre Jean Castex s'était engagé à relancer le marché après appel d'offres.

Par ailleurs, les GAFAM sont régulièrement accusés de contourner les législations fiscales nationales pour éviter de payer l'impôt[1]. Comme le rappelait la commission d'enquête du Sénat sur la souveraineté numérique, ces entreprises bénéficient du « concours de pays partenaires. À titre d'exemple, à la suite d'une procédure lancée en 2016 par la Commission européenne pour qualifier d'aide d'État le régime fiscal spécifique accordé par l'Irlande à Apple », la Cour de justice de l'Union européenne[2] a confirmé que les avantages fiscaux accordés par l'Irlande à Apple constituaient bien une aide d'État illégale. En conséquence, l'Irlande est tenue de récupérer les 13 milliards d'euros auprès d'Apple.

Plus généralement, les entreprises numériques « tirent […] profit des caractéristiques propres au secteur du numérique : (i) le peu d'accroches stables pour la fiscalité ; (ii) une part importante d'actifs incorporels, ce qui ne rend que plus ardue leur valorisation comptable ; (iii) la difficulté à localiser la valeur ajoutée créée dans l'économie numérique, du fait du découplage que ces entreprises peuvent facilement opérer entre lieu d'établissement et lieu de consommation […] ; (iv) la prévalence dans cette économie du modèle de l'intermédiaire, qui capte la marge au détriment des acteurs traditionnels »[3].

Face aux pratiques non coopératives des grandes plateformes numériques, les autorités françaises avaient choisi de « faire un exemple » en poursuivant la firme Google, en 2015, pour « fraude fiscale aggravée et délit de blanchiment de fraude fiscale aggravée ». Cette procédure avait conduit

---

[1] *Rapport d'information « L'Union européenne, colonie du monde numérique » et rapport de la commission d'enquête du Sénat sur la souveraineté numérique, p. 81-82.*

[2] *CJUE, Commission européenne contre République d'Irlande et Apple, affaire C-465/20P, 10 septembre 2024.*

[3] *Rapport précité de la commission d'enquête du Sénat sur la souveraineté numérique, p. 81-82.*

l'entreprise à conclure une convention judiciaire d'intérêt public[1] avec le Parquet national financier et un accord avec l'administration fiscale française pour un montant global de près d'un milliard d'euros.

Mais une telle démarche ne s'attaque qu'aux conséquences de ce défi fiscal lancé par les grandes entreprises du numériques aux États membres. Voilà pourquoi la France a défendu l'idée d'une taxation européenne du secteur numérique. Malheureusement, dans un domaine où les modifications doivent être adoptées à l'unanimité, aucun consensus n'a pu être trouvé et la France s'est donc résignée à mettre en place une taxe nationale[2] tout en précisant qu'elle serait supprimée dès lors qu'un accord international sur cette question entrerait en vigueur[3].

Enfin, les grands acteurs du numérique viennent parfois contester le monopole de l'État dans ses missions régaliennes : « [l]e fait le plus marquant réside dans l'appropriation par les grandes plateformes numériques non européennes des attributs de la souveraineté : un territoire transnational qui est celui de leur marché et du lieu d'édiction de normes, une population d'internautes, une langue, des monnaies virtuelles, une fiscalité optimisée, un pouvoir d'édiction de normes et de régulation. […] Il y a donc concurrence avec les États ou l'Union européenne. »[4]

Un exemple flagrant est celui des projets de monnaie privées numériques.

Tout d'abord, plusieurs acteurs du numérique ont mis en place des solutions de paiement mobiles (ApplePay, GooglePay, etc.), qui sont les seules offres de paiement mobile identiques partout en Europe.

Par ailleurs, le projet Libra/Diem de Meta, qui visait à développer une offre de paiement privée autonome des banques et des systèmes de paiement classiques, a démontré que les très grandes plateformes pouvaient menacer le monopole traditionnel des États dans l'émission de la monnaie. En effet, Libra

---

[1] Ces procédures ont été introduites en droit français par la loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude à l'initiative du Sénat.

[2] Loi n° 2019-759 du 24 juillet 2019 portant création d'une taxe sur les services numériques.

[3] Cet impôt, dont le taux d'imposition est de 3 % du chiffre d'affaires français des entreprises concernées, vise les sociétés qui proposent de la publicité en ligne, de la vente de biens ou des activités de plateforme d'intermédiation et qui réalisent plus de 750 millions d'euros de chiffre d'affaires dans le monde, dont 25 millions sur le sol français (Articles 453-45 à 453-85 du code de l'imposition sur les biens et services). En réponse, le président américain Donald Trump avait d'abord annoncé avoir confié au bureau du représentant américain pour le commerce le soin de mener une enquête sur les effets de la TSN française et sur l'éventuelle discrimination subie par les entreprises américaines, puis menacé les autorités françaises de représailles économiques et douanières sur les produits de luxe (au titre de la « section 301 du « Trade Act » (1974), le bureau du représentant des États-Unis pour les questions commerciales internationales est autorisé à prendre des mesures d'imposition de droits supplémentaires, de restrictions à l'importation etc…). La taxe a été maintenu et représente aujourd'hui une source de revenus importante et croissante pour l'État français (622 millions d'euros en 2022 ; 700 millions d'euros en 2023 ; 800 millions d'euros en 2024).

[4] « Souveraineté et numérique : maîtriser notre destin », Mme Annie Blandin-Obernesser, professeur de droit MIT Atlantique-Institut Mines-Télécom ; The Conversation, 10 novembre 2021.

aurait pu être accessible aux milliards d'utilisateurs du réseau social Facebook et de WhatsApp.

Comme le soulignait la sénatrice Florence Blatrix Contat, ces projets « font peser de nombreuses menaces sur la stabilité du système financier, sur la protection des données ou encore en matière de blanchiment »[1]. Ils doivent donc inciter les États membres de l'Union européenne à poursuivre leurs réflexions sur l'institution d'un euro numérique[2].

Les GAFAM et autres sociétés du numérique investissent aujourd'hui d'autres champs régaliens tels que le renseignement et la défense. En introduisant des possibilités de traitement massif des données (*big data*) et des solutions d'intelligence artificielle pour aider à la prise de décision, ces entreprises peuvent se rendre indispensables aux États, au risque de substituer leurs propres objectifs aux choix démocratiques.

Ainsi, la société américaine Palantir, fondée par M. Peter Thiel et financée à l'origine par le fonds d'investissement de la CIA (In-Q-Tel), a passé un contrat avec la direction générale de la sécurité intérieure (DGSI) française[3].

Autre exemple mis en valeur par une récente « mission flash » de l'Assemblée nationale sur les défis de la cyberdéfense en janvier 2024[4] : les rapporteurs ont considéré que le ministère des Armées était « aujourd'hui piégé » par sa dépendance à l'égard de certaines entreprises étrangères compétentes dans le numérique et par son utilisation du système d'exploitation Windows. Ils ont demandé en conséquence l'élaboration d'une « feuille de route » visant à « réduire l'empreinte » de ces entreprises au sein des armées, notamment en explorant le recours au logiciel libre et en développant un hébergement informatique en nuage (*cloud*) souverain.

c) Une politique européenne qui a été jusqu'à présent trop frileuse, mais des annonces récentes qui laissent supposer un changement de cap

Si la commission des affaires européennes du Sénat a souvent déploré le manque d'ambition européenne pour le numérique, deux annonces majeures semblent aller dans le sens d'une prise de conscience et d'une volonté d'inverser cet état de dépendance. À cela, il ne faut pas oublier d'adjoindre une vraie politique en faveur du *cloud* souverain.

---

[1] *Compte rendu de la réunion de la commission des affaires européennes du Sénat du 26 juin 2024.*

[2] *Rapport d'information n° 708 (2023-2024) sur l'euro numérique de M. Pascal Allizard et de Mme Florence Blatrix Contat au nom de la commission des affaires européennes du Sénat, 26 juin 2024.*

[3] *Cet exemple est développé dans l'article précité de M. Bernard Benhamou, « Souveraineté numérique : quelles stratégies pour la France et l'Europe ? », 27 octobre 2020.*

[4] *Les rapporteurs de cette mission étaient les députés Anne Le Hénanff et Frédéric Mathieu.*

(1) Le Sénat plaide depuis 2013 pour une véritable ambition numérique européenne

Pour ne plus être une « colonie du monde numérique », la commission des affaires européennes du Sénat appelait, en 2013, à sortir du « défaut de vision politique de long terme » qui caractérisait alors le monde numérique en Europe, relevant que « le défi numérique invite à dépasser les cloisonnements administratifs et à mobiliser transversalement les énergies au service d'une ambition partagée : restaurer la souveraineté européenne dans le monde numérique pour y défendre les valeurs de l'Union européenne ».

En 2014, la mission commune d'information sur la gouvernance mondiale de l'Internet avait appelé à construire une stratégie industrielle européenne pour maîtriser les données et porter ses valeurs, soulignant que « la politique européenne en matière d'industrie du net a consisté, jusqu'à aujourd'hui, à créer et mettre en place un écosystème qui soit acceptable pour l'ensemble de ses acteurs. À cette démarche, qui doit être poursuivie, doit s'en ajouter une nouvelle, consistant à soutenir nos entreprises sur les marchés extérieurs, comme le font nos principaux compétiteurs internationaux (États-Unis, Japon et Chine, notamment). […] La première priorité pour l'Europe et pour la France doit être de capitaliser sur les domaines dans lesquels elles occupent une place de leader. Ces champs d'activité sont bien plus nombreux et importants, dans le secteur du numérique, que ce que l'on peut croire. »[1] **Ses constats, il y a dix ans, étaient très similaires à ceux que nous pouvons faire aujourd'hu**i. Ses recommandations sont donc encore pleinement d'actualité : reprise en main du « destin numérique » de l'Union, attention portée aux sujets du *cloud* et des données, ambition industrielle en matière numérique, etc.

Quant aux rapporteures de la commission des affaires européennes, elles appelaient, en juin 2022, dans la proposition de résolution européenne n° 664 (2021-2022) sur le programme d'action numérique de l'Union européenne à l'horizon 2030, « à la mise en œuvre, à moyen et long terme, d'une stratégie numérique globale, cohérente et offensive, incluant un soutien affirmé au développement des compétences numériques, mais aussi à la recherche et à l'innovation, accompagné d'une véritable politique industrielle, dans une dynamique de mise en place d'écosystèmes industriels locaux » et transversaux ainsi qu'à l'octroi de moyens à la hauteur des objectifs affichés au service de l'ambition numérique de l'Union.

En 2025, ces constats, et surtout ces appels, sont plus que jamais d'actualité : l'Union européenne a besoin d'une politique volontariste, ambitieuse, concrète et d'acteurs européens.

Les annonces d'Ursula von der Leyen sur la boussole de compétitivité et la refonte de la directive marchés publics laissent entrevoir une prise de conscience des autorités européennes, d'une part, une volonté de mettre en

[1] *https://www.senat.fr/notice-rapport/2013/r13-696-1-notice.html*

place une préférence européenne, d'autre part. Cette ambition ne peut faire l'économie de leviers forts et concrets à son appui.

(2) L'enjeu de la localisation des données sensibles

Si l'Union européenne veut avoir les moyens de ses ambitions dans le domaine numérique, elle ne peut faire l'impasse sur la question de la maîtrise des données sensibles. Ces données sensibles concernent la santé, la finance, les jumeaux numériques[1], et ni les États, ni les entreprises ne peuvent se permettre une protection des données qui ne serait pas optimale.

Le projet de créer un *cloud* européen souverain est la conséquence de l'absence de protection suffisante des données confiées à des solutions fournies par des prestataires de pays tiers. Les lois sécuritaires adoptées par les États-Unis, notamment le « *FISA Act* », dotent en effet les autorités américaines d'importants instruments d'interception de données de toutes sortes détenues par des entreprises privées et leur permettant de faire avancer leurs investigations.

Partant de ce constat, la solution d'un *cloud* souverain européen semble prometteuse pour sécuriser le développement de l'industrie et la protection des données. Elle consiste en effet à exiger, outre l'implantation sur le territoire européen du centre de données fournissant le service de *cloud*, que toutes les briques le composant, matérielles comme logicielles, soient entièrement européennes. Ainsi, aucun composant de pays tiers n'entrant dans la fabrication du système, cela le rendrait hermétique d'une part à toute infiltration du système, d'autre part à toute demande de communication de données en vertu d'une loi extraterritoriale.

Pour répondre aux enjeux d'indépendance et de sécurité, il est donc primordial de travailler sur l'ensemble de la chaîne avec des acteurs souverains, afin d'éviter aux données d'être exposées à des lois extraterritoriales.

Il existe des solutions pour un *cloud* souverain dans des États membres de l'Union européenne, à l'instar de la France, qui ont besoin de recommandations explicites d'utilisation de leurs plateformes. Les infrastructures existent. Certes, c'est un marché de niche dans le monde des données, mais c'est un élément dont le contrôle est essentiel.

(3) Les orientations politiques 2024-2029 de la Commission

Les orientations politiques pour les cinq années à venir présentées par Ursula von der Leyen le 18 juillet 2024 à Strasbourg comportent l'objectif de stimuler la productivité par la diffusion des technologies numériques. Ainsi que l'explique la présidente de la Commission européenne, la compétitivité européenne est entravée, et « [c]eci s'explique principalement par la diffusion

[1] *Un jumeau numérique est une réplique virtuelle qui permet de simuler, d'analyser, de surveiller en temps réel le fonctionnement d'un objet, d'un processus ou d'un système physique.*

insuffisante des technologies numériques, qui a une incidence sur notre capacité à utiliser les technologies pour créer de nouveaux services et modèles commerciaux […]. La réalisation de nos objectifs numériques et la mise en place d'un véritable marché unique numérique changeraient la donne pour notre productivité et notre compétitivité. Nous augmenterons nos investissements dans la prochaine vague de technologies de pointe… »

S'agissant de l'accès aux données, Ursula von der Leyen annonçait dans ses orientations qu'il s'agissait « non seulement [d']un moteur majeur de la compétitivité, puisqu'il représente près de 4 % du PIB de l'UE, mais il est également essentiel pour la productivité et les innovations sociétales, de la médecine personnalisée aux économies d'énergie. […] Tout en garantissant des normes élevées en matière de protection des données, nous soutiendrons les entreprises en améliorant le libre accès aux données, notamment pour aider les PME à remplir leurs obligations de déclaration. L'Europe a besoin d'une révolution dans le domaine des données. »

En outre, une annonce d'ampleur est celle concernant la révision de la directive sur les marchés publics, afin de pouvoir donner la préférence aux produits européens dans les marchés publics pour certains secteurs stratégiques. **La commission des affaires européennes appelle à ce que le secteur numérique entre dans le champ des secteurs stratégiques concernés et que la procédure de révision débute dans les plus brefs délais**.

La Commission européenne souligne enfin que ces orientations comportent aussi un axe relatif à la mise en œuvre et à l'application de la législation dans le domaine du numérique, Mme von der Leyen annonçant un renforcement et une intensification des contrôles au cours du mandat 2024-2029.

(4) La boussole pour la compétitivité, première traduction d'ampleur de ces orientations politiques

La présidente de la Commission européenne et le commissaire français Stéphane Séjouné ont présenté le 29 janvier 2025 une initiative pour regagner en compétitivité, appelée « boussole pour la compétitivité ».

Le premier pilier de cette boussole numérique vise à stimuler la productivité par l'innovation. Ainsi, l'« Europe doit être à la pointe de l'innovation dans les secteurs technologiques qui compteront dans l'économie de demain - tels que l'intelligence artificielle (IA), les semi-conducteurs et les technologies quantiques […] ».

La déclaration rappelle que l'« Europe a ouvert la voie en fournissant un cadre stable et sûr aux entreprises qui développent et exploitent des technologies numériques dans le marché unique, avec des mesures telles que les lois sur les données et la gouvernance des données, la loi sur la cyber-résilience et la loi sur l'IA […]. Les normes européennes ont influencé l'évolution du cadre réglementaire mondial. Il faut maintenant mettre l'accent

sur la mise en valeur de nos talents technologiques et le développement d'une industrie de classe mondiale » reposant sur tout un tissu d'entreprises (petites et moyennes entreprises -PME- et entreprises de taille intermédiaire-ETI) dont on accompagne la montée en puissance.

La boussole pour la compétitivité souligne que l'Europe doit pouvoir tirer parti des gains de productivité de la technologie et qu'elle a besoin des infrastructures informatiques, du cloud et des données nécessaires à la domination de l'IA, d'une part, et conserver une position de *leader* dans les technologies quantiques, en remédiant à la fragmentation réglementaire, en alignant les programmes européens et nationaux et en soutenant les investissements dans les infrastructures paneuropéennes, d'autre part.

« Si nous voulons que l'avenir de l'industrie soit "*made in Europe*", l'Union européenne doit relancer le cycle de l'innovation. » Partant de ce constat, et pour éviter que des entreprises européennes cherchent des financements aux États-Unis puis s'y délocalisent. En matière de « Tech » notamment, la Commission européenne annonce ainsi travailler au déploiement d'un programme d'investissement TechEU pour soutenir l'innovation, renforcer la capacité industrielle de l'Europe et développer les entreprises qui investissent dans des technologies innovantes.

La présentation du paquet « boussole pour la compétitivité » revient également sur la politique de la concurrence comme levier important pour renforcer la compétitivité de l'Europe, arguant que « l'application de la loi sur les marchés numériques ouvrira des écosystèmes fermés et permettra aux entreprises innovantes de proposer de nouveaux services numériques aux clients ». Selon la Commission, « 70 % de la nouvelle valeur créée dans l'économie mondiale au cours des dix prochaines années sera générée par le numérique ».

Enfin, la Commission souligne que pour combler le retard en matière d'innovation, il faudra « investir dans des infrastructures numériques de pointe, notamment des réseaux de fibre optique modernes, des solutions sans fil et satellitaires, investir dans la 6G et les capacités de *cloud computing*. Pourtant, l'Europe est loin d'atteindre ses propres objectifs de la Décennie numérique 2030 en matière de connexions d'infrastructure. Pour corriger le tir, une loi sur les réseaux numériques proposera des solutions pour améliorer les incitations du marché à construire les réseaux numériques du futur. »

La commission des affaires européennes du Sénat souhaite rappeler que l'innovation est la première pierre pour, à terme, changer un marché. Elle se réjouit donc des initiatives qui sont prises en ce sens au niveau européen et veut insister sur le fait qu'il faut non seulement amplifier les budgets mais aussi, et surtout, les refonder avec des mécanismes différents, pour qu'ils ne soient pas uniquement l'occasion pour les grandes structures européennes de s'associer à des PME. Ils doivent en effet permettre à des PME-ETI de monter en puissance.

(5) Un élan qui doit englober toutes les composantes du numérique

La commission des affaires européennes du Sénat souhaite souligner, en cohérence avec son précédent rapport sur la boussole numérique, que le champ numérique comporte d'une part les infrastructures (6G, semi-conducteurs, *edge computing* , *cloud*, etc.), d'autre part les technologies telles que les technologies critiques et émergentes (intelligence artificielle, calcul quantique), mais aussi la maîtrise d'algorithmes sensibles, les compétences et la capacité de faire pénétrer et de tirer le meilleur parti des outils numériques dans tous les aspects de l'économie et de la société. C'est un tout, et toute stratégie doit en tenir compte sous peine d'atteindre rapidement ses limites.

À cet égard, tant les annonces sur la boussole pour la compétitivité que le programme de travail de la Commission sont rassurants, en ce qu'ils semblent prendre en compte tous les champs du numérique. Sont ainsi mentionnés :

– **un futur texte européen sur les réseaux numériques**, outil visant d'une part à tendre vers les objectifs fixés par la boussole numérique (Décennie numérique 2023)[1] et, d'autre part, à essayer de combler les retards européens en matière de réseaux de fibre optique modernes, de solutions sans fil et satellitaires, d'investir dans la 6G et les capacités de *cloud computing*. Le programme de travail, quant à lui, annonce une augmentation des investissements dans les supercalculateurs, les semi-conducteurs, l'Internet des objets, la génomique, l'informatique quantique et les technologies spatiales. Rappelons qu'en septembre dernier, l'Union européenne a annoncé investir 65 millions d'euros dans les puces quantiques *via* l'entreprise commune « Semi-conducteurs », qui a lancé des appels à propositions pour soutenir des initiatives de recherche et d'innovation dans le domaine des semi-conducteurs ;

Vocabulaire numérique : de quoi parle-t-on ?

Si le monde numérique entoure désormais la plupart des actions du quotidien et que son omniprésence dans les débats contemporains n'est plus à démontrer, il n'est pas toujours aisé d'appréhender le champ recouvert par chacun des mots du vocabulaire numérique.

– **intelligence artificielle** : la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité. L'IA regroupe les approches d'apprentissage automatique (la machine a la capacité d'» apprendre » à partir de données à sa disposition), les approches fondées sur la logique et la connaissance, et les approches statistiques. L'IA peut-être générative, c'est-à-dire qu'elle est capable de générer des images, des vidéos ou de la musique en reproduisant la capacité cognitive humaine de manière globale ;

[1] *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr*

– **calcul quantique** : l'utilisation des propriétés quantiques (comme la superposition) pour effectuer massivement des opérations sur des données à l'aide d'un ordinateur quantique, permettant ainsi de dépasser les capacités offertes par des ordinateurs classiques. Le calcul quantique s'opère en bits quantiques (qubits) ;

– **supercalculateur :** très grand ordinateur, réunissant plusieurs dizaines de milliers de processeurs, et capable de réaliser un très grand nombre d'opérations de calcul ou de traitement de données simultanées

– **semi-conducteur** : matériau dont la conductivité électrique est intermédiaire entre celle des métaux et celle des isolants. Les semi-conducteurs entrent dans la fabrication des appareils du quotidien et sont essentiels au développement des technologies, c'est pourquoi ils sont devenus stratégiques et un véritable enjeu de souveraineté ;

– **centre de données**, ou *data center* : emplacement physique abritant des infrastructures informatiques et de télécommunications destinées à stocker, à traiter ou à distribuer des données de façon sécurisée ;

– **informatique en nuage**, ou *cloud computing* : utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans une infrastructure informatique (*cloud*) composée de nombreux serveurs distants interconnectés ;

– **algorithmes** : ensemble de règles opératoires permettant d'obtenir un résultat. Sur les réseaux sociaux, un algorithme désigne l'ensemble de données et de règles qui déterminent le contenu à afficher en priorité. Certains algorithmes sont dits « auto-apprenants » car leur comportement évolue en fonction des données qui leur ont été fournies ;

– ***open source*** : dont le code source est libre d'accès, réutilisable et modifiable.

– **la prise en compte de l'intelligence artificielle (IA) comme composante incontournable du monde numérique**. L'adoption en 2024 du règlement européen sur l'intelligence artificielle[1] a été un premier pas européen, certes incomplet, mais qui a le mérite de se saisir de cette donnée aux répercussions nombreuses. En complément à cette loi, le programme de travail de la Commission pour 2025 annonce trois axes concernant l'intelligence artificielle : (i) garantir l'accès à de nouvelles capacités de supercalcul adaptées au secteur de l'IA et à ses jeunes entreprises, au moyen d'une initiative sur les fabriques d'IA, (ii) encourager de nouvelles utilisations industrielles de l'IA et améliorer les services publics grâce à une stratégie pour l'application de l'IA et (iii) mettre en commun les ressources européennes grâce au Conseil européen de la recherche sur l'IA.

[1] *Règlement (UE) 2024/1689 établissant des règles harmonisées en matière d'intelligence artificielle.*

L'intelligence artificielle, enjeu de pouvoir de l'année 2025 ?

À peine investi président des États-Unis, Donald Trump a annoncé le lancement du projet *Stargate*, doté de 500 milliards de dollars (environ 485 millions d'euros), qui devrait permettre, selon le président américain, de « bâtir les infrastructures physiques et virtuelles pour porter la prochaine génération d'IA » et créer « plus de 100 000 emplois » aux États-Unis. Le projet rassemble OpenAI (à l'origine de ChatGPT), la société d'investissement japonaise SoftBank et le géant du numérique Oracle. Pour ce faire, plusieurs centres de données sont déjà en cours de construction au Texas, d'autres suivront sur le territoire américain, les lieux exacts restant encore à définir. Ainsi le vice-président américain J. D. Vance a-t-il déclaré, lors de son discours au sommet pour l'action de l'IA, que les États-Unis feraient tous les efforts pour encourager les politiques pro-croissance », ajoutant que « [l]es États-Unis sont les leaders dans l'IA et notre administration entend qu'ils le restent ».

En France, à la veille de l'ouverture du sommet mondial pour l'action de l'IA, Emmanuel Macron a annoncé **un investissement de 109 milliards d'euros** dans les prochaines années pour l'IA en France. Les investissements proviendront notamment les Émirats arabes unis (qui souhaitent bâtir un grand *data center* en France), mais aussi de grands fonds d'investissement américains et canadiens, et de grandes entreprises françaises. Arguant que la France a des talents, mais que « nous sommes en retard sur les data centers », il en déduit que « la première des batailles qu'on doit faire en tant qu'Européens, c'est investir, investir, investir » tout en régulant en parallèle. Le projet développé avec les Émirats Arabes Unis serait donc d'ouvrir un grand *data center* en France, qui serait doté d'une capacité énergétique d'un gigawatt et qui ferait partie d'un campus IA. Ce campus serait développé par un consortium de champions franco-émiratis.

En outre, la France s'est associée à l'Allemagne, la Finlande, la Slovénie, la Suisse, le Maroc, le Kenya, le Nigéria et le Chili pour créer la **Fondation sur l'IA, baptisée *Current AI***, qui vise à financer le développement d'outils et bases de données d'IA open source. Des grandes entreprises sont également associées au projet, à l'instar Google et Salesforce, ainsi que des entreprises du monde de l'IA *open source* comme Mistral, Hugging Face et Pleias. En outre, le projet rassemble aussi des fondations philanthropiques telles que Ford, MacArthur et McGovern. Un total de 400 millions d'euros a été levé pour le moment grâce aux premiers membres, pour un objectif de 2,5 milliards d'ici cinq ans.

Au niveau européen, rappelons que l'initiative sur les fabriques d'IA, intégrée dans la **stratégie « continent de l'IA »** figure dans les priorités de la Commission 2024-2029. La présentation de cette stratégie est prévue en ce premier semestre 2025, avec l'objectif, s'agissant des fabriques d'IA, de garantir l'accès à de nouvelles capacités de supercalcul adaptées au secteur de l'IA et à ses jeunes entreprises. À cet égard, la Commissaire, Henna Virkkunen, vice-présidente exécutive chargée de la souveraineté technologique, de la sécurité et de la démocratie, a déclaré le 10 février 2025 que le supercalculateur français Alice-Recoque était un « candidat solide » pour intégrer la stratégie « d'usines à IA ». L'objectif est de combler le retard sur les capacités de calcul en Europe, *via* par exemple la création de giga-usines permettant à terme de multiplier par cinq la puissance de calcul en Europe.

Consciente qu'elle doit prendre le virage de l'intelligence artificielle, l'Union européenne a annoncé le 11 février 2025, par la voix d'Ursula von der Leyen, vouloir **mobiliser 200 milliards d'euros** pour des investissements. Annoncé comme « le plus grand partenariat public-privé dans le monde pour le développement d'une IA fiable dans l'intelligence artificielle en Europe », il regroupera plus de 60 entreprises (telles que Airbus, L'Oréal, Mercedes, Siemens, Spotify ou encore Mistral AI) sous le nom « EU AI Champions Initiative ». L'Union européenne devrait s'engager sur un montant de 50 milliards d'euros, en plus des 150 milliards promis par les grands groupes qui participent à l'alliance. Sur ce total, 20 milliards devraient être investis dans les « *gigafactories* ». La présidente de la Commission européenne estime qu'en matière d'IA, « le *leadership* mondial est toujours à saisir ».

*d) L'*open source*, solution miracle ?*

Lors de son audition, le 11 février 2025, Patrick Laurens-Frings, directeur général par intérim de NumSpot, société fondée par quatre actionnaires français (Banque des territoires ; Bouygues télécom ; Dassault systèmes et La Poste) et qui ambitionne de devenir le leader européen du cloud de confiance, a présenté *l'open source* comme facteur de performance, « communauté de milliers de personnes indépendantes de toute ingérence étrangère ».

En parallèle, les annonces récentes lors du sommet pour l'action de l'IA ont montré un soutien de la France, mais aussi d'autres pays et d'entreprises, pour le développement des IA *open source*. « La France souhaite aboutir dans le cadre du Sommet à la création d'une nouvelle plateforme mondiale qui servira d'incubateur pour mettre l'intelligence artificielle davantage au service de l'intérêt général. Cette initiative favorisera la mise en place d'une infrastructure commune et ouverte, de l'accès aux données et à la puissance de calcul jusqu'au développement de modèles à faible consommation d'énergie adaptés à des besoins spécifiques.

Il s'agit d'un effort collectif élaboré à la suite de consultations avec des dizaines de pays, des centaines d'organisations de la société civile et des entreprises de tous les continents, et qui vise à développer des biens communs de l'IA dans les domaines des données, des modèles ouverts, de la participation citoyenne, réutilisables par tous les États et organisations qui souhaiteraient s'en saisir, en réponse aux aspirations partagées par les acteurs consultés. »[1]

Plusieurs initiatives vont dans ce sens :

– Pleias, une start-up française, a développé trois modèles de langage multilingue qui ont été entraînés sur des données libres de droits, respectant non seulement le droit d'auteur, mais aussi les données personnelles ;

[1] *https://www.elysee.fr/sommet-pour-l-action-sur-l-ia/ia-au-service-de-l-interet-public*

– Linagora, éditeur de solutions Open Source, qui a pour objectif d'» [i]nventer et développer des logiciels libres et open source éthiques », est aussi un acteur de la communauté et du consortium OpenLLM France, qui vise à « développer un LLM français, souverain, réellement *Open Source* reposant sur des corpus de données d'apprentissage publics et ouverts, des algorithmes documentés pour en assurer l'explicabilité et proposant une licence d'utilisation libre, non restrictive » ;

– À un niveau plus global, le projet « *Current AI* », annoncé lors du sommet pour l'action de l'IA, porte un « objectif assez offensif de diversification du marché de l'IA », et donc de création de concurrence.

De leur côté, Google, OpenAI, Discord, Roblox, Bluesky, Hugging Face, Microsoft ou Mozilla ont annoncé s'allier pour bâtir Roost[1], une fondation, dotée de 27 millions de dollars, dont l'objectif est de bâtir des outils de modération en open source dont pourront se servir gratuitement tous les éditeurs de services en ligne. Le fonctionnement serait le suivant : une entreprise pourra se servir des connaissances mises en commun, en s'engageant à améliorer en retour ces connaissances. Le principe est donc de fournir les outils pour que les entreprises puissent ensuite bâtir leur propre système de modération.

L'exemple de la plateforme conversationnelle LUCIE

La plateforme conversationnelle française LUCIE.chat, est développée notamment par OpenLLM France avec l'objectif suivant : fournir une alternative ouverte, éthique et souveraine, qui ne dépend pas des grandes entreprises technologiques étrangères du fait du recours à l'*open source*. Enfin, affirmant garantir un accès sans restriction aux modèles et aux données, les dirigeants de LUCIE souhaitent permettre aux chercheurs, aux industriels et aux institutions publiques de développer leurs propres applications en toute indépendance.

Lors de son lancement, LUCIE a fait l'objet d'un détournement de son usage et d'un emballement médiatique malveillant associé. Elle a donc été rapidement, mais temporairement, fermée. Néanmoins, l'intérêt du public pour une telle plateforme a été confirmé par le fait qu'au 30 janvier 2025, le modèle a été téléchargé plus de 4 000 fois (pour une utilisation locale) et que les données d'entrainement ont fait l'objet de 65 000 téléchargements.

[1] *Robust Open Online Safety Tool*

II. LA PROPOSITION DE RÉSOLUTION N° 351 DÉPOSÉE PAR DIDIER MARIE ET SES COLLÈGUES ET LA POSITION DE LA COMMISSION DES AFFAIRES EUROPÉENNES

A. LE CONTENU DE LA PROPOSITION DE RÉSOLUTION N° 351 (2024-2025) DÉPOSÉE PAR LE GROUPE SOCIALISTE, ÉCOLOGISTE ET RÉPUBLICAIN DU SÉNAT

Déposée le 18 février 2025, cette proposition de résolution comporte trois volets :

– un appel à la mise en œuvre sans trembler des textes européens ;

– un appel à la souveraineté européenne dans le domaine numérique ;

– un appel au renforcement de l'arsenal juridique européen contre les ingérences étrangères, la désinformation et les atteintes à la démocratie ou aux valeurs.

1. Un appel à la mise en œuvre sans trembler des textes européens

À ce titre, la proposition de résolution :

- salue l'annonce de la Commission européenne sur l'approfondissement de son enquête sur X ;

- condamne les mesures mises en place par certains réseaux sociaux de réduction de la modération et, à cet égard, demande à la Commission de mettre en œuvre ses prérogatives au titre du DSA concernant la lutte contre la manipulation de l'information ;

– enjoint à la Commission européenne à réitérer ses engagements de (i) mise en œuvre des textes réglementaires, y compris jusqu'aux sanctions, et (ii) renforcement et intensification des contrôles de l'application des textes DMA et DSA ;

- demande l'application des dispositions de l'article 9 du RGPD, qui interdisent les traitements portant sur les données personnelles sensibles[1], sauf exceptions limitées[2], afin de désactiver les algorithmes de

[1] *L'article 9 liste ces données à caractère personnels sensibles : ce sont les données à caractère personnel révélant « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement de données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».*

[2] *Les exceptions, listées également à l'article 9 du RGPD sont les suivantes ; consentement explicite d'une personne sauf si le droit de l'Union européenne ou des États membres empêche la levée de l'interdiction ; traitement nécessaire à l'exécution des obligations ou à l'exercice des droits du responsable de traitement ou de la personne concernée en matière de droit du travail ou de sécurité sociale ou à la sauvegarde des intérêts vitaux de cette personne ; traitement effectué une fondation, une association ou toute autre organisation à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale concernant exclusivement ses membres ; traitement concernant*

recommandation par défaut et obliger les plateformes en ligne à avertir soigneusement leurs utilisateurs et à leur demander explicitement leur consentement.

2. Un appel au renforcement de l'arsenal juridique européen

La proposition de résolution européenne appelle à un renforcement de l'arsenal juridique européen, qui pourrait se traduire notamment par l'établissement de règles d'équilibre similaires à celles qui existent pour les médias traditionnels, notamment en période électorale mais aussi par l'adoption rapide du « bouclier démocratique européen » annoncé Ursula von der Leyen pour lutter contre la manipulation de l'information et l'ingérence étrangères en ligne.

3. Un appel à la souveraineté européenne dans le domaine numérique

La proposition de résolution européenne comprend un dernier axe visant le renforcement d'une souveraineté numérique européenne. Il est proposé que ce renforcement passe notamment par :

– l'émergence d'acteurs européens du numérique et le soutien à des *clouds* européens souverains ;

– la mise en place d'une politique industrielle volontariste ;

– la mise en place au niveau européen de normes minimales en matière d'éthique et de respect des droits fondamentaux, obligatoires pour tous les algorithmes, dès leur création ;

– ou encore une priorité au rattrapage du retard technologique pointé par le rapport Draghi ainsi que des financements adaptés pour permettre une politique de recherche renforcée. Elle préconise en particulier de doubler le montant des crédits du programme européen « Horizon Europe ».

---

des données rendues manifestement publiques par la personne concernée ; traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou pour des motifs d'intérêt public important ; traitement nécessaire aux fins de la médecine préventive ou de la médecine du travail ou pour des motifs d'intérêt public dans le domaine de la santé publique.

Horizon Europe

Horizon Europe est le programme-cadre de l'Union européenne pour la recherche et l'innovation pour la période 2021-2027.

Ce programme dispose d'un budget de 95,5 milliards d'euros sur 2021-2027.

Ses objectifs sont les suivants :

- renforcer les bases scientifiques et technologiques de l'Union européenne ;

- stimuler la compétitivité, y compris celle de son industrie ;

- concrétiser les priorités politiques stratégiques européennes ;

- contribuer à répondre aux problématiques mondiales, dont les objectifs de développement durable.

Dans un rapport présenté le 22 janvier 2025[1], la Cour des comptes a observé que le taux de retour de financement d'Horizon Europe obtenu par la France était inégal selon les trois piliers du programme. Ainsi, si la France, même en deçà d'un objectif de 17,5 %, améliore sa position dans le pilier 1 (recherche fondamentale), les performances sont moins bonnes sur le pilier 2 (organisé autour de six thèmes de recherche appliquée) mais satisfaisantes sur le pilier 3 (innovation) ; la France est au deuxième rang européen.

B. LA POSITION DE LA COMMISSION DES AFFAIRES EUROPÉENNES DU SÉNAT : SOUTENIR ET RENFORCER LA PROPOSITION DE RESOLUTION EUROPÉENNE

1. Soutenir la proposition de résolution européenne

a) Soutenir la proposition en rationalisant sa rédaction

La commission des affaires européennes soutient, dans son principe, la proposition de résolution européenne, qui s'inscrit dans la continuité des positions qu'elles ont défendu au cours des dernières années lors des débats sur le DSA, le DMA ou encore la boussole numérique.

Elle estime que l'adoption de cette proposition est justifiée à double titre. Tout d'abord, dans un souci de cohérence avec l'ensemble des précédents votes ici au Sénat sur ces sujets actuels et importants. Ensuite, par principe, alors que la plupart des États membres appellent l'Union européenne à ne pas faiblir dans la mise en œuvre de normes adoptées à la suite d'un débat démocratique et visant à protéger nos concitoyens, malgré les attaques dont elles peuvent faire l'objet.

[1] *« La mobilisation des fonds européens en matière de programmes de recherche : les programmes Horizon 2020 et Horizon Europe – un effort à accentuer », communication à la commission des finances de l'Assemblée nationale, 22 janvier 2025.*

Cependant, dans un souci de clarté, la commission des affaires européennes du Sénat préconise de modifier la rédaction initiale de la proposition afin :

- d'améliorer la clarté du dispositif par le regroupement de considérants redondants et l'ordonnancement des recommandations au sein de trois parties distinctes : faire respecter le cadre normatif européen en vigueur, au premier rang le DSA, renforcer les modalités de régulation des très grandes plateformes en ligne, mobiliser tous les efforts au service de la souveraineté numérique de la France et de l'Union européenne ;

- d'appeler le Gouvernement et ses partenaires européens, dans la mise en œuvre de la réglementation numérique européenne, à privilégier l'application intransigeante de ces dernières au maintien du modèle économique des très grandes plateformes en ligne, qui, en lui-même, constitue aujourd'hui un risque systémique ;

- de souligner que la crédibilité des enquêtes ouvertes par la Commission européenne au titre du DSA est dépendante du délai raisonnable de leur déroulement ;

– préciser la rédaction afin de rappeler que la liberté d'expression est le fondement essentiel de nos sociétés démocratique et est garantie par les Constitutions des États membres de l'Union européenne, par la Convention européenne des droits de l'homme et des libertés fondamentales et par la Charte européenne des droits fondamentaux, mais qu'elle s'exerce dans les conditions prévues par la loi et dans le respect de l'État de droit.

b) Rappeler le principe de la liberté d'expression et la sanction de ses abus

À cet égard, la commission des affaires européennes du Sénat souhaite rappeler que **la liberté d'expression doit rester le principe**. Dans cette optique, établir un mécanisme administratif permettant la suspension **d'un service de manière immédiate dès les premières détections de faux comptes ou fausses informations, sans le temps d'une enquête, peut certes** sembler être un moyen de pression immédiat sur des acteurs économiques, mais **serait problématique quant au respect de la liberté d'expression**, d'autant plus si le « temporaire » était prolongé ultérieurement. Elle serait assimilée à de la censure.

Un cas particulier : la suspension de *Russia Today* France

Le 1er mars 2022, une semaine après le début de l'agression russe en Ukraine, les médias *Russia Today* et *Sputnik*, accusés de mener des actions de propagande continues et concertées en soutien du gouvernement russe, ont été interdits de diffusion dans toute l'Union européenne par le Conseil de l'Union européenne. Ce dernier a considéré que les actions de ces médias constituaient une menace pour l'ordre et pour la sécurité publics de l'Union européenne.

La société *Russia Today* France a contesté cette décision devant le Tribunal de l'Union européenne, estimant que seule l'ARCOM pouvait sanctionner un média audiovisuel pour un contenu éditorial inapproprié.

Dans un jugement de sa grande chambre, en date du 27 juillet 2022[1], le Tribunal a au contraire reconnu la compétence du Conseil de décider de mesures restrictives au titre de la politique étrangère et de sécurité commune. Il a en outre confirmé que cette mesure d'interdiction « temporaire », proportionnée et répondant à un objectif d'intérêt général, ne remettait pas en cause le contenu essentiel de la liberté d'expression.

Un précédent existe en France avec l'annulation de la majeure partie des dispositions de la loi visant à lutter contre les contenus haineux sur Internet[2] par le Conseil Constitutionnel au nom de la liberté d'expression[3].

En pratique, le dispositif initial de cette loi imposait aux hébergeurs et fournisseurs d'accès à Internet de retirer les « contenus manifestement haineux » ou de rendre inaccessible de tels contenus, largement définis.

Sur saisine de soixante sénateurs, le Conseil Constitutionnel avait censuré cette disposition en estimant qu'il constituait une **atteinte qui n'était pas « nécessaire, adaptée et proportionnée »**. Il observait en effet que, compte tenu des difficultés d'appréciation du caractère manifestement illicite des contenus signalés dans le délai imparti, de la peine encourue dès le premier manquement et de l'absence de clause spécifique d'exonération de responsabilité, les opérateurs auraient été incités à retirer tous les contenus signalés, « par précaution » si l'on peut dire.

Or, pour le Conseil, la liberté d'expression est à la fois « l'une des garanties essentielles du respect des autres droits et libertés et de la souveraineté nationale »[4] mais aussi une « condition de la démocratie »[5]. Cette

[1] *Arrêt du Tribunal de l'Union européenne, RT France contre Conseil de l'Union européenne, 27 juillet 2022, affaire T-125/22.*
[2] *Loi n°2020-766 du 24 juin 2020.*
[3] *Décision n°2020-801 DC du 18 juin 2020 – loi visant à lutter contre les contenus haineux sur Internet.*
[4] *Décision n°84-181 DC du 11 octobre 1984.*
[5] *Décision n°2009-580 DC du 10 juin 2009.*

liberté contient aujourd'hui celle « d'accéder » aux « services de communication au public en ligne »[1].

Exemples internationaux d'interdiction des réseaux sociaux TikTok et X

Les cas d'interdiction durable des réseaux sociaux restent rares.

En Europe, **l'Albanie** a instauré en janvier 2025 une interdiction à l'encontre de la plateforme TikTok, invoquant des préoccupations sur la violence chez les jeunes que le réseau social pourrait susciter et amplifier. Cette interdiction est prévue pour durer un an, le temps de trouver des solutions techniques pour empêcher l'utilisation de la plateforme par les mineurs.

En Inde, TikTok a été banni en 2020, ainsi que 58 autres applications chinoises, officiellement en raison de préoccupations liées à la diffusion de contenus dangereux pour les mineurs, mais aussi afin de freiner la propagation perçue de l'influence chinoise dans le pays.

Dix-neuf pays dans le monde ont imposé des restrictions à l'égard de TikTok. Pour certains, il s'agit d'une interdiction de téléchargement de l'application sur les smartphones professionnels des employés du gouvernement et du secteur public, comme aux États-Unis, en France, au Canada ou au Royaume-Uni. Pour d'autres, l'interdiction s'étend aussi aux téléphones personnels des citoyens.

S'agissant de X, la plateforme est actuellement bloquée en Russie, en Chine, en Iran, en Corée du Nord, au Myanmar, au Pakistan, au Turkménistan et en Érythrée. Depuis 2015, 30 autres pays ont restreint temporairement son accès, particulièrement en période de crise politique.

L'interdiction comme conséquence d'un rapport de force : exemples du Brésil et des États-Unis

En avril 2024, la justice brésilienne a enquêté sur la plateforme X, l'accusant d'avoir réactivé des comptes bannis sur la plateforme. En réaction, Elon Musk a fermé les bureaux de X au Brésil, malgré l'obligation légale d'y maintenir au moins un représentant légal sur place. Le 31 août 2024, la Cour suprême a suspendu la plateforme après son refus de se conformer aux exigences du pays. L'interdiction a été levée le 8 octobre 2024 après le paiement d'une amende de 4,8 millions d'euros et après s'être acquitté des obligations imposées par la justice brésilienne.

Aux États-Unis, le Congrès a adopté en avril 2024 une loi visant TikTok pour des risques présumés d'espionnage par la Chine. La société mère, ByteDance, avait jusqu'au 19 janvier 2025 pour s'y conformer, mais la justice américaine a rejeté ses recours. TikTok a été bloqué à cette date, avant d'être rétabli le lendemain grâce à un décret de Donald Trump suspendant l'application de la loi pour 75 jours. Pour résoudre la crise, Trump a proposé que les États-Unis obtiennent 50 % du capital de TikTok.

[1] *Voir note précédente.*

Interdire l'accès des réseaux sociaux aux mineurs : une solution tentée par plusieurs États, sans qu'on puisse aujourd'hui en tirer des conclusions

L'Australie a adopté, le 28 novembre 2024, une loi interdisant l'accès aux réseaux sociaux aux moins de 16 ans, avec des amendes pouvant atteindre 30,7 millions d'euros en cas de non-respect. Toutefois, les modalités d'application restent floues, et certaines plateformes comme WhatsApp et YouTube pourraient être exemptées. Les entreprises auront un an pour se conformer, le temps que les régulateurs précisent les règles.

En Floride, une loi interdisant l'ouverture de comptes aux moins de 14 ans entrera en vigueur en janvier 2025, mais sans détails sur son application. **L'Espagne** a proposé une législation similaire l'an dernier, sans date d'examen ni méthode de vérification d'âge définie.

Enfin, **en Chine**, et c'est extrêmement révélateur, l'accès des mineurs à Internet est très règlementé. Le temps de connexion aux réseaux sociaux et au temps de jeu en ligne sont limités de 40 minutes à deux heures par jour en fonction de l'âge et sont interdits la nuit. TikTok n'existe que sous l'appellation « Douyin » dans une version algorithmique qui propose essentiellement des contenus à caractère pédagogique aux utilisateurs mineurs, contrairement à la version occidentale.

c) Demander une mise en œuvre pleine et entière de l'ensemble des dispositions du DSA

À cet égard, la commission des affaires européennes du Sénat préconise d'**exploiter totalement les dispositions du DSA**, en particulier :

- la possibilité, pour le régulateur, de procéder à des inspections dans les locaux des plateformes en ligne. Selon la DG Connect, malgré les nombreuses enquêtes ouvertes, cette possibilité n'a pas encore été utilisée ;

- l'autorisation, pour les chercheurs indépendants, d'accéder aux données des très grandes plateformes en ligne. Là encore, cette disposition demeure à ce jour, largement « virtuelle » ;

- les sanctions des manquements constatés, en particulier contre des opérateurs réticents à suivre la réglementation européenne ou en « situation de récidive ».

d) Souligner que certaines dérives constatées constituent des infractions pénales qui peuvent être efficacement sanctionnées par le droit pénal

En France, de longue date, les fraudes informatiques et l'escroquerie en ligne sont réprimées pénalement. Mais, avec la numérisation de la vie quotidienne, la généralisation des procédures d'identification en ligne et d'autorisation de traitements de données personnelles, ainsi que la multiplication des objets connectés, les infractions numériques constituent une part croissante du contentieux pénal, en particulier concernant **les contenus illicites** et **les traitements de données personnelles non autorisés**.

Les contenus illicites sur Internet, doivent, comme précisé *supra*, être bloqués ou enlevés, par les plateformes en ligne, conformément au DSA et à la loi SREN. Ils peuvent faire en outre constituer des délits ou des crimes et faire alors l'objet de sanctions pénales.

Les infractions pénales liées aux contenus illicites sur Internet et leur sanction en droit pénal français

Infraction	**Sanction pénale**
Cyberharcèlement	2 ans d'emprisonnement et 30 000 euros d'amende 3 ans d'emprisonnement et 45 000 euros d'amende en cas de circonstances aggravantes Article 222-33 du code pénal
Diffusion, fixation, enregistrement, transmission de l'image ou de la représentation d'un mineur à caractère pédopornographique	5 ans d'emprisonnement et 75 000 euros d'amende 7 ans d'emprisonnement et 100 000 euros d'amende en cas de diffusion sur un réseau de communications électronique Article 227-23 du code pénal
Apologie du terrorisme	5 ans d'emprisonnement et 75 000 euros d'amende 7 ans d'emprisonnement et 100 000 euros d'amende en cas de diffusion sur un service de communication au public en ligne Article 421-2-5 du code pénal

Les plateformes doivent démontrer leur diligence et leur coopération loyale dans cette lutte contre les contenus illicites. *A contrario*, la justice pénale peut les poursuivre. Ainsi, en août dernier, M. Pavel Durov, le fondateur de la messagerie Telegram, qui modérait très modérément les contenus et répondait rarement aux réquisitions judiciaires, avait été interpellé à son arrivée en France, puis mis en examen, en particulier pour « refus de communiquer les informations nécessaires aux interceptions autorisées par la loi » et « complicité » de plusieurs délits et crimes qui s'organisaient sur la plateforme (trafic de stupéfiants, pédopornographie, escroquerie, etc.). Dans l'attente de son procès, il a été remis en liberté avec une interdiction de quitter le territoire français.

Les risques de traitements de données personnelles non autorisés se sont également multipliés.

Ainsi, l'article 226-18 du code pénal punit de cinq ans d'emprisonnement et de 300 000 euros d'amende **le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite**. Cette infraction vise, par exemple, les cas de cookies installés à l'insu des utilisateurs. Une même peine sera infligée au détenteur de données personnelles qui, à l'occasion du traitement de ces données, en détourne la finalité pour un autre usage[1].

La conservation de données personnelles sensibles d'une personne « en mémoire informatisée », sans le consentement exprès de l'intéressée, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende[2].

Quant **au fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données, l'article 323-2 du code pénal le punit d'une peine de cinq ans d'emprisonnement et de 150 000 euros d'amende**. Cette infraction vise les attaques par déni de service[3] ou par injection d'un « *malware* »[4] dans un système. Mais, pour le juriste Michel Séjean[5], cet article du code pénal peut concerner aussi la modification des algorithmes de recommandation d'un réseau social, à l'insu des utilisateurs de ce dernier.

Sur ce fondement, le député (Renaissance) des Côtes d'Armor Éric Bothorel, a effectué un signalement auprès du parquet de Paris, dont la section de lutte contre la cybercriminalité (J3) a ouvert une enquête sur les changements d'algorithmes du réseau social X. Ces changements ont fait l'objet, simultanément, d'une plainte de l'eurodéputée Aurore Lalucq (Place publique) et de la sénatrice Marie-Claire Carrère-Gée (Les Républicains) devant l'ARCOM, qui a décidé d'en saisir la Commission européenne, avec information à l'autorité de contrôle des services numériques d'Irlande, État membre où X a installé son siège européen.

La commission des affaires européennes propose par ailleurs d'**enrichir ce texte en y ajoutant des considérations visant à renforcer et à élargir sa portée**, présentées ci-après.

---

[1] *Article 226-21 du code pénal.*

[2] *Article 226-19 du code pénal.*

[3] *Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.*

[4] *Logiciel malveillant conçu pour infecter, endommager ou accéder à un système informatique.*

[5] *« Le code pénal face à la manipulation des opinions par voie de recommandations faussées », Dalloz, 6 février 2025.*

2. Conforter le modèle de régulation européen et consolider la stratégique numérique européenne

a) Garantir le pluralisme des réseaux sociaux et créer une offre alternative aux GAFAM

De là, pour le professeur David Colon, la position dominante des GAFAM sur l'information des citoyens et les effets préoccupants de leur « capitalisme de surveillance »[1] pour les sociétés démocratiques européennes comme pour les individus, la meilleure solution est sans doute d'encourager, au niveau européen, **la création de plateformes souveraines et fondées sur des règles éthiques rigoureuses.** En pratique, ces dernières pourraient être financées grâce aux contributions des citoyens et des entreprises soucieux du pluralisme des réseaux sociaux, d'une part, et du respect de règles éthiques en la matière, d'autre part.

La commission des affaires européennes du Sénat constate que la situation actuelle pousse à la recherche de solutions, parmi elles la mise en place d'outils attractifs, porteurs d'un véritable contenu, rompant avec la culture du vide et de la mise en scène est séduisante. À cet égard, elle estime que l'**actuelle réforme de l'audiovisuel public pourrait être l'occasion parfaite pour la concrétisation d'une telle recommandation**.

b) Envisager un centre d'expertise et un réseau de détection européen sur les ingérences étrangères comprenant un système d'alerte rapide

L'Union européenne s'est dotée de différents outils pour lutter contre les ingérences étrangères. Tout d'abord, une proposition de directive destinée à mieux encadrer l'activité des représentants d'intérêts travaillant pour le compte de pays tiers, est en négociation (elle a fait l'objet d'un débat d'orientation au Conseil, en juin 2024)[2].

Concernant plus spécifiquement les ingérences en ligne, outre le DSA, qui impose aux plateformes de retirer les contenus illicites, rappelons que l'Union européenne dispose également d'un cadre normatif pour assurer la transparence et le ciblage des publicités politiques (afin de repérer et, le cas échéant, de déjouer toute ingérence étrangère à l'origine de ces dernières)[3].

Le 18 juillet 2024, dans ses orientations politiques pour la Commission européenne 2024-2029, Mme von der Leyen annonçait vouloir renforcer ces outils par la mise en place d'» un bouclier européen de la démocratie » afin « de lutter contre la manipulation de l'information et les ingérences étrangères en ligne ». Pour cela, elle indiquait vouloir s'appuyer sur l'expérience du service français de vigilance et de protection contre les ingérences numériques

---

[1] *« L'âge du capitalisme de surveillance », Shoshana Zuboff, 2020.*
[2] *Proposition de directive COM (2023) 637 final du 12 décembre 2023.*
[3] *Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique.*

étrangères (Viginum) et sur celle de l'agence suédoise de défense psychologique.

De son côté, auditionné au Parlement européen, le 17 février 2025, Marc-Antoine Brillant, actuel chef de Viginum, a rappelé que « la protection du débat numérique de chaque pays relev[ait] de sa souveraineté » mais que l'institution d'un centre d'expertise européen, qui accompagnerait les États membres « dans la structuration de leurs capacités de réponse et de préparation face à des campagnes de manipulation de l'information » serait logique.

Sur la base de ces observations, **la commission des affaires européennes considère en premier lieu que la mise en place éventuelle d'un dispositif de veille et de détection des ingérences étrangères numériques s'inspirant de Viginum » au niveau européen doit être examinée mais qu'elle devrait être précédée par une analyse d'impact exhaustive envisageant des solutions opérationnelles pertinentes et examinant sa compatibilité avec les traités européens** (et, en particulier, avec l'article 4, paragraphe 2, du traité sur l'Union européenne qui affirme que la sécurité nationale est de la compétence exclusive des États membres).

Organisation et missions de Viginum

Le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a été créé par le décret n° 2021-922 du 13 juillet 2021. Placé auprès du Secrétaire général de la défense et de la sécurité nationale et composé d'une cinquantaine d'agents, il est un service d'investigation en ligne ayant une compétence nationale. Ses missions sont les suivantes :

- détecter et caractériser, en analysant les contenus accessibles publiquement sur les plateformes en ligne des opérateurs, les opérations de manipulation de l'information menées par des pays tiers ou des entités étrangères, et sécuriser le bon déroulement du débat public souverain, en particulier lors des « grands rendez-vous » (scrutins nationaux ; évènements sportifs ou culturels majeurs…). Pour ce faire, Viginum va se concentrer, non sur les contenus, mais sur les processus d'ingérence et de manipulation[1] (création de faux sites d'information, référencement privilégié sur les moteurs de recherche, amplification d'actions physiques sur les réseaux sociaux, recours non transparent à des influenceurs, etc.) et est autorisé à mettre en œuvre un traitement automatisé des données personnelles publiquement accessibles sur les plateformes en ligne ayant plus de 5 millions de visiteurs par mois sur le territoire français ;

- assister le secrétaire général de la défense et de la sécurité nationale dans sa mission d'animation et de coordination des travaux interministériels en matière de protection contre les opérations précitées ;

[1] *Parmi ces processus, on peut citer la création de comptes inauthentiques ou de faux sites d'information, le référencement privilégié de contenus constituant une manipulation de l'information, l'amplification d'actions physiques sur les réseaux sociaux, le détournement d'images ou de citations réels, ou encore le recours non transparent à des influenceurs…*

- fournir toute information utile à l'ARCOM dans l'accomplissement des missions qui lui sont confiées par la loi du 30 septembre 1986 relative à la liberté de communication ;

- contribuer aux travaux européens et internationaux dans ce domaine. Ainsi, Viginum est intégré au système d'alerte rapide mis en place par le Service européen d'action extérieure afin de partager sans délai des alertes et informations sur des actions d'ingérence étrangère en cours.

Comme déjà indiqué, Viginum mène à l'heure actuelle un travail efficace d'alerte et de sensibilisation des opérateurs et des utilisateurs en décryptant les actions ou tentatives d'ingérence étrangères dans le débat public français : opérations du réseau de propagande russe « Portal Kombat »[1], manœuvres informationnelles des autorités azerbaïdjanaises en Nouvelle-Calédonie[2], synthèse de la menace informationnelle sur les jeux Olympiques d'été de Paris 2024[3], etc.

Si l'analyse d'impact souhaitée conclut à la compatibilité avec les traités et à la pertinence d'un « bouclier européen pour la démocratie », la commission des affaires européennes considère que ce **dernier devrait être plutôt un réseau souple et décentralisé**, rassemblant les services et agences des États membres en charge de la lutte contre les ingérences étrangères en ligne existants, auxquels serait ajouté un organe similaire spécifiquement compétent pour éviter toute ingérence dans les communications, sites ou forums des institutions de l'Union européenne. Ce réseau qui serait conforme au principe de subsidiarité, pourrait être nommé « Vigie Europe » et devrait en outre bénéficier de financements existants et préalablement identifiés.

En deuxième lieu, ce réseau « Vigie Europe » devrait bénéficier des moyens et de la visibilité d'un « système d'alerte rapide », dont l'embryon existe déjà au sein du Service européen pour l'action extérieure (Viginum y participe), afin de diffuser au plus vite les informations relatives à une tentative d'ingérence.

En troisième et dernier lieu, la commission des affaires européennes, reprenant une préconisation du Conseil d'État dans sa dernière étude annuelle, dont l'objet était la « souveraineté », estime qu'une clause spécifique devrait être prévue dans ce dispositif pour laisser toute latitude aux autorités françaises et des autres États membres de choisir les modalités de partage d'informations et de coopération compatibles avec leurs impératifs de la sécurité nationale.

[1] *Rapports du 12 et du 14 février 2024.*
[2] *Rapport du 17 mai 2024.*
[3] *Rapport du 13 septembre 2024.*

En complément, il faut signaler qu'au Parlement européen, début février, une commission spéciale sur la défense de la démocratie, présidée par l'eurodéputée française Nathalie Loiseau, a été mise en place. Elle se donne pour objectif d'analyser l'état de la menace et les dispositifs de réponse en place dans les 27 États membres, en vue de proposer une éventuelle modification du cadre normatif européen.

c) Renforcer l'efficacité des contrôles des très grandes plateformes en ligne en y associant mieux les autorités de régulation nationales compétentes

Dès lors que les grandes plateformes en ligne ont leur siège européen hors de notre pays, le régulateur français, dans le cadre du DMA comme du DSA, est quasiment dépourvu de moyens d'action à leur égard, leur contrôle relevant pour l'essentiel de la Commission européenne. Certes, comme l'a expliqué son directeur général lors de son audition, l'ARCOM contribue à l'heure actuelle à la désignation des « signaleurs de confiance » exigés par le DSA et participe aux réunions du comité européen pour les services numériques. En outre, dans un souci de coopération loyale, l'autorité transmet régulièrement à la Commission européenne des plaintes et des signalements sur les décisions et contenus des très grandes plateformes en ligne à la Commission européenne. Auditionnée par vos rapporteures, la DG Connect de la Commission européenne s'est d'ailleurs félicitée de cette coopération.

Mais en retour, l'ARCOM semble peu informée de l'évolution des enquêtes en cours ouvertes par la Commission, ce qui n'est pas normal. Et pour l'heure au moins, elle ne semble jamais associée auxdites enquêtes alors même que le DSA prévoit une possibilité d'enquêtes conjointes (le texte vise une enquête conjointe aux coordinateurs nationaux mais son extension aux enquêtes de la Commission est parfaitement envisageable). Cette situation est insatisfaisante.

En effet, les conséquences des actions des très grandes plateformes en ligne sont « systémiques » et concernent donc tout autant la Commission européenne que les États membres. Or, **s'il était nécessaire de désigner un « chef de file » pour contrôler les très grandes plateformes en ligne, l'intervention de la seule Commission européenne dans ces dossiers n'apparaît pas comme la solution la plus pertinente**.

Ce constat avait déjà été émis par le Sénat dans ses résolutions européennes sur le DMA et le DSA[1].

La situation actuelle souligne un « effet ciseau » croissant entre les ressources limitées de la Commission européenne pour mener à bien en solitaire, les nombreuses enquêtes ouvertes depuis plusieurs mois contre la majorité des très grandes plateformes en ligne, qui, elles, disposent du temps, de l'argent et des compétences nécessaires pour retarder ou bloquer les procédures. Même si la Commission européenne a déjà obtenu des effectifs

[1] *Résolution européenne n°70 (2021-2022) du 14 janvier 2022.*

additionnels pour sa DG Connect afin que celle-ci dispose de ressources supplémentaires pour ces investigations, ces effectifs ne seront pas suffisants.

Simultanément, au fil des années, les autorités de régulation nationales, plus proches des acteurs « de terrain » du numérique, ont bâti des expertises sectorielles précieuses. Elles connaissent de surcroît parfaitement leur écosystème numérique national.

La commission des affaires européennes demande donc :

- un changement de philosophie des régulateurs nationaux et européens afin que, dans l'accomplissement de leurs missions, ils privilégient le strict respect du cadre normatif européen au maintien du modèle économique des très grandes plateformes en ligne, qui constitue un risque systémique par lui-même ;

- une nouvelle fois, dans le cadre du DMA, la mise en place d'un réseau de régulation numérique réunissant la Commission européenne et les autorités sectorielles nationales compétentes dans la protection des données et la régulation des télécommunications[1] ;

- dans le cadre du DSA, une réciprocité dans la transmission d'informations entre la Commission européenne et les coordinateurs nationaux pour les services numériques et une meilleure association de ces contrôleurs nationaux aux enquêtes de la Commission européenne sur les agissements des très grandes plateformes en ligne.

d) Imposer une véritable responsabilité des « médias algorithmiques » sur les contenus hébergés

Le Sénat a estimé à plusieurs reprises que le régime de responsabilité très limité des très grandes plateformes en ligne fournissant des informations et des contenus politiques sur la base d'algorithmes de recommandation, était insuffisant et, à l'initiative de la sénatrice Catherine Morin-Desailly, rapporteure, avait demandé une révision de la directive pour faire émerger au niveau européen un « troisième statut » de responsabilité entre ceux d'hébergeur et éditeur de contenus[2].

De même, le Sénat recommandait, dans sa résolution européenne n° 70 du 14 janvier 2022 précitée sur le DSA, d'aller plus loin qu'une reconnaissance circonstanciée de responsabilité au regard du droit de la consommation des plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, car « **ce statut d'» hébergeur » ne reflète par le caractère actif de plateformes** – en

[1] *Cette proposition a déjà été émise dans la résolution européenne n°32 (2021-2022) du Sénat sur la proposition de règlement sur les marchés numériques (DMA), en date du 12 novembre 2021. Cette résolution a été adoptée sur le rapport des sénatrices Florence Blatrix Contat et Catherine Morin-Desailly.*

[2] *Résolution européenne n° 31 (2018-2019) du 30 novembre 2018 sur la responsabilisation partielle des hébergeurs de contenus numériques.*

particulier les réseaux sociaux et places de marché, mais aussi, par exemple, les plateformes de partage de vidéos ou de musique – qui, par le biais notamment d'**algorithmes d'ordonnancement des contenus** , jouent bien un rôle de sélection des contenus, en augmentant la visibilité de certains au détriment d'autres, sur la base de paramètres déterminés par les plateformes et dans leur intérêt.

Le DSA a répondu partiellement à la demande du Sénat en fixant des obligations renforcées[1] aux fournisseurs de services intermédiaires en fonction de leur taille sur le marché et des risques que leurs activités peuvent susciter. **Néanmoins, malgré ces avancées dans la responsabilisation des plateformes en ligne, leur responsabilité juridique sur les contenus qu'ils hébergent ou qu'ils produisent demeure limitée.**

Ainsi, un fournisseur de services n'est pas responsable des informations stockées à la demande d'un destinataire du service, à condition que ce fournisseur n'ait pas effectivement connaissance d'un contenu illicite et si, lorsqu'il en prend connaissance, il agit promptement pour retirer ce contenu illicite ou en bloquer l'accès[2].

De plus, les fournisseurs de services intermédiaires ne sont soumis ni à une obligation générale de surveillance des informations qu'ils transmettent, ni à une obligation de stockage ou de recherche active des faits ou des circonstances révélant des activités illégales[3].

Certes, le DSA est d'application récente et il conviendra d'examiner ses modalités de mise en œuvre à l'égard des très grandes plateformes au cours des prochains mois. C'est la volonté politique, de la Commission européenne comme des États membres, qui sera déterminante pour faire la preuve de son efficacité.

Cependant, l'inspiration du DSA est « contractuelle ». Il pose une gradation d'obligations à respecter par les plateformes en ligne, en fonction de leur taille et du caractère systémique ou non des risques que leur activité induit, afin de les inciter à respecter spontanément ses dispositions. Les sanctions ne sont prévues qu'en tout dernier recours.

Or, dans un contexte marqué simultanément par la difficulté persistante des plateformes en ligne à modérer les contenus illicites, par la rapidité de diffusion de tels contenus sur les réseaux sociaux, et par leur caractère addictif, mais aussi par certaines expériences étrangères récentes de

---

[1] *Les plateformes doivent ainsi donner suite aux injonctions de retrait de contenus illicites par les autorités compétentes, respecter des mesures de transparence renforcée et reconnaître le statut de « signaleur de confiance ». Les très grandes plateformes en ligne doivent en outre mettre en place des procédures d'évaluation et d'atténuation des risques[1], organiser des audits indépendants pour évaluer le respect de leurs obligations et donner accès au coordinateur pour les services numériques de leur État membre d'établissement ainsi qu'à la Commission européenne, aux données nécessaires pour contrôler le respect du DSA.*

[2] *Article 6 du DSA.*

[3] *Article 8 du DSA.*

régulation démontrant l'efficacité d'un « bras de fer », le renforcement des contrôles et du régime de responsabilité des très grandes plateformes en ligne qui constitue des « médias algorithmiques » semble souhaitable.

La commission des affaires européennes du Sénat appelle donc à réformer le régime européen de responsabilité des fournisseurs de services en ligne, pour **créer un nouveau régime de responsabilité renforcée pour les très grandes plateformes utilisant des algorithmes d'ordonnancement des contenus**, conformément au souhait déjà exprimé par le Sénat dans sa résolution européenne de 2018 sur la responsabilité des hébergeurs de services en ligne.

e) Assumer un rapport de force international pour valoriser les données dans le respect du RGPD et relever le défi de la localisation des données sensibles dans l'Union européenne

Rappelons tout d'abord qu'une initiative qui viserait la localisation dans l'Union européenne, de toutes les données des citoyens français et des autres États membres, n'offrirait que des garanties limitées face aux législations étrangères à portée extraterritoriales (comme le *Cloud Act* américain) et à la porosité, déjà évoquée, entre certains acteurs du numérique et leurs gouvernements : comme le soulignait déjà la commission d'enquête du Sénat sur la souveraineté numérique, « quand bien même des données seraient physiquement localisées sur le territoire français ou européen, les entités qui contrôlent les centres de données (*data centers*) continueront, en raison de leur nationalité, à être également soumises à des régimes juridiques les obligeant à coopérer avec des puissances étrangères »[1].

En réalité, l'Union européenne a « toutes les cartes en main » mais il lui faut faire preuve de volonté politique pour appliquer ses règlements en assumant, si nécessaire, un rapport de force.

Dans cet esprit, comme le préconise le Sénat depuis plusieurs années[2], États membres et institutions de l'Union européenne doivent travailler à **rendre plus effectif le droit à la portabilité des données**[3], qui permet à un utilisateur de quitter une plateforme pour une autre avec une copie de ses données personnelles. Ce droit doit faciliter la concurrence entre responsables de traitement et développer la capacité « d'autodétermination informationnelle »[4] des utilisateurs.

---

[1] *Rapport de la commission d'enquête, p 69.*

[2] *Dans sa résolution européenne n° 32 (2021-2022) du 12 novembre 2021 sur la proposition de règlement sur les marchés numériques (DMA), le Sénat demandait aux contrôleurs d'accès de « prendre des mesures permettant une mise en œuvre effective des principes d'interopérabilité et de portabilité des données […], qui sont des éléments clef du bon fonctionnement du marché numérique ».*

[3] *Articles 20 du RGPD et 6, paragraphe 9, du DMA.*

[4] *« Les droits émergents dans le monde numérique : l'exemple du droit à l'autodétermination informationnelle » de Pauline Türk, revue Politeia, n° 31, décembre 2017.*

Il en va de même pour **l'obligation d'interopérabilité,** c'est-à-dire l'obligation, pour les différents systèmes, d'échanger des informations et d'utiliser mutuellement les informations échangées, prévue à l'article 6, paragraphe 7, du DMA[1]. Cette obligation s'impose aux acteurs du numérique reconnus « contrôleurs d'accès ». En pratique, cette obligation d'interopérabilité prévoit que le contrôleur d'accès doit permettre gratuitement :

- aux fournisseurs de services et aux fournisseurs de matériel informatique **d'interopérer efficacement** avec les mêmes caractéristiques matérielles et logicielles auxquelles on accède ou qui sont contrôlées par l'intermédiaire de son système d'exploitation ou son assistant virtuel, que celles qui sont disponibles pour les services ou le matériel fournis par le contrôleur d'accès, et d'accéder à ces caractéristiques ;

- aux entreprises utilisatrices et à d'autres fournisseurs de services fournis conjointement à des services de plateforme essentiels, ou à l'appui de ceux-ci, « **d'interopérer effectivement** avec les mêmes caractéristiques du système d'exploitation, logicielles ou matérielles, que ces caractéristiques fassent partie ou non d'un système d'exploitation, que celles qui sont disponibles pour ce contrôleur d'accès ou que celui-ci utilise dans le cadre de la fourniture de tels services, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité ».

Les contrôleurs d'accès fournissant des services de communication interpersonnelles non fondés sur la numérotation doivent, de leur côté, rendre interopérables « *au moins les fonctionnalités de base* » relatives aux messageries textuelles et au partage d'images, de messages vocaux et de vidéos[2].

[1] *Article 6, paragraphe 7 du DMA.*

[2] *Ces obligations sont d'application immédiate. Elles doivent en principe, être confortées, deux ans après la désignation du contrôleur d'accès, par une obligation d'interopérabilité concernant la messagerie textuelle entre des groupes d'utilisateurs finaux habituels et le partage d'images, de de messages vocaux et de vidéos entre une conversation de groupe et un utilisateur final individuel. Quatre ans après la désignation du contrôleur d'accès, ces obligations d'interopérabilité doivent concerner les appels vocaux et vidéos.*

Un exemple concret : l'accompagnement d'Apple par la Commission européenne pour respecter l'obligation d'interopérabilité

Depuis la mise en œuvre du DMA, en mars 2024, Apple s'est vu reconnaître le statut de « contrôleur d'accès » au titre du DMA par la Commission européenne, au titre de ses systèmes d'exploitation iOS et iPad OS.

Ainsi, dans le cadre de la procédure de « spécification » prévue par le DMA[1], le 19 septembre 2024, la Commission européenne a ouvert deux procédures afin d'accompagner la firme dans ses actions de conformité visant à mettre en œuvre effectivement l'obligation d'interopérabilité.

La première procédure porte sur plusieurs caractéristiques et fonctionnalités de connectivité iOS, utilisées pour les appareils connectés (jeux intelligents, casques d'écoute ou de réalité virtuelle, etc.). La Commission européenne va préciser selon quelles modalités Apple devra assurer l'interopérabilité effective de ces appareils avec des smartphones sur des fonctionnalités telles que les notifications, le couplage des appareils et la connectivité.

La seconde procédure porte sur le processus mis en place par Apple pour répondre aux demandes d'interopérabilité des développeurs et des tiers pour iOS et iPad OS. La Commission européenne y précisera si la solution arrêtée permet à tous les développeurs de profiter de manière effective et prévisible de l'interopérabilité.

Les conclusions de la Commission européenne sur ces procédures seront publiées le 19 mars 2025.

Cette obligation ne concerne toutefois pas l'intégralité des interfaces et modalités de fonctionnement des réseaux sociaux. Or, tant pour redonner le choix aux utilisateurs que pour leur permettre de reprendre le contrôle sur leurs données, il serait pertinent que cette interopérabilité puisse être étendue à l'ensemble de leurs interfaces et à leurs systèmes de recommandation[2]. Cette évolution pourra s'appuyer sur la décision « Alphabet » de la CJUE du 25 février 2025[3]. Celle-ci a affirmé que le refus d'une entreprise en position dominante d'assurer l'interopérabilité de sa plateforme avec l'application d'une autre entreprise qui deviendrait plus attractive est abusif, sauf exceptions[4].

La Commission européenne devra en outre ne pas rompre l'équilibre actuel de sa réglementation numérique dans la nouvelle stratégie sur l'utilisation des données qu'elle envisage, qui vise à fluidifier l'accès et le partage des données en faveur des entreprises « tout en respectant des normes

[1] *Article 8, paragraphe 2.*

[2] *Voir l'avis du Conseil national du numérique de juillet 2020 et le dossier intitulé « Ouvrir les réseaux sociaux : 4 pistes en 5 questions », établi par le Pôle d'expertise de la régulation numérique (PEREN) du Gouvernement, décembre 2024.*

[3] *CJUE, Alphabet et autres, 25 février 2025, C-233/23.*

[4] *Ces exceptions sont au nombre de deux : menace sur l'intégrité ou la sécurité de la plateforme ; impossibilité technique d'assurer l'interopérabilité.*

élevées en ce qui concerne la protection de la vie privée et la sécurité »[1]. Pour la commission des affaires européennes du Sénat, il est encore plus clair de confirmer que **cette stratégie devra respecter explicitement le RGPD**.

Enfin, la commission des affaires européennes veut saluer les efforts accomplis pour développer une offre pour l'hébergement souverain des données sensibles *via* le label SecNumCloud délivré par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et appelle à poursuivre ces efforts. Elle demande le **renforcement de la coopération européenne pour faire émerger un *cloud* souverain en *open source***.

f) Mieux protéger les mineurs

La protection des mineurs est une exigence fondamentale qui est prévue l'article 24 de la charte des droits fondamentaux de l'Union européenne. Cet article affirme aussi que « l'intérêt supérieur de l'enfant doit être une considération primordiale ». Elle est aussi un enjeu de souveraineté alors que 86% des mineurs de 8 à 18 ans sont inscrits sur les réseaux sociaux[2].

Or, la numérisation des sociétés européennes a une conséquence directe : celle d'une surexposition fréquente des mineurs aux écrans. En moyenne, les jeunes français âgés de 7 à 19 ans passent 3 h 11 sur les écrans chaque jour[3] pour échanger sur des messageries instantanées, pour regarder des vidéos, pour écouter de la musique ou pour faire des jeux vidéo.

Cette surexposition les conduit souvent à passer trop de temps devant les ordinateurs, tablettes et autres smartphones qui ont envahi leur vie quotidienne. Avec des risques avérés désormais bien identifiés : manque de sommeil et troubles du sommeil, activité physique insuffisante, anxiété, troubles de l'attention, etc.

Dans son ouvrage, *La civilisation du poisson rouge*, Bruno Patino, journaliste et actuel président d'ARTE, rappelait ainsi : « Le poisson rouge tourne dans son bocal. Il semble redécouvrir le monde à chaque tour. Les ingénieurs de Google ont réussi à calculer la durée maximale de son attention : 8 secondes. Ces mêmes ingénieurs ont évalué la durée d'attention de la génération des "*millenials*"[4], celle qui a grandi avec les écrans connectés : 9 secondes. »[5]

Sur ce point, la proposition de résolution prend acte de la mise en œuvre effective de l'une des dispositions « phares » du DSA, à savoir l'interdiction des publicités ciblées en ligne à destination des mineurs. Elle salue aussi les enquêtes ouvertes par la Commission européenne et visant les

---

[1] *Orientations politiques pour la Commission européenne 2024-2029, p 13.*
[2] *Étude de l'association e-Enfance 3080-Caisse d'Épargne, 2023.*
[3] *Étude IPSOS 2024 sur les jeunes et la lecture, effectuée pour le Centre national du livre.*
[4] *Appelée également « génération Y », elle regroupe les personnes nées entre le milieu des années 1980 et le milieu des années 1990.*
[5] *« La civilisation du poison rouge ; petit traité sur le marché de l'attention », Grasset, 2019.*

réseaux Meta, Snap, TikTok et YouTube au nom de la protection des mineurs et demande que dans leurs conclusion, l'intérêt supérieur de l'enfant prévale sur tout autre considération. Ces enquêtes s'intéressent en particulier aux mesures mises en œuvre pour protéger la santé des mineurs, aux moyens mis en œuvre par ces réseaux pour réduire les risques de stimulation des dépendances comportementales liés aux systèmes algorithmiques et aux dispositifs de vérification de l'âge des utilisateurs.

La surexposition des mineurs aux écrans soumet en outre les enfants et les adolescents à diverses menaces : consultation de contenus haineux ou inappropriés sur Internet, problèmes d'addiction, cyberharcèlement, escroquerie, « pédopiégeage ».

À titre d'exemple, la commission d'enquête du Sénat sur le réseau social TikTok a démontré que l'algorithme de recommandation de ce dernier était particulièrement efficace et qu'il mettait souvent en avant des contenus dangereux ou inappropriés : contenus liés aux désordres alimentaires et au suicide davantage proposés aux personnes vulnérables (dont les adolescents), défauts de modération face à la multiplication des « *challenges* » dangereux sur l'application, politique de modération ambigüe sur les contenus « hypersexualisés », etc.

La présente proposition de résolution européenne rappelle la responsabilité juridique et éthique des plateformes en ligne pour lutter contre ces contenus illicites.

En complément, la commission des affaires européennes du Sénat souhaite la **publication rapide de lignes directrices au niveau européen**, afin d'inciter les plateformes à adopter les standards les plus élevés de protection.

La présente proposition de résolution européenne se félicite également de l'adoption, sous l'impulsion des associations de protection de l'enfance et du Sénat, des dispositions de loi visant à sécuriser et à réguler l'espace numérique (ou SREN) du 21 mai 2024, obligeant les plateformes en ligne fournissant des contenus pornographiques à instaurer un système de vérification de l'âge de leurs utilisateurs et, s'ils ne la respectent pas, à des mesures de blocage ou de déréférencement.

Elle s'inquiète enfin du blocage des négociations de la proposition de règlement COM (2022) 209 final établissant des règles pour prévenir et combattre les abus sexuels contre les enfants en ligne, présentée par la Commission européenne le 11 mai 2022, et demande donc solennellement l'**adoption de cette réforme importante sans délai**, conformément aux préconisations de sa résolution européenne n° 77 du 20 mars 2023.

La proposition de règlement établissant des règles pour prévenir et combattre les abus sexuels sur les enfants en ligne et la résolution européenne du Sénat n° 77 du 20 mars 2023

Pour rappel, cette proposition est partie du triste constat que l'Union européenne occupait la place peu enviable de premier « hébergeur » de contenus à caractère pédopornographique dans le monde[1].

À titre principal, cette proposition de règlement tend à :

- imposer une évaluation des risques et des mesures d'atténuation des risques aux fournisseurs de services d'hébergement et de services de communications interpersonnelles, ainsi que des obligations de détection des contenus pédopornographiques sur injonction d'autorités nationales compétentes ;

- soumettre ces fournisseurs à une obligation de signalement des contenus détectés liés à des abus sexuels sur des enfants, et sur injonction de l'autorité compétente, à une **obligation de retrait** de ces contenus ou de blocage de leur accès ;

- instituer **un centre de l'Union européenne dédié à la prévention et à la lutte contre les abus sexuels sur mineurs**, qui recevrait les signalements, servirait d'intermédiaire entre les fournisseurs et les autorités compétentes des États membres.

La résolution européenne n° 77 du Sénat, adoptée en commission des affaires européennes, le 15 février 2023 sur le rapport des sénateurs Ludovic Haye, Catherine Morin-Desailly et André Reichardt, devenue définitive le 20 mars 2023, a rappelé que la lutte contre les abus sexuels sur les enfants devait être une priorité de tous les instants pour l'Union européenne et a approuvé le principe d'obligations de résultats imposées aux fournisseurs.

Elle a toutefois demandé **la mise en place d'un dispositif d'injonctions de détection efficace sans impliquer ni une surveillance généralisée et permanente des communications** (messages électroniques, conversations téléphoniques, etc.), **ni une remise en cause systématique du chiffrement**, qui est nécessaire à la confidentialité des communications dans certains cas spécifiques. En conséquence, **elle a soutenu les injonctions de détection et de retrait sur des contenus identifiés** mais a rejeté la recherche indifférenciée de contenus pédopornographiques et de « pédopiégeage ». Elle a aussi constaté que les technologies mises en avant par la Commission européenne pour cette détection n'étaient – en l'état – **pas fiables**, entraînant un nombre trop élevé de « faux positifs »[2].

Elle a refusé la création d'un nouveau centre de l'Union européenne (faible valeur ajoutée, missions en majorité déjà assurées par Europol et dépendance humaine et logistique à son égard, coût de fonctionnement[3]), demandant plutôt la

[1] *Selon la Commission européenne, le nombre de ces abus sexuels en ligne commis dans l'Union européenne est ainsi passé de 23 000 en 2010 à 725 000 en 2019.*

[2] *Selon la Commission européenne, les techniques de détection utilisant l'intelligence artificielle sont fiables à 80 % (ce qui induit un pourcentage d'erreurs élevé à 20 %). Pour les experts français, ce taux de fiabilité varie plutôt entre 50 et 70 %.*

[3] *La position intermédiaire du centre entre fournisseurs et autorités compétentes aurait pour conséquence de ralentir les suites des signalements transmis. Le centre serait dans les faits installé aux côtés des locaux d'Europol (à La Haye) et devrait bénéficier de ses ressources humaines et*

confirmation d'Europol comme pôle principal de la lutte contre les abus sexuels sur les enfants.

Elle a enfin incité les négociateurs européens à **prévoir une obligation de déréférencement des contenus pédopornographiques** (solution déjà en vigueur en France), **à valoriser l'expérience française réussie de la plateforme PHAROS**[1] et **à instaurer des mesures interdisant l'accès des mineurs aux contenus pornographiques** (activation par défaut des dispositifs de contrôle parental sur les téléphones des mineurs, instauration de dispositifs de vérification de l'âge des utilisateurs pour l'accès à certains sites, campagnes de « *name and shame* » à l'encontre des fournisseurs récalcitrants, etc.).

g) Assumer une véritable stratégie de souveraineté stratégique européenne

Soucieuse de s'appuyer sur la commande publique pour favoriser la politique industrielle européenne, la commission des affaires européennes du Sénat a pris note avec intérêt des orientations politiques présentées par Ursula von der Leyen, le 18 juillet 2024. Dans ces orientations, Mme von der Leyen a annoncé une révision de la directive « marchés publics » qui « permettra de donner **la préférence** aux produits européens dans les marchés publics pour certains secteurs stratégiques ».

En pratique, cette révision devrait être présentée en 2026.

La commission des affaires européennes du Sénat considère que le secteur numérique doit être intégré à la notion de secteur stratégique dans le cadre de cette révision.

En effet, l'annonce de la mise en place d'une « préférence européenne » dans certains marchés publics témoigne de la prise de conscience d'un changement d'ère, déjà décrit précisément dans le rapport Draghi. Ce changement implique, pour les États membres et l'Union européenne, de sortir d'une certaine « naïveté » à l'égard du fonctionnement des marchés, et de favoriser la constitution d'alliances industrielles capables de rivaliser dans le secteur numérique avec les concurrentes chinoises et américaines en particulier.

En outre, la commission des affaires européennes appelle à placer cette ambition numérique au rang des priorités budgétaires lors des négociations du prochain cadre financier pluriannuel de l'Union européenne.

---

matérielles. Son organigramme complexe n'augurerait pas d'une grande efficacité opérationnelle. Et il devrait bénéficier d'un budget annuel de plus de 28 millions d'euros à échéance 2030.

[1] *Créée en 2009, la plateforme PHAROS (pour Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements) reçoit des signalements concernant les contenus illégaux sur Internet, qui peuvent émaner de tout citoyen. Elle sert de relais pour demander, après évaluation du bien-fondé de cette demande, le retrait de ces contenus aux hébergeurs de services en ligne concernés. Par défaut, PHAROS dispose d'un droit de retrait à l'égard des contenus pédopornographiques et terroristes. Le retrait intervient alors dans les 24 heures (article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique). L'équipe de PHAROS est constituée d'une cinquantaine de gendarmes et de policiers.*

Enfin, elle préconise que la notion de souveraineté européenne couvre de façon effective tous les pans du numérique, incluant les y compris le quantique, l'*open source*, les semi-conducteurs, le *cloud computing* et les supercalculateurs.

h) Activer le levier de la commande publique, outil indispensable au service de l'ambition européenne

A l'heure actuelle, la commande publique représente environ 16 % du produit intérieur brut (PIB) de l'Union européenne.

Elle est encadrée par plusieurs textes européens relatifs à la passation des marchés publics[1], aux concessions, et à l'accès des opérateurs économiques, des biens et des services des pays tiers à ces marchés publics et concessions[2].

L'essence de ce cadre normatif[3] est de permettre un accès libre des entreprises aux marchés publics européens afin de privilégier la plus performante en appliquant les principes de libre circulation des marchandises, de liberté d'établissement, d'égalité de traitement et de non-discrimination, et de transparence.

En pratique, dans cette procédure, les pouvoirs adjudicateurs sont tenus d'attribuer les marchés publics sur la base du critère de « l'offre économiquement la plus avantageuse », après une procédure d'appel d'offres. Ce critère tient compte du prix de l'offre mais également de conditions complémentaires (facteurs environnementaux et sociaux, qualité, caractère innovant, etc.). En revanche, aucune utilisation « stratégique » de la commande publique, à des fins de politique industrielle, n'a été prévue dans ce cadre, destiné à garantir une concurrence libre et équitable.

Cependant, pour les entreprises françaises et européennes du numérique, celle-ci a pu souvent être faussée par le refus de certains pays tiers d'ouvrir leurs propres marchés publics et /ou par leur soutien massif à leurs entreprises nationales à travers une politique d'aides d'État assumée. Simultanément, le choix, par les organes publics européens, de prestataires ayant leur établissement dans un pays tiers et déjà dominants dans le secteur concerné au titre de l'offre économique la plus avantageuse, n'est pas satisfaisant car il empêche la consolidation d'un écosystème numérique

---

[1] *Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE.*

[2] *Règlement (UE) 2022/1031 du Parlement européen et du Conseil du 23 juin 2022 concernant l'accès des opérateurs économiques des biens et des services des pays tiers aux marchés publics et concessions de l'Union et établissant des procédures visant à faciliter les négociations relatives à l'accès des opérateurs économiques, des biens et des services originaires de l'Union aux marchés publics et concessions des pays tiers (Instrument relatif aux marchés publics internationaux – IMPI).*

[3] *Par exception, les marchés publics liés à la défense et à la sécurité nationales sont encadrés par des règles spécifiques.*

européen durable. Pour parvenir à cet objectif, les règles du marché sont insuffisantes.

La France dispose d'une procédure – mal connue – permettant de favoriser les entreprises françaises et européennes dans la commande publique : en effet, l'article L. 2112-4 du code de la commande publique prévoit que « l'acheteur peut imposer que les moyens utilisés pour exécuter tout ou partie d'un marché, pour maintenir ou moderniser les produits acquis soient localisés sur le territoire des États membres de l'Union européenne ». Il s'agit bien cependant d'une dérogation aux règles des marchés publics à appréhender au cas par cas et devant être justifiée par l'objet du marché (assurer la sécurité des informations ou des approvisionnements, ou prendre en compte des considérations environnementales ou sociales).

En outre, tirant les leçons des crises du Covid-19 et de la guerre en Ukraine, qui ont souligné leurs dépendances dans des secteurs critiques, la France et l'Union européenne font évoluer leurs dispositifs juridiques.

Par ailleurs, sur un « mode défensif », l'Union européenne a adopté, pour la première fois, un règlement prévoyant que, pour tout marché public et tout contrat de concession, les acheteurs et les autorités concédantes peuvent prendre des mesures de restriction d'accès à la commande publique à l'égard des opérateurs économiques de pays tiers n'ayant pas passé d'accord avec l'Union européenne sur les marchés publics et/ou qui pratiquent des restrictions à l'accès des entreprises européennes à leurs propres marchés publics[1].

Au-delà de ces dispositions, la commission des affaires européennes appelle à **activer le levier de la commande publique**, en tant qu'outil stratégique au service de l'ambition numérique européenne.

Comme l'indiquait déjà l'exposé des motifs de la proposition de résolution européenne n° 664 (2021-2022) précitée, « l'usage du levier de la commande publique [permettrait de] favoriser à la fois l'innovation et le passage à l'échelle d'acteurs européens dans certains secteurs critiques, afin de stimuler la formation d'écosystèmes numériques européens ».

La commission des affaires économiques du Sénat, saisie de cette proposition de résolution européenne, soutenait cette position en indiquant qu'» [o]util stratégique de politique économique, indispensable à l'émergence d'acteurs innovants y compris dans le secteur numérique, le levier de la commande publique demeure peu utilisé en France et dans l'Union européenne, alors qu'il représentait pourtant 111 milliards d'euros en 2020 pour la France uniquement.

---

[1] *Règlement (UE) 2022/1031 du 23 juin 2022 (Instrument relatif aux marchés publics internationaux).*

« À cet égard, les récentes conclusions de la mission d'information du Sénat sur l'excellence de la recherche et la pénurie de champions industriels sont particulièrement éclairantes :

« - l'utilisation du droit de la commande publique peut s'avérer plus frileuse en France que dans d'autres pays ;

« - toutes les possibilités permises par le droit de la commande publique ne sont pas pleinement exploitées ;

« - la formation des acheteurs publics aux achats innovants devrait être renforcée afin de privilégier davantage les TPE, PME et jeunes pousses ;

« - les principes généraux de la commande publique pourraient être complétés, à l'instar de ce qui a été fait en Allemagne, pour y intégrer d'autres considérations que la libre concurrence telles que le soutien aux PME ou à l'innovation. »[1]

Auditionnés par la commission des affaires européennes, la délégation à la prospective et le groupe numérique du Sénat le 30 janvier 2025, Bernard Benhamou et Jean-Marie Cavada ont indiqué que « parmi les leviers essentiels figure la commande publique, qui joue un rôle moteur aux États-Unis depuis la mise en place du Small Business Act en 1953. Ce dispositif, inexistant en Europe, oriente une part significative des marchés publics vers les petites et moyennes entreprises. De même, un European Buy Act, ciblant les entreprises stratégiques les plus sensibles, pourrait constituer une réponse efficace au déséquilibre actuel. »

Lors des auditions menées sur la présente proposition de résolution, il a été rappelé l'importance que revêtait la commande publique pour faciliter l'émergence d'une souveraineté industrielle. À titre d'exemple, en France, pour la certification de « hébergeur des données de santé », un critère, non pas de souveraineté, mais de transparence a été mis en place : un opérateur candidat à la certification doit ainsi signaler les lois extraterritoriales auxquelles il est soumis, donc s'il existe ou non un risque d'accès aux données, et, le cas échéant, désigner le pays concerné.

Cela est de nature à renforcer la souveraineté dans la mesure où cela incite à discriminer selon ce critère essentiel qui est la localisation des données et, par conséquent, incite à choisir des plateformes de cloud de confiance qui maitrisent la chaine de bout en bout.

La commission des affaires européennes du Sénat estime que pour agir sur ce levier de la commande publique, il est nécessaire de **sensibiliser les différents acteurs et les acheteurs**, notamment dans les collectivités territoriales, afin qu'ils soient conscients des enjeux de ce sujet. En incitant les

---

[1] *Rapport n°774(2021-2022) de la commission des affaires économiques du Sénat sur la proposition de résolution n°664 (2021-2022) au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur le programme d'action numérique de l'Union européenne à l'horizon 2030 - Sénat, https://www.senat.fr/rap/l21-774/l21-774.html*

entreprises à se tourner par exemple vers des **plateformes labellisées SecNumCloud**[1], non seulement elles privilégient des solutions respectueuses du droit européen mais, de plus, elles participent au développement de plateformes européennes souveraines. La commande publique doit aider à favoriser le développement du marché français et européen de l'informatique en nuage.

[1] *« Élaboré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence du point de vue technique, opérationnel ou juridique. D'une part, les prestataires proposant une offre d'informatique en nuage (cloud) doivent présenter une bonne hygiène informatique, d'autre part, les données doivent être protégées en conformité avec le droit européen. » Source : ANSSI*

EXAMEN EN COMMISSION

La commission des affaires européennes, réunie le 13 mars 2025, a engagé le débat suivant :

M. Jean-François Rapin, président. – Mes chers collègues, nous nous réunissons ce matin pour examiner la proposition de résolution européenne (PPRE) déposée par Didier Marie et plusieurs de ses collègues du groupe socialiste, écologiste et républicain. Cette proposition vise à l'application stricte du cadre réglementaire numérique de l'Union européenne et appelle au renforcement des conditions d'une réelle souveraineté numérique européenne.

Cette démarche s'inscrit dans la continuité des travaux conduits depuis plusieurs années par nos collègues Catherine Morin-Desailly et Florence Blatrix Contat, qui ont cette fois mené de nombreuses auditions dans des délais serrés et ont tenu à ajuster jusqu'au bout leur position sur la proposition. C'est ce qui explique que vous ayez été destinataires, hier, d'une ultime version modifiée de cette position, qui tient compte des échanges ayant eu lieu, mardi soir, entre le ministre de l'Europe et des affaires étrangères, le ministre délégué chargé de l'Europe et les membres des commissions des affaires européennes de l'Assemblée nationale et du Sénat.

L'approche de nos rapporteurs est ambitieuse mais elle semble à la hauteur des défis auxquels l'Europe est confrontée.

À ce stade, il faut rappeler que l'Union européenne a su mettre en place un cadre réglementaire particulièrement puissant, conforme à nos valeurs, avec le règlement général sur la protection des données (RGPD), le règlement européen sur les marchés numériques (*Digital Markets Act* ou DMA) et le règlement européen sur les services numériques (*Digital Services Act* ou DSA).

Le 29 janvier dernier, l'ancien commissaire européen Thierry Breton déclarait devant notre commission que, pour la première fois, ce cadre bénéficiait « d'une portée extraterritoriale dans l'espace numérique ».

Depuis longtemps, les États-Unis imposent une extraterritorialité de leurs règles, à travers le dollar ou leur réglementation financière. Les États membres de l'Union européenne ont, pour leur part, bâti un ensemble de normes qui empêche désormais les grandes plateformes en ligne de faire ce qu'elles veulent sur notre territoire. L'offensive des « GAFAM », acronyme des entreprises américaines Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft, contre ce cadre normatif, dans le sillage de l'élection de M. Donald Trump à la présidence des États-Unis d'Amérique, est, en quelque sorte, la reconnaissance de ces nouvelles capacités européennes.

Parallèlement, nous avons malheureusement observé, lors d'élections récentes, notamment en Roumanie, des actions d'ingérences étrangères et de de manipulation de l'information *via* les réseaux sociaux. Le sujet que nous abordons ce matin est donc essentiel, et je remercie Catherine Morin-Desailly et Florence Blatrix Contat de nous faire part de leur analyse.

Mme Catherine Morin-Desailly, rapporteure. – La proposition de résolution européenne de nos collègues poursuit un triple objectif. Elle demande une application stricte du cadre réglementaire européen du numérique et son respect par toutes les plateformes en ligne. Elle appelle à un renforcement de ce cadre réglementaire pour mieux responsabiliser les plateformes. Enfin, elle demande que soient accentués les efforts des États membres et de l'Union européenne pour bâtir une véritable souveraineté numérique européenne.

Avec Florence Blatrix Contat, nous voudrions tout d'abord nous excuser pour l'envoi, hier après-midi, d'une rectification de notre position sur cette proposition de résolution. Je vous rassure, elle n'en modifie pas du tout le sens, mais en complète utilement les dispositions. Je remercie notre président d'avoir accepté cette démarche, car elle nous permet d'être en cohérence, non seulement avec la rencontre déjà évoquée avec les ministres mardi soir, mais également avec l'audition de M. Bruno Patino, président du directoire d'Arte France et responsable du comité de pilotage des États généraux de l'information.

En mars 2013, dans un rapport dont j'étais la rapporteure, notre commission s'interrogeait sur le fait de savoir si l'Union européenne était en passe de devenir une colonie numérique. Douze ans après, où en sommes-nous ? Force est de constater que le chemin pour parvenir à une véritable souveraineté numérique européenne est encore très long.

En effet, les grandes plateformes en ligne américaines, les fameuses GAFAM, et chinoises, à l'exemple de TikTok, dominent clairement le marché européen. Ainsi, Google reste le moteur de recherche sollicité par les utilisateurs européens dans 90 % des cas. Trois firmes américaines, AWS, Microsoft et Google, se partagent 70 % du marché européen de l'informatique en nuage, autrement dit le *cloud*. Enfin, les réseaux sociaux de ces plateformes sont devenus omniprésents dans nos vies quotidiennes. Facebook, c'est 35 millions d'utilisateurs en France. X, ex-Twitter, c'est 33 millions. Et TikTok, 22 millions.

Comme nous l'a indiqué M. Bruno Patino, l'Europe paye aujourd'hui de ne pas avoir cherché à maîtriser les outils qui « sont en bout de chaîne », les « derniers centimètres qui relient aux individus », c'est-à-dire les réseaux sociaux. Or, comme l'ont démontré nos précédents travaux avec Florence Blatrix Contat sur le DMA et le DSA, ainsi que les commissions d'enquête du Sénat sur la souveraineté numérique européenne, sur TikTok, ou sur la lutte

contre les ingérences étrangères, cette dépendance européenne n'est pas sans danger.

Tout d'abord, ces réseaux et plateformes sont fondés sur un « modèle toxique » qui mêle l'économie de l'attention et les « clics rémunérateurs », incitant l'utilisateur à rester connecté le plus longtemps possible. Cela permet à la plateforme de collecter des données et de lui proposer ensuite des services ou publicités ciblés. Pour conserver cette attention, la plateforme va établir des algorithmes de recommandation qui vont favoriser la diffusion de fausses informations et la valorisation de contenus polémiques, violents, sexualisés et extrêmes.

Autre danger, rappelé par M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique, lors de son audition au Sénat, le 30 janvier dernier, les données sont devenues un outil de contrôle des populations. Les réseaux sociaux réunissent tellement d'informations sur nous qu'ils peuvent nous manipuler d'une manière qui était totalement impensable par le passé. Enfin, en raison des législations extraterritoriales américaines, telles que le *Cloud Act* ou le *Foreign Intelligence Surveillance Act* (FISA), ou chinoises, nos données personnelles sont accessibles aux services de renseignement de ces pays. Voilà pourquoi l'existence d'un cadre réglementaire européen protecteur est si important.

Je vous rappelle qu'il comporte trois piliers. Le premier pilier est le règlement général sur la protection des données, ou RGPD, entré en vigueur en 2018, qui permet aux utilisateurs des plateformes de conserver une maîtrise de leurs données personnelles tout en autorisant leur valorisation raisonnée. Le règlement européen sur les marchés numériques, ou DMA, tend à imposer des obligations spécifiques aux plateformes en ligne si importantes et si oligopolistiques sur le marché européen qu'elles en contrôlent l'accès afin de préserver la concurrence. On peut citer la nécessité d'obtenir un consentement explicite de leurs utilisateurs pour utiliser leurs données personnelles à des fins de publicité ciblée ou l'obligation d'interopérabilité des fonctionnalités de base des messageries.

Enfin, le troisième pilier est le règlement européen sur les services numériques, ou DSA, qui vise à éviter un « *far-west* numérique », pour reprendre l'expression de l'ancien commissaire Thierry Breton, en obligeant les grandes plateformes en ligne à faire preuve de transparence, à modérer les contenus qu'elles hébergent et à agir contre les contenus illicites comme l'apologie du terrorisme ou les contenus pédopornographiques.

À ce titre, la Commission européenne peut mener des enquêtes mais, il faut le déplorer, ces dernières ne sont soumises à aucun délai.

Cette réglementation, complétée par le règlement encadrant l'utilisation de l'intelligence artificielle, est cohérente. Mais est-elle suffisante ? Alors que le DMA et le DSA sont entrés en vigueur il y a un an, en mars 2024, elle est aujourd'hui confrontée à plusieurs défis.

Mme Florence Blatrix Contat, rapporteure. – Tout d'abord, au cours de ces derniers mois, les réseaux sociaux ont été utilisés par des pays tiers pour mener des campagnes d'ingérence et de manipulation de l'information. Je veux citer deux exemples qui ont été documentés par le service français de vigilance et protection contre les ingérences numériques étrangères, Viginum. Le premier concerne les actions de déstabilisation en ligne menées par l'Azerbaïdjan sur les réseaux X et Facebook contre la France au sujet de la situation en Nouvelle-Calédonie, avec la diffusion de photomontages et de vidéos truquées montrant des policiers tuant des manifestants.

Le second exemple a eu lieu en novembre dernier. Le réseau social TikTok a servi de levier à une manipulation massive d'algorithmes et d'influenceurs pour favoriser la candidature à l'élection présidentielle roumaine d'un parfait inconnu défendant une ligne pro-russe, M. Calin Georgescu. Ce dernier est arrivé en tête du premier tour mais la Cour constitutionnelle roumaine a annulé le scrutin.

J'y ajoute ce qui, selon moi, constitue un mélange des genres problématique, à savoir le soutien public et répété de M. Musk, à la fois chef d'entreprise, dirigeant du réseau X et responsable du nouveau département de l'efficacité gouvernementale du gouvernement américain, sur son réseau, à un parti d'extrême droite allemand, l'AFD, lors des dernières élections au *Bundestag*.

Autre sujet d'inquiétude, depuis le retour de M. Donald Trump à la Maison-Blanche, les dirigeants des grandes plateformes numériques américaines, qui avaient tous rallié sa campagne, ne cessent de dire tout le mal qu'ils pensent de la réglementation européenne du numérique, qui, selon eux, ne serait rien d'autre que de la censure limitant la liberté d'expression et un obstacle à l'innovation. Cette volonté de démantèlement de la réglementation européenne a depuis été confirmée par le vice-président américain, J. D. Vance, et par les commissions compétentes du Congrès américain.

Il faut sans doute y voir une preuve de l'efficacité de la réglementation européenne qui contraint les GAFAM à ne pas collecter nos données sans notre consentement, n'importe quand, n'importe comment et pour n'importe quel usage. Mais face à ces risques, la réaction de la Commission européenne, qui assure en premier lieu le respect de ce cadre, a semblé hésitante et « à géométrie variable » selon les dossiers. Ainsi, dans la campagne d'ingérence en Roumanie, la Commission européenne a ouvert une enquête au titre du DSA sur TikTok dès le 17 décembre, en particulier sur l'obligation de la plateforme d'évaluer et d'atténuer les risques systémiques liés à l'intégrité de l'élection présidentielle.

En revanche, concernant les interventions de M. Musk, elle s'est abstenue de réagir publiquement pendant plusieurs jours. C'est sous la pression de plusieurs États membres, dont la France, qu'elle a décidé le 17 janvier dernier d'approfondir son enquête déjà en cours au sujet du réseau

X. Plus généralement, on peut déplorer la lenteur des enquêtes menées par la Commission européenne sur les réseaux sociaux au titre du DSA. Comme le résumait notre ministre de l'Europe et des affaires étrangères, Jean-Noël Barrot, le 8 janvier dernier : « Soit la Commission européenne applique avec la plus grande fermeté les lois que nous nous sommes données pour protéger notre espace public, soit elle ne le fait pas et alors il faudra qu'elle consente à rendre aux États membres de l'UE, à rendre à la France, la capacité de le faire ».

Pire, il nous disait mardi soir, lors de la rencontre qu'il organisait avec M. Haddad, que la Commission européenne hésitait à intervenir. Ce constat est préoccupant. Voilà pourquoi cette proposition de résolution européenne déposée par le groupe socialiste, écologiste et républicain demande une application pleine et entière de la réglementation européenne du numérique, en particulier du DSA. Elle souhaite aussi un renforcement des moyens de contrôle des plateformes numériques, en particulier en fixant des normes éthiques minimales pour tous les algorithmes de recommandation dès leur conception, en imposant à ces algorithmes le respect de l'interdiction des données personnelles sensibles prévues à l'article 9 du RGPD et en demandant l'adoption rapide du « bouclier européen de la démocratie » annoncé par la Commission européenne pour la fin de cette année contre les ingérences étrangères.

Enfin, la proposition dessine les grands axes d'une politique de souveraineté numérique européenne avec la mise en place de plateformes en ligne souveraines et le développement de *cloud* souverains, dans la lignée de nos propres propositions formulées dans nos rapports que dans les débats dans l'hémicycle. Elle veut aussi le renforcement des efforts européens dans l'intelligence artificielle en s'appuyant sur les réseaux publics européens. Elle appelle enfin de ses vœux une politique de recherche ambitieuse avec un doublement du budget du programme de recherche et d'innovation européen Horizon Europe.

Mme Catherine Morin-Desailly, rapporteure. – Cette proposition de résolution européenne répond à des interrogations justifiées compte tenu du contexte politique et international actuel. Comme vient de le rappeler Florence Blatrix Contat, cette proposition fait aussi écho au travail que nous menons depuis longtemps au sein de notre commission. En accord avec sa philosophie générale, nous vous proposons néanmoins plusieurs modifications et ajouts pour renforcer la portée du texte.

Le premier axe de nos recommandations est d'appliquer sereinement et fermement la réglementation en vigueur. Nous demandons ainsi fermement à la Commission européenne de faire preuve de diligence dans ses enquêtes ouvertes au titre du DSA et d'examiner les possibilités même de suspension des services défaillants dans le cadre du mécanisme de gestion de crise que ce texte prévoit. Je rappelle que deux pays ont suspendu TikTok et X, à savoir l'Inde et le Brésil, respectivement. Visiblement, ils ont obtenu des résultats. Nous rappelons aussi que certaines dérives constatées, comme le fait de laisser

des contenus illicites sur Internet ou de favoriser des ingérences étrangères, sont en France pénalement répréhensibles. Le fondateur de la messagerie Telegram, M. Pavel Durov, l'a appris à ses dépens, puisqu'il a été mis en examen en août dernier et qu'il est aujourd'hui passible de 10 ans de prison pour une douzaine d'infractions liées au maintien de contenus illicites et au refus de coopération avec les autorités judiciaires.

Le deuxième axe de nos recommandations consiste à mieux protéger nos démocraties européennes. Comment ? En luttant contre les ingérences étrangères et les tentatives de déstabilisation de nos sociétés, en nous dotant clairement des outils concrets. Le DSA, comme nous le signalions déjà avec Florence Blatrix Contat en 2021, comporte des lacunes. Certes, ce texte constitue un premier pas prometteur et attendu qui a permis de poser les règles et les principes de l'Union européenne, mais il faut constater, un an après son entrée en vigueur, que ce texte n'est sans doute pas aussi dissuasif que nous l'aurions souhaité.

Nous vous proposons donc plusieurs compléments à cette proposition de résolution européenne pour lutter contre les ingérences étrangères en matière numérique. Tout d'abord, il nous semble pertinent de renforcer l'efficacité des contrôles des très grandes plateformes en ligne en y associant de façon beaucoup plus importante les autorités de régulation nationales compétentes. Au titre du DSA, c'est l'autorité de régulation du pays dans lequel la plateforme a son siège, en général l'Irlande, qui est en première ligne, avec la Commission européenne, sur les contrôles et les enquêtes. Les autorités de régulation des autres pays, l'ARCOM en France, sont peu ou pas assez associées, alors même qu'elles participent aux réunions du Comité européen pour les services numériques et qu'elles peuvent transmettre à la Commission européenne des plaintes et des signalements sur les décisions et contenus des très grandes plateformes en ligne. De plus, au fil des années, les autorités de régulation nationales, plus proches des acteurs de terrain du numérique, ont bâti, il faut le dire, des expertises sectorielles précieuses qu'il convient de ne pas négliger.

Il n'est ni logique ni pertinent de fonctionner de façon aussi cloisonnée. Aussi, nous proposons d'ajouter dans le dispositif une meilleure association des contrôleurs nationaux aux enquêtes de la Commission européenne sur les agissements des très grandes plateformes en ligne. Nous vous proposons également de renforcer la coopération européenne en créant un réseau de veille et de détection des ingérences étrangères numériques, souple et décentralisé, rassemblant les services et agences des États membres en charge de la lutte contre les ingérences étrangères en ligne, quand elles existent, comme notre Viginum français. Car, et je crois que nous pouvons vraiment en être fiers, Viginum fonctionne bien. Ce centre d'expertise européen n'aurait pas vocation à remplacer les structures nationales, bien sûr, mais serait un outil de coopération entre celles-ci. À cet égard, si de nombreux pays cherchent à créer une entité comme Viginum à leur échelle, sachez que

pour l'instant, seuls deux pays membres de l'Union européenne disposent d'une telle structure. Il s'agit de la France et de la Suède. Ce système de vigilance et de détection des ingérences étrangères permettrait d'accroître les moyens et la visibilité du système d'alerte rapide, dont l'embryon existe déjà au sein du service européen pour l'action extérieure, auquel participe Viginum, afin de diffuser au plus vite les informations relatives à une tentative d'ingérence.

Par ailleurs, il faut revoir le régime de responsabilité des fournisseurs de services sur les contenus hébergés. Nous demandions déjà dans notre résolution européenne sur le DSA, il y a trois ans, d'aller plus loin car le statut d'hébergeur ne reflète pas le caractère actif des plateformes alors même qu'elles jouent bien un rôle de sélection des contenus par les algorithmes d'ordonnancement en augmentant la visibilité de certains au détriment d'autres, sur la base de paramètres déterminés par elles et dans leur intérêt. Je vous rappelle encore une fois que ces plateformes fonctionnent sur l'accumulation de très grandes masses de données, principalement des données personnelles. Elles sont exploitées par ces algorithmes de recommandation des contenus et d'adressage de la publicité. Leur objectif est d'inciter les utilisateurs à passer le plus de temps possible sur leurs réseaux sociaux car cela génère forcément du contenu pour ces dernières. Un tel processus conduit à enfermer les utilisateurs dans des « bulles de contenus » qui peuvent avoir des conséquences graves sur les comportements commerciaux, sociaux ou politiques. C'est un modèle pervers, qui est fondé exclusivement sur la profitabilité.

Je rappelle que Mme Frances Haugen, lanceuse d'alerte et ancienne ingénieure chez Facebook, lorsqu'elle a été entendue au Sénat le 10 novembre 2021, nous avait mis en garde : « Attention, malgré la régulation, les plateformes privilégieront toujours le profit à la sécurité des enfants. »

Face à ce constat inquiétant, la maîtrise des données personnelles est une première étape. Dans la droite ligne du RGPD, nous appelons à réformer le régime européen de responsabilité des fournisseurs de services en ligne et à créer un régime renforcé pour les plateformes qui utilisent ces algorithmes d'ordonnancement, proche de celui des éditeurs de contenu.

Mme Florence Blatrix Contat, rapporteure. – Nous souhaitons aussi favoriser la création d'une offre alternative aux GAFAM en encourageant, au niveau européen, la création de plateformes souveraines fondées sur des règles éthiques rigoureuses. Déjà, dans la résolution sur le DSA, nous appelions à ce que les algorithmes respectent obligatoirement un socle minimal de normes éthiques intégrées dès l'étape du développement, selon le principe de *safety by design*, à savoir, sécurité dès la conception. À défaut de trouver dans les GAFAM ce préalable nécessaire, il est urgent de créer des plateformes européennes conformes à nos valeurs.

Enfin, je veux insister sur deux points sur lesquels tant les États membres que les institutions de l'Union européenne peuvent agir pour rendre le respect des données plus effectif. Tout d'abord, le droit à la portabilité des données permet à un utilisateur de quitter une plateforme pour une autre avec une copie de ses données personnelles et l'obligation d'interopérabilité, c'est-à-dire l'obligation d'échanger des informations et de les utiliser. Or, cette obligation ne concerne pas les réseaux sociaux, ce qui limite la possibilité laissée aux utilisateurs de reprendre le contrôle sur leurs données. Peut-être les choses vont-elles évoluer puisque la Cour de justice de l'Union européenne a récemment jugé que le refus d'une entreprise en position dominante d'assurer l'interopérabilité de sa plateforme avec une application développée par une entreprise tierce peut constituer un abus de position dominante. Nous avons donc une première piste.

On peut ajouter à cela l'interopérabilité des algorithmes qui permettrait à tout utilisateur de pouvoir choisir les produits, les applications qu'il souhaite utiliser, quelles que soient les fonctionnalités présentes dans le système d'exploitation.

Le troisième axe sur lequel nous souhaitons insister est la nécessité de redoubler d'efforts pour bâtir une souveraineté européenne en matière numérique. La France et l'Union européenne regorgent d'entreprises talentueuses. Nous devons les soutenir dans leurs projets et dans leur développement.

Je citerai à nouveau M. Bernard Benhamou qui, le 30 janvier dernier, devant notre commission, a eu cette phrase choc : « Si nous ne prenons pas des mesures pour accompagner le développement de nos propres technologies stratégiques, au premier rang desquelles figure l'IA, nous nous enfermerons dans ce que certains analystes désignent déjà comme une « trappe à médiocrité technologique » qui semble caractériser l'Europe ces dernières années. » Nous appelons l'Union européenne à se mobiliser pour faire émerger des infrastructures nécessaires au développement du numérique : le quantique, l'*open source*, les semi-conducteurs, le *cloud computing*, les supercalculateurs.

Sur ce point, il n'est pas inutile de rappeler que le programme de travail de l'Union européenne pour 2025, que nous examinerons la semaine prochaine, prévoit des mesures sur les fabriques d'IA et une stratégie sur le quantique. Le numérique doit également être placé au rang des priorités budgétaires lors des négociations du prochain cadre financier pluriannuel de l'Union européenne. À cet égard, nous confirmons notre soutien à la proposition de doubler le budget de recherche et d'innovation européenne, Horizon Europe, afin de répondre aux défis de l'IA et du quantique.

Mais il faut aussi mobiliser, et c'est important, la commande publique. Nous ne l'avons pas suffisamment fait ces dernières années. À cet égard, la réforme annoncée de la directive sur les marchés publics en 2026 devrait

permettre aux États membres d'activer ce levier de la commande publique pour favoriser la politique industrielle européenne. Mme von der Leyen a d'ores et déjà annoncé, lors de la présentation de ses orientations politiques en juillet 2024, une révision de la directive sur les marchés publics afin de donner la préférence aux produits européens dans les marchés publics pour certains secteurs stratégiques. Nous nous en réjouissons et invitons la Commission à intégrer le secteur du numérique à la notion de secteur stratégique dans le cadre de cette révision qui devrait intervenir l'année prochaine.

Je voudrais rappeler que la commande publique représente environ 16 % du PIB de l'Union européenne. C'est donc un outil stratégique essentiel au service de l'ambition numérique européenne, dont l'importance nous a été rappelée à plusieurs reprises lors des auditions que nous avons menées. Cependant, le choix par des organes publics européens de prestataires ayant leur établissement dans un pays tiers et déjà dominants dans le secteur concerné, au titre de l'offre économique la plus avantageuse, n'est pas satisfaisant car il empêche la consolidation d'un écosystème numérique européen durable. Nous devons nous donner les moyens d'être acteurs de notre développement, comme nous l'avons rappelé dans notre rapport sur l'euro numérique où la préfiguration menée par la Banque centrale européenne (BCE) reposait sur le groupe Amazon.

Voilà, mes chers collègues, les éléments que nous souhaitions vous apporter concernant ce texte. Nous nous sommes attachées à vous présenter nos propositions de façon la plus sereine possible, sans nous laisser emporter par les dérapages médiatiques des uns et des autres sur les réseaux sociaux. Nous sommes persuadés que l'Union européenne dispose de bons textes, mais qu'il sera certainement nécessaire de les étoffer, et sur lesquels il ne faudra pas transiger, car ils sont conformes à nos valeurs et à nos principes. Je vous remercie.

M. Jean-François Rapin, président. – Merci pour toutes les précisions apportées au texte. Je voudrais remercier les auteurs de la proposition de résolution, parce que nous avons eu des discussions préalables importantes, et tout le monde a su faire un pas pour parvenir à un consensus. Merci également à nos deux rapporteures qui m'ont informé au fur et à mesure de l'avancée de leur travail. Je sais qu'il a été mené avec grand soin et grande expertise. C'est tout l'intérêt de notre commission d'avoir des personnes pointues dans tous les domaines qui touchent à l'Union européenne.

J'avais tenu à ce que notre commission puisse entendre l'ancien commissaire européen Thierry Breton sur l'évolution de la gestion des politiques numériques par l'Union européenne. Cette audition a été éclairante. J'ai aussi été sensible au discours des ministres lors de notre échange de mardi dernier, qui allait plus loin que le texte que vous alliez proposer. Ils nous ont avertis qu'il y avait un réel danger et qu'il nous fallait être très attentifs sur ce dossier. La France va de nouveau entrer dans une période électorale, en

particulier avec les élections municipales de 2026. Nous pouvons supposer que certains acteurs hostiles tenteront de perturber ces élections.

M. Thierry Breton nous a confirmé que l'Union européenne disposait désormais des outils pour réglementer le numérique et qu'il fallait les utiliser au mieux. Selon lui, dans sa « faiblesse bienveillante », l'Union européenne n'a sans doute pas voulu les mettre en œuvre intégralement. Le moment est donc opportun pour rappeler à l'Union européenne de faire preuve de lucidité et de courage.

M. Dominique de Legge. – Je vous remercie pour vos travaux, qui confortent ceux de la commission d'enquête sur les ingérences étrangères, que j'ai eu l'honneur de présider.

Permettez-moi de revenir sur le considérant 29 qui évoque des manipulations de l'information qui peuvent s'immiscer dans les processus démocratiques de l'Union européenne. Monsieur le Président, vous venez d'évoquer un risque de manipulation lors des prochaines élections municipales. Je pense donc, tout comme vous, que ce risque ne concerne pas seulement le processus démocratique européen, mais également ceux des États membres. Donc, je suggère que l'on puisse rajouter dans ce considérant le membre de phrase « et des États membres ».

Il en est ainsi décidé.

M. Didier Marie. – Je voudrais remercier nos rapporteures pour le travail réalisé, toujours dans des délais contraints – c'est tout le problème du dépôt de ces PPRE, dont on a pu parler dans le cadre de la révision en cours du Règlement du Sénat.

Mon groupe avait déposé cette proposition de résolution européenne au regard du contexte international et du contexte politique européen. Je voudrais à mon tour remercier le ministre Barrot qui, à la suite de mon interpellation mardi soir, a complété et précisé la position du gouvernement, ce qui vous a amené à adopter une rédaction plus ferme sur certains sujets.

Depuis plusieurs années, vous l'avez dit, certains acteurs étatiques utilisent les réseaux sociaux pour tenter de déstabiliser nos démocraties en multipliant les fausses informations et les ingérences. Depuis quelques mois, nous assistons, impuissants, à une accélération de ces agissements, non plus seulement par des États hostiles, mais par des plateformes ultradominantes qui se servent de leurs infrastructures mondialisées pour disséminer de fausses informations et servir une idéologie réactionnaire.

Ces agents politiques, nous avons pu les voir à l'œuvre, en Roumanie lors de la dernière élection présidentielle, en Allemagne, récemment, où la plateforme X a soutenu très ouvertement l'AFD, ou encore en Nouvelle-Calédonie, dans le cadre d'une opération de déstabilisation menée par l'Azerbaïdjan. Face à ces mastodontes numériques mal intentionnés,

aucun de nos pays ne dispose d'une plateforme ou d'une infrastructure de même nature.

L'Union européenne, il faut malheureusement le souligner, a échoué à établir une stratégie économique claire dans le numérique et s'est révélée incapable d'aider à l'émergence d'acteurs de premier plan, laissant le champ ouvert à ces mastodontes que je citais. Cette déficience européenne se traduit par une dégradation dramatique de la diversité des médias, du débat public et de la participation démocratique.

Face à ces menaces pour l'intégrité de nos systèmes démocratiques et pour la liberté des citoyens, il est indispensable que l'Europe défende son modèle de régulation et soit capable de s'opposer à toute tentative d'ingérence. Cela implique l'application stricte des règles et des sanctions existantes, le renforcement de notre arsenal législatif face au contournement de celles-ci, mais aussi que l'Union européenne se dote des outils permettant de compenser le désavantage qui frappe les acteurs européens face aux géants étrangers et facilite l'émergence de champions européens.

En déposant cette proposition de résolution européenne, notre groupe a réaffirmé son engagement pour une Europe forte, une Europe souveraine et actrice de la transformation numérique. Je me réjouis avec mes collègues que les conclusions des travaux qui ont été menés par nos deux rapporteures confirment l'ensemble des propositions que nous avons faites, soulignant aussi la qualité de la réflexion menée. Nous exprimons notre satisfaction au sujet du travail réalisé.

Nous soutenons par ailleurs le renforcement d'un certain nombre de propositions qui ont été présentées à l'instant par les deux rapporteures, d'autant qu'un travail commun avait été mené en amont sur ces sujets. Je me félicite tout d'abord qu'on insiste sur la dénonciation de la lenteur des enquêtes menées aujourd'hui par l'Union européenne et la non-utilisation du panel des possibilités de sanctions. Il faut, y compris dans ce domaine, faire preuve de dissuasion à l'égard des acteurs qui agissent contre nos intérêts.

Je me réjouis aussi de la réintroduction de la nécessité de mobiliser des moyens financiers conséquents et donc du doublement du budget d'Horizon Europe, parce que l'Union européenne aura besoin d'un budget solide pour combler son retard technologique et favoriser la compétitivité européenne. Elle est, dans ce domaine, encore trop frileuse.

De même, nous soutenons pleinement ce qui est mentionné quant à la création de plateformes éthiques et souveraines pour constituer une alternative aux réseaux sociaux existants et permettre l'émergence d'acteurs européens qui puissent jouer leur rôle à l'échelle européenne et mondiale.

Enfin, on peut s'interroger sur l'opportunité de demander à la Commission européenne d'engager de nouvelles initiatives législatives pour compléter le dispositif, afin que ces points que nous évoquons n'en restent pas au stade des bonnes intentions, mais puissent effectivement être actés dans le

temps. Cette PPRE va permettre d'alerter la Commission et, je crois, l'inviter à aller plus loin et plus vite pour réguler les réseaux sociaux.

Ce texte porte un message politique fort à l'égard des acteurs du numérique, à l'égard desquels il nous faut réaffirmer l'importance de l'État de droit et la primauté de la régulation. La nouvelle Commission « von der Leyen II », dont on présentera le programme de travail la semaine prochaine, doit faire preuve de fermeté face aux géants du numérique. Il en va de l'autonomie économique de l'Union européenne ainsi que de la résilience de notre démocratie face à ce grand danger qui est celui de la manipulation de l'information et des ingérences.

M. Louis-Jean de Nicolaÿ. – Je voudrais à mon tour remercier les rapporteures parce que leur PPRE est très complète. Je pose toutefois les questions suivantes : que fait-on maintenant et comment le fait-on ?

J'ai été très intéressé par votre volonté de développer l'intelligence artificielle au niveau européen. Notre effort doit porter non seulement sur le développement des outils mais aussi sur la formation des personnes permettant de développer l'intelligence artificielle sur le continent européen, afin de relever le défi posé par les GAFAM qui, sinon, vont se développer encore plus, avec des algorithmes « inondant » l'ensemble du marché européen et mondial.

L'Europe a 450 millions d'habitants, mais nous sommes 7 milliards d'habitants sur la planète, donc il reste 6,5 milliards de personnes qui, si je puis dire, ne dépendent pas du marché européen. Il nous faut protéger notre marché. Mais, pour cela, l'Europe doit devenir un des principaux centres de la recherche mondiale dans les communications.

La PPRE me semble couvrir l'ensemble des actions qu'il faut mettre en place pour le moment, mais il nous faut insister sur l'importance des investissements à réaliser, non seulement par la Commission européenne, mais aussi par les États membres, ainsi que sur l'élaboration d'une stratégie de recherche et de développement de l'intelligence artificielle sur le territoire européen.

M. André Reichardt. **–** À mon tour, je voudrais remercier toutes celles et ceux qui ont travaillé sur cette proposition de résolution européenne. Je trouve que ce texte, que je voterai naturellement, est particulièrement bien construit. Il vise, comme son titre l'indique, d'abord à une application rigoureuse du cadre réglementaire existant à l'heure actuelle. Il appelle aussi au renforcement des conditions permettant de cheminer vers une réelle souveraineté numérique européenne.

J'ai été sensible à ce qui a été dit sur l'ambiguïté des décisions de la Commission européenne en matière de respect du cadre réglementaire existant. Nous avons en effet tous en tête des propositions de réglementation européennes présentées à grand renfort de communication et que la Commission, par la suite, peine à faire respecter. Elle n'est pas toujours à la

hauteur de ce que l'on pourrait attendre pour défendre effectivement ce cadre réglementaire.

Avec Catherine Morin-Desailly, en 2023, nous avions travaillé sur une proposition de règlement importante qui devait renforcer la lutte contre les abus sexuels sur les mineurs en ligne. Or, en lisant la proposition de résolution, malgré l'urgence de l'adoption de la réforme telle qu'elle avait été indiquée au départ, je comprends que les négociations sur ce projet demeurent bloquées. Pourriez-vous me préciser où nous en sommes véritablement ? Pour moi, c'est une illustration du fait que cette Commission européenne parle beaucoup, mais agit peu.

Il en va de même sur la boussole numérique. Il y a eu beaucoup d'annonces et un concept nouveau. Mais alors qu'il y avait l'obligation d'avancer très vite et de mobiliser tous les financements, où en sommes-nous ?

Enfin, s'agissant de la souveraineté numérique, je voudrais vous faire part de mes interrogations. Vous demandez à la Commission européenne de créer les conditions permettant l'émergence d'acteurs numériques européens afin d'assurer un contrôle, une localisation et une exploitation des données conformes à la législation européenne, ainsi qu'une information fiable et sourcée. C'est très bien car en effet, en principe, il faudrait aller vers des acteurs numériques européens qui apportent les garanties que n'apportent pas les acteurs actuels. Mais, en pratique, croyez-vous qu'une telle évolution soit possible dans une Union européenne qui, à l'heure actuelle, est composée d'États membres qui visent essentiellement à protéger leurs propres intérêts sur le plan économique et social ?

Mme Audrey Linkenheld. – Je souscris au contenu de cette proposition de résolution, à la fois travaillée par Didier Marie et améliorée, complétée par les rapporteures.

Cela montre encore une fois le besoin d'une réglementation européenne sur ces sujets cyber, et, plus largement, numériques. Nous avons eu l'occasion, avec nos collègues Catherine Morin-Desailly et Cyril Pellevat, de souligner l'enchevêtrement de cette réglementation européenne dans le domaine de la cybersécurité. Certains textes européens fraîchement adoptés ne sont même pas encore appliqués que la Commission européenne propose déjà de nouveaux textes. Simultanément, la cybermenace est bien réelle et s'accélère.

Or, l'Europe a du mal à suivre et, quand elle le fait, elle ne le fait pas toujours correctement, avec des difficultés pour l'ensemble des acteurs à suivre le mouvement. Il nous faut bien sûr des réglementations, mais veillons également à ce qu'elles soient cohérentes sur le fond et, surtout, à ce qu'elles soient effectivement appliquées une fois adoptées. Cette PPRE a aussi la vertu de rappeler qu'il y a le besoin de faire et la manière de faire.

Je me permets simplement de faire une petite remarque formelle sur le considérant 40. Je trouve qu'une formulation mériterait un amendement

rédactionnel. Il est écrit que le Sénat « rejette » les attaques formulées par les responsables de plateformes contre les règles européennes. Je propose plutôt d'écrire que le Sénat les « conteste » ou les « réfute ».

Il est décidé de remplacer « rejette » par « conteste ».

Mme Mathilde Ollivier. **–** Cette proposition de résolution européenne arrive à point nommé, dans ce moment de bascule et de réflexion globale sur les interdépendances et les points de vulnérabilité de l'Union européenne dans tous les domaines. Il est donc important de travailler à notre indépendance stratégique.

Je voudrais revenir sur trois points. D'abord, je trouve important que vous ayez pu parler dans cette résolution de la liberté d'expression et de notre attachement à cette liberté, dans une période où certains acteurs et personnalités politiques sont tentés de donner un blanc-seing à la propagation de propos racistes, homophobes et anti-scientifiques sur les plateformes au nom de cette liberté. On se rappelle il y a quelques années de Mark Zuckerberg se tournant vers les familles de victimes de jeunes enfants et adolescents qui s'étaient suicidés, et qui leur disait : « Je m'excuse, nous allons travailler sur la réglementation et la régulation de nos plateformes. » Aujourd'hui, quelques années plus tard, il nous annonce qu'il est en train de retirer toute la réglementation et toute la régulation de ces plateformes.

Nous avons donc ici absolument besoin de travailler sur la mise en œuvre des règles que nous nous sommes fixées à l'échelle européenne et de ne pas courber l'échine ou, en tout cas, ne pas se laisser faire face au comportement de certains de ces acteurs américains. Vous êtes plusieurs à avoir mentionné les propos marquants du ministre lors de nos échanges mardi. Il a évoqué la frilosité des commissaires à agir de peur de recours devant la Cour de justice de l'Union européenne (CJUE). Voilà pourquoi cette résolution est importante. Nous avons besoin d'actions fortes de l'Union européenne, nous ne devons pas avoir peur face à ces acteurs américains qui ne respectent pas forcément nos règles.

Un dernier point qui me semble important : vous avez parlé de l'importance d'avoir un doublement, dans le prochain cadre financier pluriannuel, du budget d'Horizon Europe. Cela devait déjà être le cas en 2017, lorsqu'on discutait du passage d'Horizon 2020 à Horizon Europe. Il y avait des discussions autour du développement du deuxième pilier d'Horizon Europe, notamment sur le *European Innovation Council (EIC)*, au sujet de l'importance d'investissements publics qui doivent s'adosser à des financements privés, en particulier pour les « licornes » dans le domaine du numérique. Les innovations numériques ont besoin de s'appuyer sur une base de financement public, notamment dans les premières phases de développement, mais doivent aussi pouvoir s'appuyer sur des fonds privés ou sur des fonds d'investissement.

Lorsque nous discuterons du prochain CFP et du prochain budget d'Horizon Europe, il sera important de faire le bilan de ces budgets et de ces financements que nous avons essayé de mettre en place en faveur de l'innovation en Europe. Il faudra alors s'interroger sur deux points : ces politiques ont-elles fonctionné ; comment allons-nous aujourd'hui convaincre les acteurs privés qui doivent investir dans la recherche ?

Mme Florence Blatrix Contat, rapporteure. – Il est exact que cette PPRE tombe vraiment au bon moment. On l'a vu avant-hier lorsqu'on a rencontré nos homologues de l'Assemblée nationale, qui ont aussi effectué un travail sur le sujet. Il était important que le Sénat puisse se saisir de cette problématique.

Je partage évidemment toutes les analyses de Didier Marie, qui vont dans le sens de nos propositions. Sur l'évolution du DSA, il nous faudra aller plus loin mais, sans attendre, la Commission européenne doit agir plus vite et plus fermement.

Le développement de l'intelligence artificielle est vraiment essentiel. Plusieurs programmes européens sont prévus à ce sujet. Le sommet pour l'action sur l'intelligence artificielle s'est tenu à Paris le 11 février dernier. À cette occasion, plusieurs projets de financement ont été annoncés. Pour la Commission européenne, c'est vraiment une priorité politique.

S'agissant de la boussole numérique, je crois qu'on peut dire que les objectifs n'ont pas été atteints. Voilà pourquoi la proposition de résolution recommande de relancer ce processus.

Quant à savoir si nous croyons à nos propositions, ma réponse est évidemment affirmative. Il me semble que nous n'avons pas le choix ! Le Président de la République a indiqué que nous entrions dans une économie de guerre, alors tirons-en les conséquences. La guerre informationnelle fait partie de la guerre et l'espace public est un des champs de la guerre. Nous devons donc reprendre notre souveraineté dans ce domaine.

Lors de son audition, M. Bruno Patino nous a indiqué que l'Union européenne avait sans doute perdu la partie pour établir des plateformes européennes du type de Meta ou X. Simultanément, il a souligné que la question de l'interopérabilité des plateformes était essentielle pour que des offres alternatives puissent se développer. Il a également évoqué deux domaines clés dans lesquels l'Europe aurait intérêt à investir car elle peut encore construire son propre modèle : les messageries privées et l'IA conversationnelle.

Il est absolument essentiel, pour les États membres et l'Union européenne, de décider de financements crédibles pour Horizon Europe si nous voulons bâtir cette souveraineté numérique. A l'heure où il est question d'exclure les dépenses de défense des règles du pacte de stabilité et de croissance, peut-être devrions-nous considérer les dépenses en faveur de notre souveraineté numérique comme faisant partie de nos efforts de défense.

Mme Catherine Morin-Desailly, rapporteure. – Je souhaite en quelques mots compléter les propos de Florence Blatrix Contat, en précisant tout d'abord qu'une partie de nos propositions émane des conclusions des États généraux de l'information, dont nous avons auditionné au moins deux acteurs : Bruno Patino et David Colon. Par cohérence, je vous propose, si vous en êtes d'accord, que nous mentionnions ces travaux parmi les visas de notre proposition.

Il en est ainsi décidé.

Plusieurs interventions, à juste titre, se demandaient si nous avons les moyens de nos ambitions. Mais les moyens, il faut se les donner ! Il nous faut établir des plateformes éthiques, par exemple dans le cadre de la réforme à venir des audiovisuels publics européens. Il nous faut prendre acte de l'évolution des pratiques : en 2025, on ne regarde plus la télévision de façon linéaire comme autrefois. La télévision est désormais très souvent regardée en *replay* ou *via* les réseaux sociaux. Si ces acteurs audiovisuels publics partageaient leurs contenus sur une plateforme commune directement consultable, plutôt que passer par les réseaux extérieurs, ce serait de l'argent public bien utilisé et qui ne dépendrait pas des algorithmes d'ordonnancement privilégiant telle information plutôt que telle autre, tel contenu plutôt que tel autre. Ces modèles alternatifs pourraient être financés par la puissance publique et par des acteurs privés. L'ambition de l'alliance du public et du privé est ici tout à fait nécessaire. Il est probable qu'à un moment donné, les citoyens en auront assez d'être « lobotomisés », d'être « saoulés » et manipulés par les grandes plateformes en ligne, et qu'ils chercheront alors d'autres outils pour se documenter et converser les uns avec les autres, quitte à payer un abonnement.

Je vous confirme qu'au cours des dernières années, il y a eu un empilement, une succession rapprochée de textes sur le numérique parce qu'auparavant, il n'y avait aucune réglementation européenne. Tout restait à faire. Ce n'est pas faute d'avoir demandé cette réglementation dès 2015, lorsque j'étais rapporteure de la mission commune d'information du Sénat sur la gouvernance de l'internet, qui était présidée par Gaëtan Gorce. Nous avions alors formulé 50 propositions pour bâtir ce cadre, qui auraient pu être mises en œuvre progressivement. Si tel avait été le cas, nous ne serions sans doute pas dans cette situation de dépendance aujourd'hui. Dans nos recommandations, nous demandions une politique industrielle du numérique. Faute d'avoir tiré ces leçons, aujourd'hui, l'Europe régule plus qu'elle n'innove et cette situation est moquée par nombre d'acteurs du numérique et de représentants de pays tiers. Or, cette politique industrielle puissante et volontaire, qui privilégie nos propres acteurs, est une condition de notre autonomie stratégique.

Nous avons aussi souligné l'importance du levier de la commande publique. Depuis plusieurs années, nous répétons que nos secteurs stratégiques doivent être confiés à des entreprises européennes et françaises.

C'est par le levier de la commande publique que les Russes, les Chinois et les Américains ont développé leur propre secteur.

Concernant la boussole numérique, le rapport que nous avions fait devant notre commission pointait déjà les carences de ce texte, qui énonçait de bonnes intentions, d'ailleurs, dans une approche transversale, mais ne donnait aucun moyen financier et ne créait aucun dispositif incitatif à des associations volontaires, qui conjugueraient aides nationales et aides européennes dans une perspective stratégique mêlant recherche, développement et soutien aux entreprises, commandes publiques et développement de secteurs très ciblés.

Pour le *cloud*, nous avions défendu l'idée d'un soutien aux développeurs de *cloud* français et européens et pourtant, cette préconisation ne s'est pas retrouvée dans la boussole numérique. Cela nous confirme qu'il faut revoir les façons de travailler dans les institutions européennes.

Le débat en séance publique qui a eu lieu hier sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité a souligné, à juste titre, que la nouvelle réglementation donnait un cadre de résilience à nos propres entreprises et à nos collectivités, à charge pour elles de solliciter des solutions souveraines pour s'équiper, être résilientes et se protéger. Il existe ainsi une immense opportunité, par effet de ruissellement, pour développer la filière cyber française et européenne. C'est une occasion à ne pas rater pour construire enfin notre autonomie stratégique. Je voudrais vous rappeler que si M. Donald Trump est parfois qualifié d'agent du Kremlin, c'est que la première des ingérences étrangères constatées, à savoir, l'affaire Cambridge Analytica en 2016, avait permis à la Russie de profiter des carences de Facebook et de Cambridge Analytica pour manipuler les élections américaines.

Enfin, le projet de règlement visant à lutter contre les abus sexuels sur les mineurs en ligne est effectivement bloqué au niveau du Conseil parce que les États membres n'arrivent pas à se mettre d'accord sur le sujet complexe de l'ouverture ou non des messageries aux services d'enquête. L'Allemagne et les Pays-Bas bloquent toujours sur cette question parce qu'ils défendent un respect absolu de la vie privée. Jusqu'où est-il possible et efficace d'aller dans la création de « portes dérobées » dans les messageries et dans le contenu des plateformes ? En effet, avec une telle « porte dérobée » dans nos téléphones, nos données ne seraient plus chiffrées. Cela signifie qu'il serait beaucoup plus simple, pour les services d'enquête, de repérer et d'appréhender un délinquant ou un narcotrafiquant, mais que chacun d'entre nous serait aussi plus vulnérable aux actions de collecte de nos données menées par des puissances étrangères, des services de renseignement ou le crime organisé. Ce sujet-là est donc en suspens mais, dans l'esprit de notre résolution européenne de 2023, les États membres doivent trouver une solution permettant de mettre fin à ces abus inacceptables.

M. Jean-François Rapin, président. – Concernant la question des atteintes et des abus sexuels sur enfants, c'était un thème important de discussion lors de la dernière réunion du groupe de contrôle parlementaire conjoint d'Europol à Varsovie, à laquelle j'ai assisté avec la présidente de la commission des lois, notre collègue Muriel Jourda. Europol a en effet mis en œuvre des moyens conséquents pour aider les services de police des États membres à faire face à ce fléau, le plus souvent lié à des réseaux de crime organisé.

PROPOSITION DE RÉSOLUTION EUROPÉENNE

(1) Le Sénat,

(2) Vu l'article 88-4 de la Constitution,

(3) Vu le traité sur le fonctionnement de l'Union européenne (TFUE), et notamment son article 114,

(4) Vu la charte des droits fondamentaux de l'Union européenne,

(5) Vu la Convention de sauvegarde des droits de l'homme et des libertés fondamentales,

(6) Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), dit « RGPD »,

(7) Vu le règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques ou *Digital Markets Act* (DMA)),

(8) Vu le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques ou *Digital Services Act* (DSA)),

(9) Vu la recommandation (UE) 2023/2829 de la Commission du 12 décembre 2023 relative à des processus électoraux inclusifs et résilients dans l'Union, au renforcement du caractère européen des élections au Parlement européen et à une meilleure garantie de leur bon déroulement,

(10) Vu les lignes directrices de la Commission à l'intention des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sur l'atténuation des risques systémiques pour les processus électoraux, présentées en vertu de l'article 35, paragraphe 3, du règlement (UE) 2022/2065 (Texte présentant de l'intérêt pour l'EEE) (C/2024/3014),

(11) Vu la procédure formelle ouverte par la Commission européenne le 18 décembre 2023 à l'encontre du réseau social X visant à évaluer s'il a pu enfreindre le règlement DSA concernant l'utilisation de l'algorithme, les risques liés à la diffusion de contenus illégaux tels que les discours de haine et les contenus terroristes, les risques liés au débat public et aux processus électoraux, les obligations de transparence concernant les

publicités diffusées et l'accès aux données de la plateforme pour les chercheurs,

(12) Vu les constatations préliminaires adressées par la Commission européenne à X le 12 juillet 2024 dans le cadre de cette même procédure,

(13) Vu le programme stratégique de l'Union européenne pour la période 2024-2029,

(14) Vu les orientations politiques pour la Commission européenne pour 2024-2029,

(15) Vu la feuille de route de la vice-présidente exécutive de la Commission européenne, chargée de la souveraineté, de la sécurité et de la démocratie dans le domaine de la technologie,

(16) Vu les rapports de la commission spéciale du Parlement européen INGE 1 et INGE 2 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation,

(17) Vu le rapport de M. Enrico Letta, intitulé « Much more than a market – Speed, security, solidarity – Empowering the Single Market to deliver a sustainable future and prosperity for all EU citizens », publié en avril 2024,

(18) Vu le rapport de M. Mario Draghi, du 9 septembre 2024, sur le futur de la compétitivité européenne et une stratégie de compétitivité pour l'Europe,

(19) Vu le rapport « L'Europe, colonie du monde numérique ? » n°443 (2011-2012) de Mme Catherine Morin-Desailly au nom de la commission des affaires européennes,

(20) Vu le rapport d'information du Sénat n°696 (2013-2014) 8 juillet 2014 « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet » de Mme Catherine Morin-Desailly, fait au nom de la mission commune d'information du Sénat sur la gouvernance de l'Internet, ainsi que la résolution européenne n°122 (2014-2015),

(21) Vu les conclusions du rapport du Sénat n° 7 (2019-2020) du 1er octobre 2019, intitulé « Le devoir de souveraineté numérique : ni résignation, ni naïveté », fait au nom de la commission d'enquête sur la souveraineté numérique,

(22) Vu les conclusions du rapport d'information du Sénat n° 831 (2022-2023) du 4 juillet 2023, intitulé « La tactique Tiktok : opacité, addiction et ombres chinoises », fait au nom de la commission d'enquête sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence,

(23) Vu les conclusions du rapport d'information du Sénat n° 739 (2023-2024) du 23 juillet 2024, intitulé « Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la nation face à la néo-guerre froide », fait au nom de la commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères visant notre vie démocratique, notre économie et les intérêts de la France sur le territoire national et à l'étranger afin de doter notre législation et nos pratiques de moyens d'entraves efficients pour contrecarrer les actions hostiles à notre souveraineté,

(24) Vu la résolution européenne n° 138 (2021-2022) du Sénat du 22 juillet 2022 sur le programme d'action numérique de l'Union européenne à l'horizon 2030,

(25) Vu le rapport d'information du Sénat n° 274 (2021-2022) du 8 décembre 2021, intitulé « Amplifier la législation européenne sur les services numériques (DSA), pour sécuriser l'environnement en ligne », fait au nom de la commission des affaires européennes,

(26) Vu la résolution européenne du Sénat n° 70 (2021-2022) du 14 janvier 2022 sur la proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numérique (Législation sur les services numériques – Digital Services Act – DSA) et modifiant la directive 2000/31/CE, COM(2020) 825 final,

(27) Vu le rapport des États généraux de l'information du 12 septembre 2024, intitulé « protéger et développer le droit à l'information : une urgence démocratique »,

(28) ***<u>Sur l'application des règles numériques européennes</u>***

(29) Considérant que la liberté d'expression est l'un des fondements essentiels d'une société démocratique, garantie par les constitutions des États membres, par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et par la charte européenne des droits fondamentaux, et qu'elle s'exerce dans les conditions prévues par la loi et dans le respect de l'État de droit ;

(30) Considérant que l'Union européenne et les États membres sont désormais régulièrement sous la menace d'ingérences étrangères et de campagnes de manipulation de l'information en ligne ;

(31) Considérant que des acteurs étatiques et non étatiques malveillants utilisent la manipulation de l'information et d'autres tactiques pour s'immiscer dans les processus démocratiques de l'Union et de ses États membres ;

(32) Considérant que l'opacité et l'utilisation des algorithmes des réseaux sociaux sont susceptibles d'être mises au service de ces ingérences et manipulations ;

(33) Considérant que le RGPD, le DMA et le DSA ont été adoptés pour constituer un cadre réglementaire robuste et cohérent, mais dont il reste encore à exploiter toutes les possibilités ;

(34) Considérant que pour mieux défendre les valeurs de l'Union européenne, le Conseil s'est fixé comme priorité, conformément au programme stratégique adopté pour 2024-2029, de renforcer la résilience et le débat démocratique, de protéger la liberté et le pluralisme des médias, de lutter contre l'ingérence étrangère et les tentatives de déstabilisation et de veiller à ce que les géants du numérique prennent leurs responsabilités pour ce qui est de préserver le débat démocratique en ligne ;

(35) Considérant la décision du Parlement européen de constituer le 13 décembre 2024 une commission spéciale sur le « bouclier européen de la démocratie » afin d'évaluer les politiques et mesures existantes et à mettre en place afin de renforcer l'action de l'Union européenne contre les menaces et attaques hybrides et contre la manipulation de l'information et l'ingérence intérieure et étrangère ;

(36) Considérant que les attaques portées contre le cadre de régulation numérique européen doivent faire l'objet d'une réponse forte, appropriée, et proportionnelle à la gravité des manquements constatés et des risques encourus pour la démocratie européenne et la stabilité en Europe ;

(37) Considérant en effet que ce cadre normatif, en particulier le RGPD, permet de protéger les données des sociétés démocratiques européennes et des citoyens, tout en permettant leur partage et leur valorisation sécurisés, et qu'il doit donc être préservé ;

(38) Considérant que les réseaux sociaux et les très grandes plateformes numériques bénéficient toujours d'une position asymétrique par rapport aux médias traditionnels, notamment en matière de réglementation de la publicité, ce qui leur procure un avantage concurrentiel décisif ;

(39) Considérant que le modèle économique des réseaux sociaux et des plateformes numériques, qui les incite à maximiser par tous les moyens le temps passé par les utilisateurs sur leurs services, jusqu'à porter atteinte à leur bien-être et leur sécurité, favorise la propagation de contenus extrêmes, y compris des discours de haine ou d'apologie du terrorisme ;

(40) Salue les efforts des États membres et de l'Union européenne qui ont permis, au cours des dernières années, de bâtir un cadre harmonisé de protection des données, et de régulation des marchés numériques et des services numériques ; constate que ce cadre normatif unique au monde est à la fois propice à l'innovation, respectueux des droits fondamentaux et propice à la recherche d'une autonomie stratégique ;

(41) Souligne le rôle pionnier du Sénat depuis de nombreuses années dans l'énonciation d'une nécessaire stratégie numérique européenne comprenant une régulation ambitieuse ;

(42) Conteste les attaques formulées par plusieurs responsables de plateformes en ligne contre les règles européennes sur le secteur numérique, et observe qu'elles traduisent moins une défense de la liberté d'expression qu'une volonté d'instauration de « la loi du plus fort » et de maximisation de leurs profits ;

(43) Rappelle que le marché numérique européen est le plus important au monde et que les entreprises du numérique qui souhaitent y mener leurs activités doivent en accepter les règles ;

(44) Appelle le Gouvernement et ses partenaires européens à privilégier la mise en œuvre intransigeante de ces règles, y compris les possibilités d'inspections, au maintien du modèle économique des grandes plateformes en ligne, qui constitue en lui-même un risque systémique majeur ;

(45) Demande au Gouvernement et à ses partenaires européens de s'assurer que les dispositions du DMA garantissant que les marchés numériques européens sont contestables et équitables, en particulier celles sanctionnant les abus de position dominante dans le secteur numérique, font bien l'objet d'une mise en œuvre rapide et efficace ;

(46) Souligne la pertinence du principe de portabilité des données, visé par le RGPD et le DMA, qui permet à un utilisateur de quitter une plateforme pour une autre avec une copie de ses données personnelles ;

(47) Demande l'application des dispositions de l'article 9 du RGPD, qui interdisent les traitements portant sur les données personnelles sensibles, sauf exceptions limitées, afin de désactiver les algorithmes de recommandation par défaut et obliger les plateformes en ligne à avertir soigneusement leurs utilisateurs et à leur demander explicitement leur consentement ;

(48) Dénonce l'abandon par plusieurs plateformes en ligne de leur politique de modération (*fact checking*) et demande à la Commission européenne de prendre les mesures nécessaires pour que ces règles continuent à s'appliquer conformément à la réglementation européenne ;

(49) Approuve l'intégration d'un code de conduite européen contre la haine en ligne illicite dans le DSA, opposable aux très grandes plateformes en ligne ;

(50) Constate que la Commission européenne a ouvert plusieurs enquêtes pour violation présumée du règlement sur les services numériques, en particulier, le 17 décembre 2024, contre le réseau TikTok, soupçonné d'avoir facilité une campagne de manipulation de l'information particulièrement grave lors du premier tour de l'élection présidentielle

en Roumanie qui a conduit la Cour constitutionnelle de ce pays à annuler ce scrutin, et contre le réseau X, le 18 décembre 2023 avec un approfondissement le 17 janvier 2025, au sujet de la diffusion de contenus illicites, des mesures prises par la plateforme pour lutter contre la manipulation de l'information et sur d'éventuels changements de son système de recommandation ; s'inquiète de la lenteur des enquêtes en cours et demande une grande diligence à la Commission européenne pour leur clôture ;

(51) Demande le renforcement et l'intensification du contrôle de l'application du DMA et du DSA), conformément aux engagements pris par la Commission européenne dans ses orientations politiques pour 2024-2029 et dans la feuille de route de Mme Henna Virkkunen, vice-présidente exécutive de la Commission chargée de la souveraineté, de la sécurité et de la démocratie dans le domaine de la technologie ;

(52) Salue la publication de rapports d'évaluation des risques et d'audits par les très grandes plateformes en ligne au titre du DSA ; demande que soient pleinement exploitées les dispositions de ce dernier prévoyant cette possibilité d'audit indépendant des très grandes plateformes en ligne, y compris concernant leurs algorithmes d'ordonnancement des contenus, l'accès des chercheurs aux données de ces plateformes, et la sanction des très grandes plateformes en ligne ayant commis des manquements ;

(53) S'interroge néanmoins sur la portée réellement dissuasive du montant maximal des amendes prévu (6 % du chiffre d'affaires mondial de la société concernée) au regard, d'une part, des bénéfices engendrés, pour les plateformes, par le non-respect des textes européens et, d'autre part, du préjudice causé au fonctionnement des démocraties européennes ;

(54) Demande fermement l'examen des possibilités de suspension des services défaillants dans le cadre du mécanisme de réaction aux crises, prévu à l'article 36 du règlement précité ;

(55) Rappelle que certaines dérives des plateformes peuvent aussi constituer des infractions pénales au titre du droit national ; à cet égard, souligne que, dans le code pénal français, le changement d'algorithmes par les plateformes en ligne ayant pour effet de favoriser des opérations d'ingérence étrangère est susceptible d'être assimilé au « *fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé des données*. », passible d'une peine de cinq ans d'emprisonnement et de 150 000 euros d'amende aux termes de l'article 323-2 de ce code ;

(56) Constate également que les enquêtes des services de police sur la criminalité en ligne peuvent se heurter à une coopération insuffisante des plateformes ; appelle le Gouvernement et ses partenaires européens à prendre les mesures nécessaires pour y mettre fin ;

(57) ***Sur le renforcement des outils de régulation des très grandes plateformes en ligne***

(58) L'instauration d'une interopérabilité entre les réseaux sociaux

(59) Rappelle que le DSA impose aux contrôleurs d'accès l'interopérabilité des caractéristiques matérielles et logicielles de leurs systèmes d'exploitation et, pour ceux qui fournissent des services de communication interpersonnelles non fondés sur la numérotation, celle de leurs fonctionnalités de base relatives aux messageries textuelles, au partage d'images, de messages vocaux, de vidéos, et d'appels vocaux et vidéos ; demande leur respect plein et entier par les plateformes concernées ;

(60) Demande, dans le respect du RGPD, l'actualisation du droit européen en vigueur en vue d'instaurer l'interopérabilité de l'ensemble des interfaces et des systèmes de recommandation des réseaux sociaux ayant le statut de contrôleur d'accès, afin d'assurer une libre concurrence entre eux, de redonner une capacité de choix aux utilisateurs et de faciliter la lutte contre les manipulations de l'information ;

L'encouragement à la création de plateformes éthiques et souveraines pour constituer une alternative aux réseaux sociaux

(61) Relève que l'impact des dérives constatées dans le fonctionnement des réseaux sociaux et des plateformes sur les démocraties européennes et sur la santé mentale de leurs utilisateurs, en particulier des jeunes, résulte de l'absence d'alternative à leur modèle basé sur la collecte massive de données personnelles ; encourage donc la création d'offres alternatives souveraines et éthiques (plateformes nationales ou transnationales de réseaux sociaux, de messagerie ou d'intelligence artificielle conversationnelle) garantissant un débat démocratique et sain, fondé sur un modèle économique différent de celui des plateformes ; insiste sur la nécessaire mobilisation des pouvoirs publics pour favoriser la mise en place de telles offres, en complément de la participation des entreprises et des citoyens soucieux de la qualité du débat public ; estime que la période de réforme de l'audiovisuel public est propice à la création de telles plateformes ;

Le « bouclier européen pour la démocratie » et le système de détection des ingérences étrangères au niveau européen

(62) Soutient l'adoption rapide du « bouclier européen pour la démocratie », annoncé par la Commission européenne, afin de lutter contre la manipulation de l'information et l'ingérence étrangère ;

(63) Salue l'efficacité du service français de vigilance et de protection contre les ingérences (Viginum) pour détecter au niveau national les ingérences étrangères en ligne ; constate simultanément qu'un tel dispositif fait défaut dans la majorité des autres États membres et dans les institutions

européennes ; dans le cadre du « bouclier européen pour la démocratie », souhaite en conséquence la constitution, autour de Viginum, d'un réseau « Vigie Europe » souple et opérationnel contre de telles ingérences, comprenant un système d'alerte rapide et un centre d'excellence favorisant l'échange de bonnes pratiques ;

Une responsabilité juridique renforcée des plateformes

(64) Constate tout d'abord que le principe de responsabilité limitée des très grandes plateformes en ligne, posé par le DSA, est inadapté à celles d'entre elles qui constituent des « médias algorithmiques », en raison de leur statut d'acteur systémique, de leur utilisation d'algorithmes d'ordonnancement des contenus, de la prolifération persistante de contenus illicites sur leurs services, et de la facilitation des manipulations de l'information et des ingérences étrangères sur leurs réseaux sociaux ;

(65) Appelle de nouveau à créer, en ce qui les concerne, un régime européen de responsabilité renforcée spécifique ; considère que leurs choix de sélection, de priorisation, d'amplification ou de déréférencement de certains contenus, leur confèrent le statut d'éditeur de tels contenus ; estime que la responsabilité de ces fournisseurs doit pouvoir être directement engagée par toute personne ayant intérêt à agir contre ces contenus et pratiques ;

Une meilleure association des autorités de régulation nationales aux enquêtes de la Commission européenne sur les très grandes plateformes

(66) Soutient, au titre de la mise en œuvre du DSA, les démarches du coordinateur français pour les services numériques, l'autorité de régulation de la communication audiovisuelle et numérique (ARCOM), pour transmettre sans délai à la Commission européenne les plaintes et les alertes concernant les contenus ou agissements des très grandes plateformes en ligne ; déplore l'absence de réciprocité de la Commission et lui demande d'informer les coordinateurs nationaux sur les difficultés qui lui ont été signalées et, autant que possible, sur l'avancée des enquêtes en cours ;

(67) Souligne que les très grandes plateformes en ligne sont susceptibles de poser des risques systémiques à l'ensemble des États membres de l'Union européenne ; considère donc que les dispositions du DSA qui confèrent à la Commission européenne des pouvoirs exclusifs d'enquête et de sanction à l'égard de ces acteurs sont insatisfaisantes ;

(68) Relève que les coordinateurs des États membres ont acquis des compétences sectorielles et une connaissance précieuse de leur écosystème numérique national ; appelle donc, dans le double souci de coopération loyale et de mutualisation des moyens, à une meilleure association des autorités de régulation nationales des États membres de destination et de l'État membre d'établissement aux enquêtes et autres

actions de contrôle de la Commission européenne concernant le respect du DSA par ces très grandes plateformes ;

Un contrôle renforcé des algorithmes

(69) Souhaite également la mise en œuvre, au niveau européen, de normes minimales en matière d'éthique et de droits fondamentaux, qui devraient être respectées lors de l'élaboration des algorithmes d'ordonnancement des contenus, mais aussi de modération et d'adressage de la publicité, selon un principe de sécurité par la conception (*safety by design*) **;**

(70) Insiste sur la nécessité de rendre publics les algorithmes d'intelligence artificielle utilisés par les très grandes plateformes en ligne afin de sélectionner et de classer les contenus à chaque modification substantielle, aux fins de détection, par des chercheurs indépendants, des risques systémiques potentiels induits par leur fonctionnement, moyennant la mise en place de garanties appropriées concernant le secret des affaires ;

Une protection des mineurs plus efficace

(71) Rappelle que, conformément à l'article 24 de la charte des droits fondamentaux de l'Union européenne, « les enfants ont droit à la protection » et que « l'intérêt supérieur de l'enfant doit être une considération primordiale » ;

(72) Constate que la numérisation de la société engendre un risque de surexposition des mineurs aux écrans, au détriment de leur santé physique et mentale ; rappelle la responsabilité des plateformes en ligne pour protéger ces publics vulnérables face aux contenus illicites, haineux ou inappropriés sur internet, aux risques d'addiction, de cyberharcèlement, d'escroquerie ou de « pédopiégeage » ; souligne que plusieurs États tiers ont décidé de suspendre l'accès à certains réseaux sociaux pour des motifs de protection des mineurs ;

(73) Prend acte de la mise en œuvre effective des dispositions du DSA interdisant la publicité ciblée sur les plateformes en ligne visant les mineurs, préconisée de longue date par le Sénat ;

(74) Salue les enquêtes ouvertes par la Commission européenne visant les réseaux TikTok, Meta, Snap et Youtube pour évaluer l'efficacité de leurs mesures de protection des mineurs ; demande la publication rapide de lignes directrices au niveau européen, afin d'inciter les plateformes à adopter les standards les plus élevés de protection ;

(75) Se félicite de l'adoption, sous l'impulsion des associations de protection de l'enfance et du Sénat, des dispositions de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN), obligeant les plateformes en ligne fournissant des contenus pornographiques à instaurer un système de vérification de l'âge de leurs utilisateurs et, s'ils ne la respectent pas, à des mesures de blocage ou de déréférencement ;

(76) Souligne avec gravité que la Commission européenne, lors de la présentation de sa proposition de règlement COM(2022) 209 final établissant des règles pour prévenir et combattre les abus sexuels contre les enfants en ligne, le 11 mai 2022, avait souligné l'urgence de l'adoption de cette réforme ; constate néanmoins que les négociations de ce projet semblent bloquées depuis plusieurs mois ; demande donc solennellement l'adoption de cette réforme importante sans délai, conformément aux préconisations de sa résolution européenne n° 77 du 20 mars 2023 ;

(77) ***Sur l'ambition européenne en matière de souveraineté numérique***

(78) Considérant la part quasi-exclusive et des moteurs de recherche et des plateformes en ligne issus de pays tiers dans le marché intérieur et la dépendance devenue préjudiciable des économies et des sociétés européennes à leur égard qui nous met à la merci de ces entités,

(79) Considérant les nombreux travaux du Sénat ayant alerté l'Union européenne sur la nécessité de bâtir une stratégie européenne numérique respectueuse des droits fondamentaux et des principes démocratiques et d'une politique industrielle dédiée,

(80) Considérant les rapports de MM. Enrico Letta et Mario Draghi, qui formalisent une prise de conscience sans concession mais tardive de l'Union européenne sur cette nécessité,

(81) Considérant en particulier la nécessité pour les États membres et l'Union européenne, d'une part, d'investir massivement dans le développement de l'intelligence artificielle (IA), du *cloud,* en particulier les solutions de *cloud* souverain, et du quantique et, d'autre part, de favoriser l'émergence d'acteurs européens du numérique permettant d'assurer notre indépendance et de rivaliser avec les plateformes, réseaux et applications numériques d'états tiers, sous peine de rester une « colonie numérique »,

(82) Demande la mise en place urgente d'une politique industrielle européenne volontariste en faveur de cette souveraineté numérique européenne, en particulier dans la perspective de la généralisation de l'intelligence artificielle, ce qui suppose de remédier à la fragmentation du marché intérieur et de faciliter la constitution d'alliances industrielles européennes ;

(83) Appelle à relancer la mise en œuvre du Programme d'action numérique de l'Union européenne à l'horizon 2030 (boussole numérique) et à mobiliser l'ensemble des financements européens pertinents ;

(84) Prend note de la présentation de la « boussole pour la compétitivité », le 29 janvier dernier, par la Commission européenne, afin de favoriser

l'innovation européenne pour permettre à l'Union européenne de jouer un rôle notable parmi les acteurs du numérique ;

(85) Souhaite que la France et l'Union européenne soient des acteurs de premier plan dans le domaine de l'intelligence artificielle (IA) ; considère à ce titre que le partenariat public-privé « EU AI Champions Initiative », l'initiative sur les « fabriques d'IA » et la « stratégie pour l'application de l'IA », sont autant de dispositifs utiles pour son développement et son exploitation industrielle dans des secteurs clés ;

(86) Précise que des infrastructures publiques, résilientes et inclusives (*open source*, semi-conducteurs, *cloud computing*, supercalculateurs…) doivent garantir cette souveraineté numérique, prendre en compte les évolutions technologiques et assurer un écosystème numérique démocratique et résilient fondé sur les valeurs de l'Union européenne ; souligne l'excellence des entreprises françaises et européennes en la matière ; réitère qu'une politique incitative doit être mise en œuvre pour leur permettre de prendre toute leur place dans le monde numérique et assurer un degré d'autonomie stratégique suffisant, notamment grâce à la commande publique ;

(87) Salue à cet égard l'annonce de la révision prochaine de la directive européenne sur les marchés publics et de la reconnaissance, dans ce cadre, d'une préférence européenne dans les secteurs stratégiques ; estime essentiel de définir dans ce cadre, le numérique comme l'un de ces secteurs stratégiques ;

(88) Demande à cette fin à la Commission européenne que soient créées les conditions permettant l'émergence d'acteurs numériques européens afin d'assurer un contrôle, une localisation et une exploitation des données conformes à la législation européenne ainsi qu'une information fiable et sourcée ;

(89) Souhaite que ces mesures soient accompagnées par une politique européenne de recherche renforcée en faveur de l'innovation et des technologies liées à l'IA, s'appuyant notamment sur le renforcement des réseaux publics européens ; estime également essentiel de prévoir les financements nécessaires, en particulier par le doublement du budget du programme-cadre européen de recherche et d'innovation « Horizon Europe » ; appelle à placer cette ambition numérique au rang des priorités budgétaires lors des négociations du prochain cadre financier pluriannuel de l'Union européenne ;

(90) Invite le Gouvernement à faire valoir cette position dans les négociations au Conseil.

LA RÉSOLUTION EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, le tableau synoptique de la résolution en construction est disponible sur le site du Sénat à l'adresse suivante :

https://www.senat.fr/tableau-historique/ppr24-351.html

LISTE DES PERSONNES ENTENDUES

Commission européenne

Direction générale de la concurrence

- *M. Alberto Bacchiega*, Directeur pour les Plateformes Digitales
- *M. Antoine Babinet*, Chef d'unité adjoint – Direction Plateformes Digitales

Direction générale Réseaux de communication, contenu et technologies (DG Connect)

- *Mme Rita Wezenbeek*, Directrice pour la Règlementation et Supervision des Plateformes en ligne
- *Mme Garance Dekeyser*, chargée de dossiers dans l'unité Coordination et conformité réglementaire

Autorité de régulation de la communication audiovisuelle et numérique (ARCOM)

- *M. Alban de Nervaux*, Directeur général
- *Mme Lucile Petit*, Directrice des Plateformes en ligne
- *Frédéric Bokobza*, Directeur général adjoint

Secrétariat général de la défense et de la sécurité nationale – Vigilance et protection contre les ingérences numériques étrangères (Viginum)

- *M. Marc-Antoine Brillant*, Chef du service de Viginum
- *Mme Camille Le Roy*, État major Viginum

NumSpot

- *M. Patrick Laurens-Frings*, Directeur général
- *Mme Servane Augier,* Directrice commerciale et marketing
- *Mme Séverine Denys,* Directrice des affaires institutionnelles et réglementaires de Docaposte

Institut d'études politiques de Paris

- *M. David Colon,* Professeur agrégé d'histoire

Comité de pilotage des États généraux de l'information

- *M. Bruno Patino*, président ; président du directoire d'ARTE France, journaliste, essayiste