

N° 1159

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 19 mars 2025.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES EUROPÉENNES ⁽¹⁾
SUR LA PROPOSITION DE RÉSOLUTION EUROPÉENNE (N° 876),
DE MM. THIERRY SOTHER, JÉRÉMIE IORDANOFF et plusieurs de leurs collègues,

rappelant l'urgence démocratique d'appliquer pleinement et entièrement le règlement européen sur les services numériques,

PAR MM. JÉRÉMIE IORDANOFF ET THIERRY SOTHER,
Députés

⁽¹⁾ La composition de la commission figure au verso de la présente page.

La Commission des affaires européennes est composée de : M. Pieyre-Alexandre ANGLADE, président ; M. Laurent MAZAURY, Mmes Manon BOUQUIN, Nathalie OZIOL M. Thierry SOTHER, vice-présidents ; MM. Maxime MICHELET, secrétaires ; MM. Gabriel AMARD, David AMIEL, Philippe BALLARD, Karim BENBRAHIM, Guillaume BIGOT, Mme Céline CALVEZ, M. François-Xavier CECCOLI, Mmes Sophia CHIKIROU, Nathalie COLIN-OESTERLÉ, MM. Arthur DELAPORTE, Julien DIVE, Nicolas DRAGON, Romain ESKENAZI, Michel HERBILLON, Mme Mathilde HIGNET, MM. Sébastien HUYGHE, Jérémie IORDANOFF, Mmes Sylvie JOSSERAND, Marietta KARAMANLI, M. Bastien LACHAUD, Mme Hélène LAPORTE, M. Jean LAUSSUCQ, Mme Constance LE GRIP, MM. Pascal LECAMP, Alexandre LOUBET, Mathieu MARCHIO, Patrice MARTIN, Emmanuel MAUREL, Mmes Yaël MENACHÉ, Danièle OBONO, MM. Frédéric PETIT, Pierre PRIBETICH, Mmes Isabelle RAUCH, Sandrine ROUSSEAU, MM. Alexandre SABATOU, Charles SITZENSTUHL, Mmes Michèle TABAROT, Sophie TAILLÉ-POLIAN, Liliana TANGUY, Sabine THILLAYE, M. Frédéric VALLETOUX, Mme Estelle YOUSOUFFA.

SOMMAIRE

	Pages
INTRODUCTION	5
PREMIÈRE PARTIE : ENTRE DÉSINFORMATION ET INGÉRENCES ÉTRANGÈRES, LES PLATEFORMES EN LIGNE DEVIENNENT LES RELAIS D'INQUIÉTANTS PHÉNOMÈNES	7
A. LA CARACTÉRISATION D'UN PHÉNOMÈNE EN MUTATION	7
1. Une tentative de définition	7
2. L'essor des réseaux sociaux et les changements informationnels du public : l'altération de la liberté d'expression	9
3. Les législations nationales européennes ont cherché à répondre à la menace de la désinformation et de l'ingérence étrangère	12
B. DES RÉSEAUX SOCIAUX AUX PRATIQUES TROUBLES	16
1. Le rachat de la plateforme Twitter et l'arrivée d'une nouvelle administration américaine ont entraîné un basculement idéologique majeur sur la plateforme et amoindri considérablement sa politique de modération.....	16
a. Le coûteux rachat d'une puissante plateforme qui peinait à trouver sa rentabilité	16
b. Des changements impulsifs conduisant X à favoriser les contenus haineux, violents et mensongers	17
c. Des manipulations de l'algorithme au profit d'Elon Musk et de ses relais politiques	19
d. Une omniprésence d'Elon Musk renforçant un facteur personnel de désinformation.....	20
e. La récente opacité de X et le refus de l'étude de son contenu.....	21
f. Malgré les empêchements, une évolution détectée des opinions représentées sur X depuis son rachat.....	22
g. Après la victoire de Donald Trump, la présence d'Elon Musk à la Maison Blanche et des ingérences dans les pays européens.....	24
2. Le réseau social TikTok exerce une influence problématique caractérisée par une collecte massive de données personnelles et un algorithme captivant le public..	27

DEUXIÈME PARTIE : LA LÉGISLATION SUR LE NUMÉRIQUE PROPOSE UN CADRE JURIDIQUE RENOUVELLE QUE VOS RAPPORTEURS SOUHAITENT AMÉLIORER	32
A. UNE NOUVELLE LÉGISLATION EUROPÉENNE SUR LE NUMÉRIQUE..	32
1. Une nécessaire législation : remédier à l’obsolescence du règlement de 2000 et aller au-delà des simples codes de conduite.....	32
2. L’architecture de la nouvelle législation sur le numérique : des obligations contrôlées à l’échelon national et à l’échelon européen.....	33
3. Un équilibre à trouver entre la liberté d’expression et le modèle économique des plateformes.....	37
B. LE RÈGLEMENT SUR LES SERVICES NUMÉRIQUES EST CONFRONTÉ A DIFFÉRENTES DIFFICULTÉS DANS SA MISE EN ŒUVRE	39
1. Des enquêtes européennes à la peine	39
2. Un cas d’école de détournement de la législation sur le numérique : le premier tour de l’élection présidentielle roumaine en novembre 2024	42
C. LES PRÉCONISATIONS PORTÉES PAR VOS RAPPORTEURS SONT DE DIFFÉRENTS NIVEAUX	45
1. La Commission européenne et les acteurs nationaux doivent assumer les pouvoirs que le règlement sur les services numériques leur confère.....	45
2. Repenser le modèle des plateformes : la rentabilité du modèle économique doit aller de pair avec des architectures numériques éthiques.....	49
3. La création d’une véritable souveraineté numérique européenne.....	53
CONCLUSION	57
EXAMEN EN COMMISSION	58
PROPOSITION DE RÉOLUTION EUROPÉENNE INITIALE	73
AMENDEMENTS EXAMINÉS PAR LA COMMISSION	77
EXPOSÉ SOMMAIRE	85
PROPOSITION DE RÉOLUTION ADOPTÉE PAR LA COMMISSION	91
ANNEXES :	95

INTRODUCTION

MESDAMES, MESSIEURS,

Nous vivons actuellement **un paradoxe démocratique en matière de liberté d'expression** : il n'a jamais été aussi facile d'exprimer ses idées - grâce à l'essor exponentiel des réseaux sociaux - tout en étant aussi peu contrôlé par des outils de modération mis en place par les plateformes en ligne.

C'est notamment pour répondre à cette situation dans laquelle des acteurs privés parviennent à imposer leurs règles que **le législateur européen a décidé d'intervenir et de mettre en œuvre le règlement sur les services numériques (DSA)**.

Conçu de sorte que **tout ce qui est interdit hors-ligne le soit également en ligne** – pour reprendre l'expression de l'ancien commissaire européen Thierry Breton – **le DSA entend répondre à la prolifération des contenus dits illicites**.

Après plus d'un an de mise en œuvre du DSA et dans un contexte de bouleversement des politiques de modération sur le réseau social X, vos rapporteurs considèrent que la situation appelle réflexion et action.

Tout d'abord, il convient **d'appréhender la question de la diffusion des contenus illicites**, ici compris **comme désinformation et ingérences**, en déterminant ses frontières et son cadre applicable au niveau national.

C'est parce que la réponse ne pouvait rester nationale face à des géants du numérique à la capacité d'influence planétaire que **le DSA** a été pensé. Il vient **apporter un cadre renouvelé tout en s'efforçant de maintenir l'équilibre entre liberté d'expression et politique de modération**.

Constatant le changement majeur de politique éditoriale de X depuis son rachat, les insuffisances du DSA et les risques majeurs sur les processus électoraux, **la proposition de résolution européenne portée par vos rapporteurs appelle à une nouvelle action énergique**.

Cette action peut se réaliser **à différents niveaux** en gardant à l'esprit l'économie globale du modèle des plateformes, les conditions d'exercice de la liberté d'expression que nous souhaitons garantir et la construction d'une véritable souveraineté numérique européenne.

PREMIÈRE PARTIE : ENTRE DÉSINFORMATION ET INGÉRENCES ÉTRANGÈRES, LES PLATEFORMES EN LIGNE DEVIENNENT LES RELAIS D'INQUIÉTANTS PHÉNOMÈNES

A. LA CARACTÉRISATION D'UN PHÉNOMÈNE EN MUTATION

1. Une tentative de définition

Dans un essai écrit pour la revue littéraire *Raritan* en 1986, le philosophe américain Harry Frankfurt s'est essayé à définir la « connerie », le « baratin ». Cet essai republié en 2005 sous le titre « *De l'art de dire des conneries* » (« *On Bullshit* », en version originale) a voulu ainsi distinguer le menteur qui fait des déclarations volontairement fausses du diseur de « conneries », indifférent à la vérité.

H. Frankfurt y écrivait notamment : « Les conneries sont un ennemi plus grand de la vérité que ne le sont les mensonges ». « *Bullshit is a greater enemy on the truth than lies are.* »

Il apparaît, d'une certaine façon, que le philosophe avait anticipé les mutations de notre époque qui a vu être consacrée le concept de post-vérité – développé en 2004 par l'écrivain américain Ralph Keyes dans son ouvrage *The Post-Truth Era : Dishonesty and Deception in Contemporary Life* et reconnu mot de l'année par l'*Oxford English Dictionary* en 2016.

La question des fausses nouvelles, corollaire des « conneries » de Frankfurt ou de la « post-vérité » de Keyes est apparue récemment dans le débat public à la suite de deux événements politiques intervenus en 2016. Il s'agit du référendum britannique pour sortir de l'Union européenne et de l'élection présidentielle américaine. Lors de ces deux campagnes, le nombre de faits inexacts – voire totalement mensongers – a connu un niveau jusqu'alors jamais atteint.

Ces éléments n'ont pas eu pour seule conséquence d'altérer le débat public puisque les Britanniques ont décidé de quitter l'Union européenne sur la foi de mensonges répétés par le gouvernement de David Cameron et le parti violemment eurosceptique de Nigel Farage. De même, aux États-Unis, les mensonges colportés par le candidat républicain Donald Trump sur sa concurrente démocrate Hillary R. Clinton – puissamment aidés par une campagne d'ingérence étrangère russe – lui ont permis de remporter l'élection contre toute attente.

C'est dans ce contexte géopolitique troublé que le concept de fausses informations (infox) a pris une telle place dans le débat public, constatant qu'en dépit des dénégations et tentatives de rétablissement de la vérité certaines opinions perduraient voire prenaient plus d'importance encore. Plus grave encore, le concept

de « *faits alternatifs* » s'est affirmé – il s'agit de fausses nouvelles – à travers son usage **par la porte-parole du président Trump** tout juste élu, Kellyanne Conway, dans un échange avec la presse le 22 janvier 2017.

Les informations falsifiées ne sont néanmoins pas une nouveauté puisque le droit français les considère depuis le XIX^e siècle, comme l'illustre **l'article 27 de la loi du 29 juillet 1881 sur la liberté de la presse** qui dispose : « *La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses [...] lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros* ».

Les fausses informations trouvent à s'exprimer de différente manière, ainsi qu'une note du *think tank* Renaissance numérique datée de mars 2018 s'en faisait l'écho. La note distinguait ainsi la **désinformation** (information erronée reprise pour nuire), la **mésinformation** (fausse information reprise sans intention malveillante) et la **mal-information** (reprise d'éléments réels dans un but malveillant).

Les fausses informations ont également pu être associées aux discours de haine, s'entremêlant avec ces derniers, **avec des risques tragiques pour la vie publique et la démocratie**. Le meurtrier de la députée travailliste britannique Jo Cox, assassinée lors de la campagne référendaire sur le Brexit, se nourrissait des deux comme son profil sur les réseaux sociaux l'a illustré. Il en va de même pour le tueur néo-zélandais de l'attentat de Christchurch visant des musulmans.

Cette inquiétude au sujet des fausses informations et de leur incidence sur la vie démocratique n'est pas aisée à quantifier. Ainsi, le cabinet Bakamo estimait qu'en France la campagne de l'élection présidentielle de 2017 avait donné lieu à huit millions de partages sur les réseaux sociaux dont près d'un quart étaient constituées partiellement ou totalement de fausses informations.

De façon symétrique, la campagne présidentielle américaine de 2016 a donné été le théâtre de la diffusion massive de fausses informations ⁽¹⁾, selon lesquelles Hillary Clinton aurait vendu des armes à l'État islamique ou encore que le Pape François aurait apporté son soutien à Donald Trump. Ces vingt canulars ayant suscité le plus d'engagement ont fait l'objet de 8.7 millions de réactions sur Facebook, quand, dans le même temps, les vingt articles de presse les plus lus de médias traditionnels américains n'y ont suscité que 7.3 millions de réactions.

La difficulté d'évaluer l'impact réel des fausses informations peut néanmoins s'apprécier à la lumière d'une **étude parue dans le magazine Science**

(1) sources: https://www.lemonde.fr/pixels/article/2016/11/17/l-essor-des-fausses-informations-dans-les-derniers-mois-de-la-campagne-americaine_5032435_4408996.html
<https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook#.wvY9GWkyE>

en 2018 indiquant que **les fausses informations se propageaient six fois plus vite que les autres sur le réseau social Twitter (X)**.

À l'échelle européenne, près de **80 % des Européens interrogés** dans le cadre de l'étude Eurobaromètre indiquaient **en 2018 considérer les fausses nouvelles comme un problème**.

Il est également possible d'analyser l'impact des fausses nouvelles en soulignant **les paniques morales** dont elles peuvent être à l'origine. Le concept désigne une **réaction collective disproportionnée en réaction à un événement**, une personne ou une situation dont il est estimé qu'elle constitue une menace. Le concept inventé par le sociologie britannique Stanley Hoffmann en 1972 a connu une riche postérité. Les réseaux sociaux, en permettant la diffusion de fausses nouvelles, donnent chaque jour une actualité nouvelle au phénomène sociologique.

La capacité à agir des fausses nouvelles est aussi à considérer. Au regard de la prégnance – si ce n'est de l'emprise – du numérique, les services numériques, et singulièrement les réseaux sociaux, sont devenus le vecteur du phénomène. C'est d'ailleurs ici que **s'entrecroisent fausses nouvelles et ingérences étrangères**.

Si les fausses nouvelles sont anciennes - comme la discipline historique l'a démontré -, leur capacité à bouleverser le débat public est plus récente : les réseaux sociaux leur ont donné une force de perturbation inouïe. Plus encore, **des puissances étatiques y ont vu le moyen de s'ingérer dans les affaires d'autres États** (élections présidentielles américaines de 2016, référendum sur le Brexit de 2016, campagne présidentielle française de 2017).

Les **ingérences étrangères numériques sont des stratégies hybrides** qui se définissent par :

- l'intention de porter atteinte aux **intérêts fondamentaux de la Nation** ;
- la **propagation de contenus** manifestement inexacts ou trompeurs ;
- la **diffusion de contenus de manière inauthentique** (artificielle ou automatisée, massive et délibérée) destinée à **amplifier la visibilité ou la viralité** de ces contenus sur les plateformes numériques ;
- l'implication, directe ou indirecte, d'un **acteur étranger**, qu'il soit étatique ou non.

2. L'essor des réseaux sociaux et les changements informationnels du public : l'altération de la liberté d'expression

La **loi de 1881**, précédemment citée, avait prévu de **fixer le cadre législatif s'agissant de la liberté d'expression**. Elle ne pouvait cependant pas anticiper l'arrivée des réseaux sociaux et les multiples conséquences que ces derniers allaient entraîner.

Ainsi, **l'usage des services numériques est devenu prédominant** puisque trois quarts des citoyens européens se déclarent utilisateurs réguliers des réseaux sociaux (**70 %**), d'après l'étude d'impact datée de 2018 du règlement sur les services numériques (*Digital services Act*).

Cette croissance s'est d'ailleurs encore fortement accrue comme en témoigne le nombre d'utilisateurs des plateformes : Facebook (devenue Meta) a été créé en 2004 et a dépassé le cap des trois milliards d'utilisateurs actifs mensuels en juillet 2023. ⁽¹⁾

Quant à Twitter - devenu X en 2023 après le rachat de plateforme par Elon Musk le réseau social revendique 238 millions d'utilisateurs en juillet 2022, un bond de 15 % par rapport à juillet 2021 pour une société créée en 2006.

L'importance de l'usage des réseaux sociaux emporte des conséquences sur le mode d'information privilégié par les citoyens. La Commission européenne estime ainsi que 57 % des utilisateurs de ces derniers dans l'Union européenne privilégient ce canal pour collecter de l'information.

En 2021, Internet constitue la source principale d'information pour 67 % de la population en France. **Les réseaux sociaux seuls représentent la principale source d'information pour 38 % de la population.**

L'impact des réseaux sociaux sur l'information peut s'apprécier à travers la formule devenue célèbre de **Lawrence Lessig** professeur à l'université Harvard : « *Code is Law* ». La formule traduite en français signifie que **le programme informatique** fait la loi. Il **régit les rapports entre les acteurs : les informations diffusées** ne dépendent ainsi plus d'interactions physiques ou légales mais de programmes informatiques complexes sur lesquels la loi n'a pas d'emprise *a priori*.

Internet fait alors figure d'**espace opaque où les règles changeantes, imposées par quelques multinationales du numérique, s'imposent à chacun** sans qu'il n'en ait nécessairement une connaissance approfondie ni même une compréhension poussée. **Le pouvoir normatif des technologies**, et plus spécifiquement des grandes plateformes, coordonne les conditions d'exercice de la liberté d'expression ⁽²⁾.

Dès lors que les citoyens tendent à s'informer via les réseaux sociaux, **la question de la légitimité des sources fondant leur opinion** doit être posée. La façon dont les contenus sont ordonnancés (logique, algorithmique), la hiérarchisation des sources et la mise en avant de contenus parfois sponsorisés exercent des effets tangibles sur l'opinion publique.

Le sujet n'est pas neuf dans la mesure où **la question de la neutralité d'internet** a été posée dès ses débuts, dans les années 1990, lorsqu'il a touché le

(1) Rapport de Meta sur les résultats financiers du deuxième trimestre 2023. 26 juillet 2023.

(2) Romain Badouard, *Les nouvelles loi du web – Modération et Censure, Le Seuil, 2020.*

grand public. La décision de libéraliser le secteur des télécommunications, à l'initiative de l'administration Clinton, a rejailli sur l'ensemble du globe modifiant les équilibres économiques et au-delà.

Dès lors que **l'information** se voit aujourd'hui principalement disséminée par les services numériques, et plus particulièrement les réseaux sociaux, elle se voit **conditionnée par le cadre économique qui la régit**.

Par ailleurs, il convient de souligner qu'Internet ne se contente pas de relier des ordinateurs et des serveurs. Il connecte des aires géographiques et des systèmes culturels. Les modalités informationnelles en sont donc altérées dès lors que des influences trouvent à s'exprimer et à agir sur les individus et leur système de pensée.

En outre, il convient d'observer que **les conditions de la liberté d'expression ne sont pas les mêmes entre les différentes démocraties libérales**. Les modalités de **définition d'un abus de l'usage de la liberté d'expression** diffèrent sensiblement entre le continent européen et les États-Unis, où se sont développées les grandes plateformes qui détiennent un poids économique considérable dans les services numériques.

Aux **États-Unis, la liberté d'expression est garantie par le 1^{er} amendement de la Constitution** de façon extrêmement large. Le Congrès ne peut voter des lois qui viendraient empiéter ce droit fondamental. À l'inverse, la France dispose d'un arsenal législatif étoffé, fondé sur la Constitution, et enrichi tout au long des dernières décennies pour encadrer les modalités d'expression afin de protéger les droits d'autrui et l'ordre public.

Ces deux visions opposées emportent des conséquences pratiques dans la mesure où **le rôle dévolu à l'État quant à la régulation de la parole publique n'est pas le même**. Les États-Unis considèrent qu'il est nécessaire d'empêcher l'État d'intervenir dans le débat public quand **la France fixe un rôle éminent à l'État pour déterminer les conditions du débat** et, si besoin, sanctionner les abus.

Dans une vision libérale revendiquée, les États-Unis considèrent que les idées s'affrontent dans une sorte de mouvement concurrentiel et que l'idée la plus forte et la plus pertinente se dégage et s'impose comme une vérité.

Il est aisé de voir rapidement les limites de cette vision censément neutre puisque **la mise en cause de la neutralité de l'Internet et les conditions d'utilisation des plateformes numériques cadrent le débat**, ainsi que nous le soulignons précédemment.

La loi américaine distingue les **discours de haine** (*hate speech*) des **incitations à la violence** (*fighting words*). Il ressort de cette distinction que seules les secondes font l'objet de poursuites pénales dans la mesure où elles sont considérées comme des troubles de l'ordre public avec un passage potentiel à la violence. L'approche française, et plus généralement européenne, de la question

opère un **lien de causalité évident entre des propos haineux et le passage à la violence.**

Cette différence culturelle entre deux sphères s'est retrouvée dans l'histoire d'Internet et des réseaux sociaux par la suite. Les pionniers d'internet le concevaient selon une vision particulièrement libertaire et ont donc imaginé son fonctionnement de sorte que les principes du libéralisme informationnel trouvent à s'exprimer sans que la circulation des idées ne se trouve arrêtée par quelque obstacle.

Cette opposition entre deux approches a conditionné **le régime juridique d'expression et notamment la capacité à considérer la responsabilité des acteurs.** Il en ressort un choix européen singulier de sanctionner la désinformation ainsi que les ingérences.

Enfin, le changement caractérisant la façon dont le grand public s'informe, à travers les réseaux sociaux, pose **le débat de la distinction entre hébergeur et éditeur.** Cette question se retrouve dans le choix de législation des différents pays au niveau européen, et que nous évoquerons ultérieurement.

D'un point de vue juridique, **l'éditeur** est supposé avoir connaissance et contrôler le contenu diffusé sur son site : **il joue donc un rôle actif. L'hébergeur** en revanche, **est un prestataire technique** assurant une simple mise à disposition d'un serveur et éventuellement d'une interface.

Le débat posé par les mises à disposition d'informations, notamment lorsqu'elles sont inexacts ou trompeuses, est celui de **l'engagement de la responsabilité juridique de la plateforme en ligne.** Dans le cas de médias d'informations traditionnels, c'est le statut d'éditeur qui prévaut. Par contre, pour des plateformes en ligne dont l'activité principale n'est pas d'éditer du contenu, c'est un statut d'hébergeur qui s'impose. **En cas de délit, les dispositions applicables présentent de réelles différences.**

3. Les législations nationales européennes ont cherché à répondre à la menace de la désinformation et de l'ingérence étrangère

Le contexte britannique et américain, évoqué précédemment, ainsi que la tentative d'ingérence de puissances étrangères lors de l'élection présidentielle française de 2017 ont poussé le législateur à agir.

Ainsi, lors de l'entre-deux-tours de l'élection présidentielle française, un ensemble de plusieurs milliers de messages électroniques des équipes de campagne du candidat Emmanuel Macron a été diffusé sur Internet ⁽¹⁾. Si la majorité des correspondances étaient réelles, le fichier mis en ligne en contenait d'autres, falsifiées. Mis en ligne quelques heures avant la fin de la campagne officielle du second tour, c'est-à-dire lorsque les candidats ne peuvent plus s'exprimer, ils étaient destinés à produire le soupçon et décourager des électeurs hésitants à aller voter. Il

(1) <https://www.radiofrance.fr/franceculture/que-contiennent-les-macron-leaks-6503861>

n'a pas été possible de retracer exactement le commanditaire de l'opération appelée **Macron Leaks** mais l'affaire a été massivement relayée, et parfois déformée, par les comptes partageant des interactions avec l'extrême-droite américaine et française, lesquels étaient devenus actifs peu de temps avant le début de la campagne. Si les services de renseignement français n'ont pas réussi à identifier l'origine de la fuite, une enquête menée par le journal *Le Monde* tend à confirmer le fait qu'un groupe de hackers russes, proches du Kremlin, en soit à l'origine ⁽¹⁾.

La situation n'a pas eu de conséquences sur le résultat de l'élection, contrairement à ce qui avait pu se produire au Royaume-Uni pendant la campagne du Brexit ou aux États-Unis en 2016. Elle a néanmoins illustré **la montée grandissante du phénomène de désinformation mêlé à de l'ingérence étrangère**.

D'un point de vue technique, la décision de mettre en place de nouvelles réglementations n'est pas aisée. La France, comme indiqué précédemment, dispose d'un régime de la liberté d'expression prévu par la loi de 1881.

L'arrivée des services numériques, et particulièrement des réseaux sociaux, vient modifier le régime juridique. Jusqu'alors les seules modifications à la loi de 1881 concernaient l'ajout de restrictions (injure, incitation à commettre des délits, apologie de crimes de guerre, outrage...).

À partir de 2004, avec **la loi de confiance dans l'économie numérique (LCEN), il s'agit d'adapter la loi de 1881 à internet**, ce qui pose un nombre de problèmes pratiques d'application. La loi de 2004 vient ainsi concerner l'ensemble des internautes quand celle de 1881 s'adressait uniquement à la presse.

Par ailleurs, **la question de l'intention est posée et celle de la publicisation des propos** également. La responsabilité juridique d'un individu est mise en cause en raison de sa volonté de nuire et de sa décision de recourir à la publication d'un contenu pour cela.

La responsabilité des plateformes est alors posée. Or, **le cadre existant alors est celui défini par la directive dite e-commerce, adoptée en 2000**, que la loi LCEN a transposé en droit français. Ce texte établit un **régime de responsabilité limité** aux termes duquel un hébergeur ne peut être tenu pour responsable des contenus et activités illicites présents sur ses services, à condition qu'il n'ait pas eu connaissance de leur présence et de leur caractère illicite, ou bien qu'en ayant eu connaissance il ait agi « *promptement* » pour les retirer ou les rendre inaccessibles.

(1) - <https://www.numerama.com/politique/254983-compte-offshore-demmanuel-macron-une-intox-venue-de-4chan.html>
- <https://www.mediapart.fr/journal/france/110517/les-macron-leaks-posent-plus-de-questions-quils-ne-font-scandale>
- https://www.liberation.fr/politiques/2017/05/09/macronleaks-la-grande-foire-aux-fake-news_1567868/?redirected=1

Ce régime juridique de responsabilité limitée couplé à la diffusion des fausses nouvelles, d'utilisation de données collectées (*Cambridge Analytica*) ou de tentatives de déstabilisation extérieures ne rend pas la tâche aisée pour le législateur.

Suite à un engagement du président de la République, **une proposition de loi (PPL) relative à la lutte contre les fausses informations** a été déposée à l'Assemblée nationale par la députée Lætitia Avia (La République en Marche) le 21 mars 2018.

Cette PPL était composée de dix articles et **complétée par une proposition de loi organique**. La proposition législative ordinaire a été très largement remaniée au cours des débats parlementaires.

Le texte venait modifier le code électoral. **Il renforçait les pouvoirs du Conseil supérieur de l'audiovisuel (CSA) – depuis refondu dans l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM)** - afin de contraindre les médias sous influence étrangère qui chercherait à diffuser de fausses informations.

Il venait également encadrer l'activité des plateformes, de façon limitée, en élargissant les obligations des intermédiaires techniques des services en ligne dans le cadre de la lutte contre la diffusion de fausses informations.

Lors des débats, l'obligation pour les plateformes de **mettre en place un mécanisme de signalement** pour permettre aux utilisateurs de signaler les « fausses informations » a été considérablement modifiée de sorte qu'elles ne soient finalement plus contraintes de transmettre ces signalements à l'autorité publique.

Le CSA s'est vu confier un **rôle métaréglatoire** en lui permettant d'émettre des recommandations pour les plateformes dans la lutte qu'elles mènent contre les fausses informations.

Certaines dispositions contenues dans le texte ont permis de **faire progresser la connaissance de la problématique des fausses informations** tout en étant tenues par le cadre européen. Ainsi, des recommandations en matière de transparence des algorithmes et des données apparaissent comme trop en deçà du niveau d'exigence indispensable pour modifier réellement le modèle économique des plateformes, dont la diffusion de fausses nouvelles se nourrit largement.

La loi définitivement adoptée par le Parlement français le 24 juin 2020 contenait comme disposition maîtresse **l'obligation pour les opérateurs de plateforme en ligne et les moteurs de recherche de retirer dans un délai de 24 heures** – après notification par un utilisateur – des contenus manifestement illicites (incitations à la haine, par exemple).

Dans le cas de contenus terroristes ou pédopornographiques, le délai était réduit à une heure. Cependant, cette disposition a été censurée par le Conseil constitutionnel qui l'a considérée contraire à la liberté d'expression, garantie

constitutionnellement par l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen.

Plus récemment, **l'article 42 de la loi confortant les principes de la République**, promulguée le 24 août 2021, impose des obligations concernant le contrôle des contenus illicites.

À l'échelle **européenne, plusieurs pays ont légiféré sur les contenus illicites**. Ainsi, l'Allemagne a mis en place la loi *Netzwerkdurchsetzungsgesetz* dite *NetzDG* entrée en vigueur le 1^{er} octobre 2017. Ses dispositions, applicables aux plateformes de plus de deux millions d'utilisateurs inscrits en Allemagne, font obligation à l'intermédiaire de supprimer localement, tout **contenu « manifestement illégal »** dans les vingt-quatre heures suivant son signalement. La suppression est rendue possible si le contenu relève d'une des vingt-unes dispositions du Code pénal allemand.

Si l'illégalité n'est pas manifeste, la plateforme dispose de sept jours pour agir. *A contrario* de la loi française dite Avia, le texte allemand ne prévoit pas de sanctions en cas de non-retrait.

Les effets de la loi n'ont pas été manifestes puisque les plateformes disposent, à travers leurs conditions générales d'utilisation, de possibilités de retrait de contenus. Les retraits au titre de la loi *Netz DG* sont donc restées relativement peu importants.

En Autriche, une loi adoptée en 2020 relative aux mesures de protection des utilisateurs des plateformes (*Kommunikationsplattformen-Gesetz* ou *KoPl-G*), relativement proche de la loi allemande *Netz DG* prévoit une procédure de signalement d'un contenu illégal permettant à l'utilisateur de signaler facilement et efficacement. Les décisions de blocage ou de suppression peuvent faire l'objet d'un réexamen.

La gestion des contenus illicites a donc pris une ampleur internationale. Les **États-Unis**, pour lesquels la **section 230 du *Communication Decency Act*** de 1996 offre une protection juridique pour les fournisseurs de service en les exonérant de toute responsabilité en matière de contenu, se sont interrogés sur l'opportunité d'une régulation plus stricte. **Les plateformes ont pu d'ailleurs s'y montrer un temps favorable**, à l'image du directeur général de Facebook Mark Zuckerberg qui défendait le 25 mars 2021 devant la chambre basse du Congrès américain la révision de la section 230.

B. DES RÉSEAUX SOCIAUX AUX PRATIQUES TROUBLES

1. Le rachat de la plateforme Twitter et l'arrivée d'une nouvelle administration américaine ont entraîné un basculement idéologique majeur sur la plateforme et amoindri considérablement sa politique de modération

a. *Le coûteux rachat d'une puissante plateforme qui peinait à trouver sa rentabilité*

Twitter a vu le jour le 13 juillet **2006** à San Francisco, au sein de la Silicon Valley, berceau de la révolution numérique. Il s'agit d'un réseau social de microbloggage permettant à ses utilisateurs d'envoyer des messages appelés Tweets. Très rapidement, Twitter a acquis une taille significative puisqu'en mars 2008 c'était déjà près d'un million d'utilisateurs qui étaient comptabilisés.

Entre sa création en 2006 et 2012, la plateforme s'est enrichie d'applications aux usages divers et n'a cessé d'élargir son champ d'influence. Cotée à la bourse de New York en 2013, Twitter a poursuivi son ascension jusqu'à **connaître un nouveau changement de gouvernance qui va radicalement modifier sa structure et sa politique éditoriale.**

Un des traits caractéristiques de la plateforme est **d'avoir mis en place le fil d'actualité** qui trie le contenu publié par les comptes suivis, de manière individualisée. **Mais les algorithmes comptent parmi les propriétés intellectuelles les plus estimables de ces entreprises, qui en verrouillent donc l'accès. Il s'agit d'une agrégation de plusieurs millions de critères et de données, une œuvre si grande que même les équipes internes n'en ont qu'une vision fractionnée. Sa taille est telle que pour l'ajuster, les développeurs procèdent par empirisme, souvent par choix préférentiel** parmi plusieurs mises à jour test, tant il est difficile de savoir avec certitude les impacts qu'un changement peut avoir sur celui-ci.

Le 14 avril 2022, l'entrepreneur Elon Musk propose d'acheter la société de réseaux sociaux Twitter, Inc pour **43 milliards de dollars**. Cette proposition surprend l'ensemble de l'écosystème tant les sommes en jeu sont conséquentes et tant la démarche de Musk apparaît opaque et peu crédible. E. Musk provoque de multiples revirements durant la procédure d'achat et des implications judiciaires sont évoquées

Le rachat est finalement réalisé pour la somme de 44 milliards de dollars fin octobre 2022. **Ce rachat paraît de prime abord surprenant dès lors que la rentabilité du réseau social est à ce moment jugée très précaire.** Puisque l'intérêt financier de l'opération est douteux, des interrogations sont soulevées sur les objectifs politiques de ce rachat.

Le questionnement se renforce lorsque Elon Musk émet son premier tweet : **« L'oiseau a été libéré »** (« *The bird is freed* »), en référence au symbole graphique

du réseau social figurant un oiseau bleu. **Le commissaire européen** au marché intérieur alors en poste, Thierry Breton **répond** : « *En Europe, l'oiseau volera selon nos règles européennes.* » (« *In Europe, the bird will fly by our European rules.* »).

Le rachat de l'entreprise est accompagné par de **vives inquiétudes en matière de liberté d'expression** au regard des positions adoptées par Elon Musk. Le milliardaire a diffusé massivement de la désinformation pendant la pandémie de Covid_19, son entreprise Tesla a été poursuivie à de multiples reprises pour des cas de discrimination raciale et de harcèlement sexuel, et il est également accusé de management toxique au sein de son entreprise SpaceX.

Twitter commence alors à changer d'aspect. Musk débute sa prise de contrôle par le licenciement de trois de ses dirigeants – dont le directeur général. **Il annonce également vouloir assouplir la politique de modération de contenus de la plateforme.**

En juillet 2023, Elon Musk a rebaptisé la plateforme en « X » du nom de la banque en ligne devenue PayPal, qu'il a contribué à fonder, et dont le propriétaire est une figure aux engagements politiques libertariens assumés Peter Thiel

b. Des changements impulsifs conduisant X à favoriser les contenus haineux, violents et mensongers

Outre le changement de nom, Musk n'aura de cesse d'agir de façon impulsive à partir de son rachat

Une politique d'authentification de compte payante est également mise en place de façon extrêmement chaotique. Jusqu'alors, une encoche bleue permettait d'authentifier certains utilisateurs. Ceux-ci devaient être « *authentique, notoire et actif* », des critères vagues qui laissaient au réseau social une grande marge d'interprétation, mais qui permettaient tout de même de déceler facilement les usurpations d'identité. Dans certains cercles, et notamment parmi les sympathisants Républicains d'outre-Atlantique, être « *blue-checked* » devient un terme péjoratif de critique des élites libérales.

Après un sondage publié sur son propre compte X, Elon Musk entreprend de modifier ce système pour accorder ce macaron bleu ⁽¹⁾ à toute personne souscrivant un abonnement mensuel, ce que feront très massivement ces soutiens. Un changement ayant deux conséquences immédiates. D'abord, les comptes souscrivant à l'abonnement Twitter Blue sont largement promus dans les fils des utilisateurs, accroissant grandement leur visibilité. Ensuite, les usurpations d'identité se sont immédiatement multipliées, phénomène qui obligea même le report du lancement de l'abonnement. Ce système a d'ailleurs été l'objet d'une enquête de la Commission européenne, qui a adressé des conclusions préliminaires de violation du DSA à la plateforme, sans les faire suivre, à ce jour, de sanction.

(1) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761

La gestion des bannissements de comptes coupables de comportements et propos illicites est aussi l'objet d'une dérive marquée. Ainsi, le compte du rappeur Kanye West - devenu Ye - responsable de propos antisémites et pro-nazis est restauré. De multiples comptes bannis pour des discours extrémistes, complotistes ou haineux sont rétablis à l'image de celui de Donald Trump et de milliers de comptes suspendus ⁽¹⁾ après les émeutes du Capitole en janvier 2021. C'est le cas également de figures de l'extrême droite française et britannique.

Au nom d'une conception de la liberté d'expression très extensive, Elon Musk permet l'expression de toutes les opinions mais dans les faits favorise les paroles extrémistes des comptes justement bannis pour cette raison. *A contrario*, de multiples comptes critiques du milliardaires ou marqués à gauche sont eux bannis : en novembre 2022, il suspendait plusieurs comptes d'organisations antifascistes à la demande d'un influenceur d'extrême-droite qui les accusait d'incitation à la haine, quand il réactivait trois mois plus tard le compte de Mike Flynn, complotiste ayant participé à relayer de fausses informations sur l'attaque du Capitole.

À cette modération de l'arbitraire s'ajoute une politique de diminution structurelle de la modération de la plateforme : près de deux ans après le rachat de la plateforme, **l'entrepreneur peut se vanter d'avoir licencié 80 % des effectifs du réseau social**, et la moitié des effectifs en charge de la modération.

Sur ce point, **X a montré des lacunes majeures depuis le rachat de la plateforme par Musk**, qui a coïncidé avec l'entrée en vigueur du DSA. **Le rapport de transparence publié en 2023** (période août octobre 2023) a révélé un nombre de modérateurs francophones de 52 personnes (contre 2292 modérateurs anglophones).

S'agissant de la surveillance des contenus illicites, les chiffres bruts montrent une **inefficacité de la modération par X** similaire : 28 500 publications supprimées en 2 mois sur la plateforme d'Elon Musk contre 4 millions en 1 mois sur TikTok et pour Facebook et Instagram respectivement 46 et 76 millions de suppressions. Le premier rapport d'audit, daté de décembre 2024, met en exergue les mêmes travers.

En compensation des réductions des moyens alloués à la modération, X met en place en février 2023 les « *community notes* ». Lorsqu'un message est jugé trompeur, d'autres utilisateurs peuvent proposer une note attachée à la publication initiale et venant la corriger ou la nuancer. Elle est proposée quand un nombre suffisant d'utilisateurs, entre lesquels des désaccords ont déjà existés, la juge utile. Ce procédé est pourtant très limité. D'abord, les règles exactes d'admission d'une note de la communauté n'ont pas été publiées par le réseau social. Ensuite, une étude de chercheurs des universités du Luxembourg et de la Sorbonne ainsi que d'HEC a montré que la vitesse d'émission d'une note de la communauté est infiniment plus lente que la publication d'un message : 61,4 heures en moyenne. Enfin, ces notes peuvent être fausses ou tout simplement inexistantes sur un grand nombre de fausses

(1) <https://gizmodo.com/elon-musk-twitter-12000-banned-accounts-restored-data-1849848764>

publications : *NewsGuard* a démontré que sur 25 messages trompeurs à forte audience, postés en 2023 lors des débuts de la guerre entre Israël et le Hamas, seul l'un d'entre eux a reçu une note de communauté.

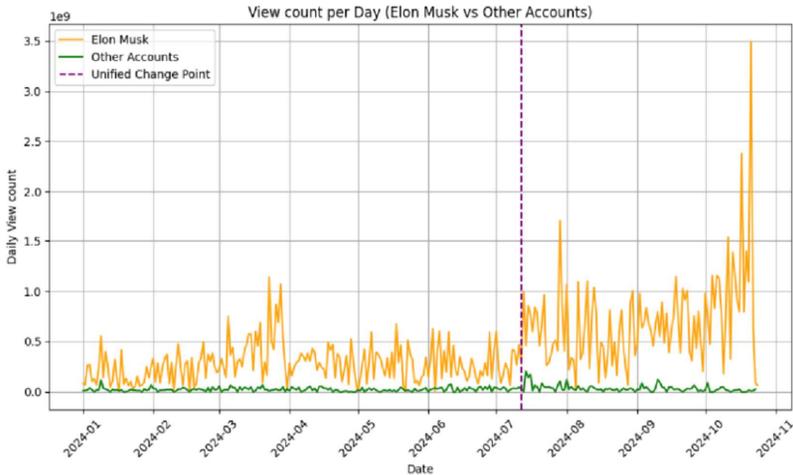
c. Des manipulations de l'algorithme au profit d'Elon Musk et de ses relais politiques

En février 2023, le média spécialisé *Platformer* ⁽¹⁾ va révéler, documents et témoignages d'employés à l'appui, qu'Elon Musk a demandé à ses équipes de travailler de manière urgente à la résolution d'un « problème d'engagement ». En cause, le dépassement du nombre d'impressions d'une publication du propriétaire de X par Joe Biden à propos du Super Bowl. La nuit même de cet évènement, il insistera pour que ses équipes proposent des solutions lui permettant d'obtenir une meilleure visibilité. Certains des employés auraient émis des réserves sur cette modification de l'algorithme, balayés par une menace directe de licenciement. Reste que les ingénieurs de X vont alors mettre en place en urgence des « *green lights* », c'est-à-dire des règles spéciales pour qu'un utilisateur soit favorisé en dehors des règles normales du jeu. Les premiers changements seront d'ailleurs ratés, puisqu'ils conduiront à inonder les fils d'actualités de tous les utilisateurs de X quasi exclusivement des publications d'Elon Musk la journée du 14 février 2023. À la tête de cette plateforme, les petits ressentiments peuvent conduire à truquer arbitrairement les règles du jeu.

Sa fréquence d'apparition dans les fils d'actualité des utilisateurs ⁽²⁾ va à nouveau croître considérablement lorsqu'Elon Musk annoncera son soutien à Donald Trump. L'algorithme sera à nouveau modifié pour favoriser ce soutien, comme va le démontrer une étude de l'Université Technologique de Queensland : à partir de juillet 2024, le nombre de vues du chef d'entreprise va augmenter de 138 %, ses retweets de 238 %, ses « *j'aime* » de 186 %, ce qui va bien au-delà de la tendance normale en période électorale.

(1) <https://www.platformer.news/yes-elon-musk-created-a-special-system/>

(2) <https://arxiv.org/pdf/2409.08781>
<https://www.newsguardtech.com/misinformation-monitor/october-2023/>



Au milieu d'une campagne dans laquelle Elon Musk prend activement le parti de Donald Trump, ce bouleversement des règles du jeu va également favoriser les Républicains, qui connaîtront une augmentation moindre mais toujours anormale de leurs statistiques. Nous observons donc un changement de paradigme où, à l'approche d'une élection, un chef d'entreprise a orienté sa plateforme au service de ses idées pour influencer un scrutin qui compte à peine plus d'électeurs que d'utilisateurs du réseau social.

d. Une omniprésence d'Elon Musk renforçant un facteur personnel de désinformation

Elon Musk est lui-même un facteur central de la désinformation sur X. Selon *Newsguard*, spécialisé dans la détection et l'étude des fausses informations, Elon Musk a relayé 17 récits identifiés parmi les fausses informations en circulation. Avec ses 219 millions d'abonnés, un chiffre qui a considérablement crû depuis le changement de l'algorithme à son profit et qui est quatre fois plus important que le nombre d'abonnés de *New York Times*, Elon Musk accorde pourtant une exposition démesurée à chacune de ses expressions.

Or, c'est aussi le cas des comptes avec lesquels il interagit. Sur les quatre comptes avec lesquels il échange le plus sur la plateforme, quatre sont des commentateurs conservateurs ayant relayés sept à douze fausses informations répertoriées comme telles. Sur la même période, de janvier à juin 2024, ces comptes ont d'ailleurs profité de « l'effet Elon Musk » en connaissant une augmentation allant jusqu'à 30 % de leur nombre d'abonnés. S'agissant de la campagne électorale qui avait alors lieu, le *Center for Countering Digital Hate* a décompté pas moins,

plus de 50 fausses informations sur le scrutin, relayées par Elon Musk, ayant été vues au cumulé 1,2 milliard de fois.

La fréquence à laquelle il est susceptible de relayer de fausses informations peut exploser selon le contexte, comme lors de l'attaque du 7 octobre 2023 ou après la tentative d'assassinat dont a fait l'objet Donald Trump. À ce moment, du 16 au 20 septembre, le *New York Times* a noté pas moins de 171 messages faux ou trompeurs écrits ou relayés par le chef d'entreprise. L'agence Bloomberg l'a souligné dans une analyse de ses tweets durant la campagne américaine, où il évoquait dans 1 300 de ses publications « *l'importation d'électeurs* ». Il s'agit d'une **théorie complotiste selon laquelle les démocrates conspiraient pour faire illégalement voter des immigrants** ⁽¹⁾ ⁽²⁾.

e. La récente opacité de X et le refus de l'étude de son contenu

Un autre changement de politique appliqué par Twitter a eu des conséquences particulièrement préjudiciables : le basculement vers un statut d'**API fermée**. Une API (« *application programming interface* » en anglais) désigne une interface de programmation permettant à un tiers de développer des applications à partir des données fournies par la plateforme.

L'impact de cette décision, intervenue en février 2023, s'apprécie à différents niveaux. Les *bots* et outils tiers basés sur l'API ne sont plus utilisables gratuitement. Plusieurs comptes retraçant les bilans carbone d'avions de milliardaires, dont celui d'Elon Musk, étaient particulièrement populaires et suivies ce qui pourrait être une part de l'explication. Musk avait d'ailleurs fait censurer certains de ces comptes, appartenant parfois à des journalistes, avant de les ré-autoriser sous la pression publique.

Cette décision impacte également les chercheurs qui utilisaient ces API pour analyser les données de Twitter comme base de données. Pour comprendre les fonctionnements des algorithmes, dont on a vu que ses critères avaient une importance dans le débat public, deux méthodes sont possibles. L'une est le « *scraping* », c'est-à-dire la collecte d'échantillons d'informations présentes sur le réseau social, pour en déduire le fonctionnement. L'autre est de créer une interface de programmation, ou API, permettant de connecter le réseau social à d'autres applications, dont des outils d'analyse qui vont puiser dans les données auxquelles les API leur donnent accès. La seconde option est de loin la plus efficace, car la collecte de données est bien plus aisée.

C'était sur cette API de Twitter que reposaient un grand nombre de projets, de recherche ou commerciaux, ou encore une grande part du travail des gestionnaires de la visibilité publique (*community managers*). Mais c'est aussi et

(1) <https://www.newsguardtech.com/fr/special-reports/elon-musk-coup-de-pouce-super-propagateurs-infox/>

(2) <https://www.nytimes.com/2024/09/27/technology/elon-musk-x-posts.html> cité par <https://www.nytimes.com/2024/09/27/technology/elon-musk-x-posts.html>

surtout à partir de cette API que les chercheurs analysaient le fonctionnement du réseau social, pour en décrire le fonctionnement et identifier ces biais. Une contribution fondamentale au débat public. C'est par exemple avec cette API que le Politoscope, outil d'analyse du CNRS, a pu déceler certaines ingérences et débats insincères dans la campagne présidentielle française de 2022.

Il apparaît donc que **ce changement de politique n'est pas neutre en termes d'utilisation de données**. Il révèle clairement une **politique de fermeture**, si ce n'est de dissimulation, de la part de X qui s'assure ainsi que la « boîte noire » de l'algorithme ne soit plus accessible et analysable facilement.

Le changement de politique en la matière est d'autant plus notable qu'historiquement X se distinguait des autres plateformes en pratiquant une politique d'ouverture. Ainsi, Facebook (groupe Meta) n'a jamais permis cette possibilité obligeant les chercheurs analysant les données à utiliser des méthodes coûteuses en temps et en énergie. De 2007 à 2023, X a donc constitué un modèle d'expérimentation particulièrement fécond pour la recherche.

Au-delà de la recherche, **l'API donnait une vue sur les tendances du débat**, notamment les biais idéologiques et de négativité. Le degré de technicité et de complexité de gestion des données nécessite une politique d'ouverture des données pour que cette gestion soit réalisable.

Ce travail aura d'autant plus d'intérêt que, ainsi que l'a fait observer **votre rapporteur Jérémie Jordanoff** au cours de l'audition de David Chavalarias, **il existe des chambres d'échos numériques dont les plateformes sont les points de départ**. Elles permettent alors de mener des démarches d'intimidation auprès de chercheurs, par exemple, tout en prenant la défense de régimes hostiles à la France. Ces chambres d'échos sont limitées en taille mais les réseaux sociaux les grossissent à l'excès aboutissant à **bouleverser l'écosystème informationnel et à mettre à l'agenda médiatique et politique des sujets montés de toutes pièces**.

f. Malgré les empêchements, une évolution détectée des opinions représentées sur X depuis son rachat

Plusieurs outils ont tenté d'analyser l'évolution des contenus du réseau social avant la fermeture de l'API puis après, grâce à la méthode dite de *scrapping*. Le mathématicien **David Chavalarias**, mathématicien et chercheur au CNRS spécialisé dans l'étude des réseaux sociaux et créateur de l'observatoire le Politoscope, a notamment montré comment **le fonctionnement et la manipulation des algorithmes ont favorisé l'essor du climato-scepticisme sur la plateforme**. Parmi les comptes ré-autorisés, certains font partie de la mouvance climatosceptique et ont ainsi pu publier à nouveau leurs messages. Leur proportion dans l'ensemble des tweets est passée à 50 % d'après les données du mathématicien.

La situation prend cependant une tournure particulièrement dramatique à l'occasion du retour au pouvoir de Donald Trump en novembre 2024. Après une campagne électorale marquée par une violence redoublée, le candidat républicain

est revenu à la Maison Blanche avec un soutien de campagne marqué de la part d'Elon Musk. Comme Musk, un ensemble de soutiens de Donald Trump pousse à une interprétation maximaliste, et orientée, de la liberté d'expression.

Ainsi, au nom de cette vision, certains discours trouvent une caisse de résonance particulière. Dès lors que X – tout comme Meta au demeurant – amplifient les dimensions d'un discours empreint d'une forte toxicité, ils contribuent à la virilisation de discours caractérisés par la haine, le dénigrement, l'humiliation ou toute autre passion triste, ainsi que l'a fait observer David Chavalarias, au cours de son audition par vos rapporteurs.

Le fil d'actualité, évoqué précédemment, se caractérise désormais par une surreprésentation de messages agressifs. L'aspect particulièrement nocif de cette situation est qu'elle n'est, en outre, pas représentative de la réalité puisqu'il s'agit d'un phénomène « boosté » par les algorithmes. L'utilisateur se retrouve confronté à des niveaux de toxicité qui ne représentent pas ses propres interactions mais celles que la plateforme veut lui imposer. Le problème prend alors une nature systémique en atteignant chacun.

Cette surreprésentation de la toxicité par l'algorithme du réseau social et la croissance du phénomène depuis la prise de contrôle d'Elon Musk est avérée. Une étude du CNRS parue dans la revue *Nature* montre, données à l'appui, que le fil d'actualité est 49 % plus toxique (insultes, attaques personnelles, obscénités, etc.) que ce que produisent les abonnements. Ce biais n'était que de 32 % avant le rachat de Twitter par Elon Musk. **Cela montre que ce n'est pas les préférences ou les actions des utilisateurs qui les exposent à du contenu toxique, mais bien la façon dont fonctionne la plateforme.**

Or, le type de contenu consommé influe directement sur les comportements électoraux. Une étude également parue dans *Nature* ⁽¹⁾ prouve que l'utilisation du réseau social conduit à une diminution du bien-être, un sentiment d'appartenance accru, la polarisation politique et l'indignation.

Parmi les autres facteurs d'influence des comportements électoraux, vos rapporteurs attirent l'attention de la représentation nationale sur la pratique de la suppression d'électeurs. Largement utilisée par l'extrême-droite américaine, mais dans d'autres mesures par tous les camps politiques, cette méthode consiste à exposer un utilisateur indécis à une grande quantité de contenu mettant en cause le candidat pour lequel il hésite de voter, le décourageant ainsi à le faire.

Ce fut par exemple le cas en 2017 quand, à partir d'un forum internet, des membres de *l'alt-right* se coordonnent avec des militants de l'extrême-droite française pour inonder les réseaux d'illustrations caricaturant le candidat Emmanuel Macron à l'approche du second tour des élections. Destinés aux électeurs de Jean-Luc Mélenchon au premier tour, ils mettaient en scène les aspects d'Emmanuel

(1) <https://www.nature.com/articles/s44271-024-00062-z#Sec18>

Macron les plus négatifs pour ces électeurs, afin de les décourager d’aller voter à nouveau au second tour.

Lors de l’élection présidentielle américaine, *l’American Sunlight Project* ⁽¹⁾ a identifié 1 200 comptes dont le profil et l’activité permettent de les identifier en tant que robots. Auteurs de 100 millions de postes favorables à Vladimir Poutine ou Donald Trump, ces robots relayaient massivement des contenus dénigrant Kamala Harris notamment auprès de la communauté afro-américaine, pour freiner sa mobilisation.

Ainsi, le débat politique n’est plus très attaché à la conviction, ni à la vérité, mais aux contenus parfois erronés qui, répétés suffisamment, installent le doute et la suspicion à l’égard d’un candidat. Plus grave encore, cette méthode n’est pas employée que par des militants politiques : elle peut être additionnée à un recours plus ou moins important de robots, potentiellement dirigés par des puissances étrangères ⁽²⁾.

g. Après la victoire de Donald Trump, la présence d’Elon Musk à la Maison Blanche et des ingérences dans les pays européens

Le soutien de Musk lui a d’ailleurs assuré une place de choix comme responsable du Département de l’Efficacité gouvernementale (*Department of Government Efficiency* dit DOGE) au risque d’un conflit d’intérêts évident. Cette structure a entrepris de licencier de façon indiscriminée les fonctionnaires jugés responsables de gabegie et en discordance avec la nouvelle administration.

Le rachat de la plateforme par Musk a donné à son discours une visibilité pouvant être particulièrement nocive. Un exemple très illustratif est la véritable cabale politique lancée par le milliardaire à l’encontre du Premier ministre britannique Keir Starmer à la fin de l’année 2024.

Réutilisant un sombre fait divers des années 1990 – un gang de pédocriminels sévissant dans le nord de l’Angleterre –, Musk a multiplié les attaques contre Starmer l’accusant de complicité, au titre de sa fonction de directeur des poursuites judiciaires publiques (procureur général) entre 2008 et 2013.

Mêlant fausses informations et ingérences étrangères, cette campagne de diffamation a atteint son acmé en janvier 2025 quand Elon Musk est allé jusqu’à réclamer la prison pour le premier ministre s’ingérant ainsi sciemment dans les affaires britanniques. L’écho donné aux comptes promouvant cette théorie conspirationniste a contraint le gouvernement Starmer à réagir.

(1) <https://static1.squarespace.com/static/6612cbdfd9a9ce56ef931004/t/6706f63421222b6005cefbcf/1728509499727/ASP+Sleeper+Agents+Report.pdf>

(2) <https://www.nature.com/articles/s41598-023-43980-4>

Cette campagne est à mettre en lien avec la figure de l'extrême droite britannique Tommy Robinson qui soulignait de façon répétée l'origine ethnique des agresseurs et celle des victimes afin d'attiser la haine raciale. Cette campagne a surgi quelques mois après plusieurs émeutes racistes à l'été 2024 que Musk a encouragé en leur donnant une visibilité renforcée.

Par ailleurs, le désormais vice-président James David Vance n'a pas hésité, dès septembre 2024, à affirmer que les États-Unis pourraient retirer leur soutien à l'OTAN si l'Europe persistait à vouloir appliquer la régulation numérique à la plateforme d'Elon Musk.

Elon Musk lui-même a pris un ensemble de positions de nature politique. Quelques semaines avant les élections générales allemandes du 26 février 2025, l'entrepreneur a donné une visibilité sans égale à la candidate du parti néonazi Alternative pour l'Allemagne (*Alternativ Für Deutschland, AFD*) Alice Weidel en expliquant que : « *Seule l'AFD peut sauver l'Allemagne* ». La prise de position a été ressentie, à juste titre, comme une ingérence dans le processus électoral allemand et a fait l'objet d'une forte réprobation en Allemagne.

De même, Elon Musk a qualifié à de multiples reprises l'ancien commissaire européen Thierry Breton, et architecte des DSA et *Digital Markets Act* (DMA), de « *tyran de l'Europe* » parce qu'il réaffirmait de façon constante son souhait de voir la législation numérique appliquée.

Sa vision idéologique peut d'ailleurs être **résumée par la phrase qu'il avait prononcée**, « *vous êtes le média désormais* ⁽¹⁾ », en s'adressant aux utilisateurs des plateformes. Comme le souligne, l'historien des médias Fabrice d'Almeida ⁽²⁾, **Musk considère que les faits et les opinions sont similaires** et qu'aucune discrimination ne peut être faite entre les deux. Cette façon de **promouvoir des opinions en les « factuaisant »** va à l'encontre du principe de construction des médias de masse depuis le XVIII^e siècle : « *une information pour exister doit être vraie et doit refléter un état universel de l'opinion* ».

C'est en vertu de ce principe que la France a adopté la loi de 1881 avec notamment la lutte contre les fausses informations, évoquées précédemment, et que les États-Unis eux-mêmes, entre 1949 et 2011, faisaient prévaloir la « *Fairness Doctrine* » ou doctrine d'honnêteté.

L'inquiétude concernant la capacité du DSA à perdurer s'est plus encore renforcée suite au **discours tenu par JD Vance à l'occasion de la traditionnelle conférence sur la sécurité à Munich** qui s'est tenue du 14 au 16 février derniers.

(1) « *You are the media now* ».

(2) *La Croix, Tribune* publiée le 4 février 2025

Dans un discours aux **accents sombres et aux propos mensongers**, le vice-président américain a réitéré les attaques à l'encontre de Thierry Breton allant jusqu'à lui prêter des propos jamais tenus.

De façon claire, le vice-président s'est ingéré dans les affaires européennes avec un propos ayant particulièrement retenu l'attention : « **La menace qui me semble la plus inquiétante pour l'Europe n'est ni la Russie, ni la Chine. La menace qui m'inquiète le plus vient de l'intérieur : l'Europe s'éloigne de ses valeurs les plus fondamentales.** »

Il a également prononcé les propos suivants : « **Je pense à Bruxelles, où les commissaires avertissent les citoyens qu'ils comptent couper l'accès aux réseaux sociaux en période de troubles dès lors qu'ils détectent ce qu'ils jugent être, je cite, « des contenus haineux ».** Vance s'attaque ainsi à la base du DSA luttant contre les contenus illicites. En version originale, **Vance évoque des « commissars »** pour évoquer les commissaires européens, terme utilisé habituellement en anglais pour désigner les **commissaires politiques de l'URSS.**

Plus loin, il déclare : « *À Washington, il y a un nouveau shérif. [...] Si votre démocratie peut être détruite avec quelques centaines de milliers de dollars de publicité en ligne venant d'un pays étranger, c'est qu'elle n'est pas très solide.* »

Le discours tenu à Munich fera sans doute date dans les relations euro-transatlantiques. Plus spécifiquement, il illustre bien la menace qui plane sur le DSA et que X incarne désormais. Au-delà, **le discours de Vance en louant le Brexit, en s'opposant au « cordon sanitaire » (brandmauer) contre l'extrême droite en Allemagne ou en fantasmant la menace d'une immigration incontrôlée**, rend tangibles les efforts américains de mettre fin à la législation numérique, quitte pour cela à utiliser la menace du chantage.

Et la toute récente déclaration, le 3 mars dernier à Barcelone lors du *Mobile World Congress* **du nouveau président de la Commission fédérale des communications (FCC) Brendan Carr**, ne fait que s'inscrire dans la ligne tenue par l'administration Trump.

Carr a ainsi affirmé que **le DSA serait à la fois incompatible avec la liberté d'expression et « avec les engagements pris par les entreprises en faveur de la diversité d'opinions ».** Cette nouvelle déclaration fait notamment suite au **mémorandum de Donald Trump**, publié le 21 février dernier, visant à exercer des représailles douanières contre les pays imposant aux entreprises technologiques américaines ce que le président américain qualifie « *d'extorsions et amendes injustes* ».

Il convient de souligner que **la nouvelle idéologie promue par l'administration Trump a infusé au sein de l'ensemble de l'écosystème des géants du numérique américain** puisque le fondateur de Meta Mark Zuckerberg a également fait volte-face *a contrario* de l'attitude qu'il avait adoptée devant le

Congrès en 2021, lorsqu'il envisageait la possibilité de limites à la liberté d'expression.

Dans une sorte de « serment d'allégeance » à Trump – pour reprendre les mots d'une des personnes auditionnées – Zuckerberg a mis fin à sa politique de modération active préférant désormais diffuser des notes de la communauté, comme X, rédigées par des utilisateurs et au crédit très relatif.

2. Le réseau social TikTok exerce une influence problématique caractérisée par une collecte massive de données personnelles et un algorithme captivant le public

Application de partage de vidéos courtes, **TikTok est créée en 2016** par l'entreprise chinoise ByteDance **à destination d'un public non-chinois**. Le réseau social connaît son succès **grâce à un algorithme de recommandation** qui favorise la viralité des contenus.

La spécificité du réseau consiste à panacher deux modèles analysant les goûts personnels en fonction des vidéos regardées d'une part, en exploitant les données issues des interactions avec d'autres personnes d'autre part. **La collecte de données par l'application** lui permet de nourrir en permanence les nouveaux contenus affichés pour l'utilisateur.

Le profilage des utilisateurs est particulièrement fin ainsi que plusieurs chercheurs l'ont observé. Les aspects problématiques de TikTok, bien que communs avec les réseaux sociaux, se caractérisent surtout par **l'intensité de l'exploitation des données**.

Les données recueillies doivent être indiquées à l'utilisateur et de façon détaillée en vertu du règlement général sur la protection des données personnelles (RGPD). Pourtant, **dans le cas de TikTok, les conditions générales d'utilisation et la politique de confidentialité se caractérisent par un certain flou** qui ne permet pas de connaître de manière exhaustive l'ampleur de la collecte.

En outre, **l'application pratique une collecte de données directement à la source via le système d'exploitation de l'appareil** (Android ou IOS) permettant d'accéder à un nombre de fonctionnalités et d'informations très importantes.

Des analyses réalisées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) tchèque ont révélé une **masse excessive de données collectées** et notamment la capacité à détecter l'installation de certaines applications tierces (« *mappage* »), la vérification régulière de la géolocalisation ou encore l'accès à l'agenda de l'utilisateur.

Cette large collecte interroge sur les finalités poursuivies. L'utilisation de l'application ne nécessite pas autant de données sauf à poursuivre d'autres objectifs. D'ailleurs, des articles de presse publiés en 2022 ont fait état de **captation**

des frappes des utilisateurs. Une telle possibilité ouvrirait la voie à l'accès à des données particulièrement sensibles (carte bancaires, par exemple).

Les informations ainsi recueillies par TikTok lui permettent un profilage extrêmement précis des utilisateurs. Ces informations sont réutilisées par l'application dans sa politique de modération de contenu ainsi que pour de la **publicité ciblée**. L'application en vient ainsi à **segmenter les utilisateurs en créant des groupes de personnes qu'elles peuvent captiver** avec des contenus dédiés.

La finesse de l'algorithme de recommandation a été très largement observée, notamment par la Commission nationale de l'informatique et des libertés (CNIL). **La performance de l'algorithme s'évalue à travers les goûts et réactions de l'utilisateur qu'il parvient à saisir.** Cela lui donne un pouvoir de prédiction particulièrement élevé. La finesse de l'analyse – notamment à travers le temps de visionnage – lui permet d'affiner les recommandations.

La rapidité de l'enrichissement des données est également permise par le format très court des vidéos diffusées. Originellement, le format était de 15 secondes, puis il a été progressivement augmenté jusqu'à 10 minutes (2022). Le format très court est cependant largement privilégié par les utilisateurs.

TikTok est en mesure de connaître le profil psychologique de l'utilisateur selon Viginum, service de surveillance des ingérences numériques. La structure a ainsi remarqué que même les mouvements de souris étaient enregistrés donnant ainsi l'image d'une plateforme où aucune information n'échappe à l'enregistrement et à l'analyse.

Cette performance ultra-sensible permet de manière certaine **la captation de données biométriques ou émotionnelles** dans la mesure où la voix et le visage sont enregistrés par le biais des vidéos. Il s'agit d'un point sensible et particulièrement inquiétant au regard de ses utilisations possibles pour l'algorithme. **Cette utilisation est susceptible de révéler les affiliations politiques, philosophiques et religieuses ainsi que l'appartenance sexuelle d'une personne.**

Disposer de données aussi personnelles est un outil particulièrement utile à l'application puisqu'il permet de calibrer la publicité ciblée de manière extrêmement précise sans même que l'utilisateur n'en ait conscience.

Une autre dimension inquiétante se révèle à travers **l'exploitation des données et son stockage. TikTok partage les données recueillies avec des parties tierces hors de l'espace européen** ce qui accroît les risques d'ingérences. De plus, les pays exploitant les données recueillies ne disposent pas nécessairement de décisions d'adéquation avec l'Union européenne reconnaissant l'équivalence des législations en matière d'usage des données.

À l'évidence, **la situation est loin d'être satisfaisante** en la matière et nécessite de remédier à ces lacunes de protection majeures en contradiction avec les normes que l'Union s'est fixée.

En outre, **les transferts de données sont également susceptibles de se produire lors de cyberattaques**. La résilience de la structure de TikTok a déjà été mise à l'épreuve avec une fuite de données observées lors d'attaques numériques.

La collecte de données a alerté CNIL à plusieurs reprises aboutissant à une condamnation partielle de TikTok en raison de la non-conformité constatée dans l'utilisation des cookies et autres traceurs, allant à l'encontre de la loi informatique et libertés (1978) et du RGPD.

Plusieurs autorités de protection des données (Italie et Pays-Bas notamment) se sont également alertées de **l'absence de protection spécifique à l'égard des mineurs**, considérés comme un public particulièrement vulnérable.

En 2021, l'autorité italienne avait imposé une suspension de tous les traitements de données provenant de personnes dont l'âge ne pouvait être établi avec certitude, en vertu de l'article 66 du RGPD, après la survenue d'un fait divers particulièrement tragique impliquant une enfant de 10 ans et l'application TikTok.

Depuis, et ce, à plusieurs reprises, TikTok a été condamné pour violation de la vie privée de jeunes enfants (Pays-Bas) et utilisation illégale de données personnelles d'enfants (Grande-Bretagne). Deux procédures, actuellement en cours, concernent le transfert de données de mineurs vers la Chine.

S'agissant de l'algorithme de recommandation, il figure comme l'un des atouts clés de l'application, ainsi que nous le soulignons plus tôt, étant donné son degré de précision. Cet algorithme a été lancé en 2018 et **utilise les ressources de l'intelligence artificielle** en pratiquant l'apprentissage automatique pour personnaliser les contenus suggérés et en tenant compte des interactions des utilisateurs. Le mode de fonctionnement de l'algorithme de TikTok lui fournit des données particulièrement entraînées.

Certains chercheurs considèrent que **ce mode d'exploitation des données ne fait que renforcer les convictions de l'utilisateur l'enfermant alors dans une bulle** et participant d'un phénomène d'addiction à l'application.

L'algorithme présente une autre caractéristique particulièrement dommageable : son **opacité**. Il est impossible d'en connaître la construction exacte, ni le lieu de stockage des données, vraisemblablement en Chine. **L'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) a critiqué le processus d'évaluation des algorithmes qui reste inaccessible au public.**

Cette absence d'informations sur l'algorithme est d'autant plus dommageable que **la présence de contenus manifestement faux est avérée sur la plateforme** et que la responsabilité des algorithmes est donc posée. L'asymétrie d'informations concernant ce type de plateforme est à opposer à la transparence des médias d'informations.

En outre, comme sur la plateforme X, **des contenus sont invisibilisés par l’algorithme de recommandation** (processus de *shadowbanning*). Ce phénomène est à mettre en regard de la réduction de la visibilité de certains contenus que la plateforme reconnaît pratiquer. Ainsi, en Russie pour respecter la loi locale édictée par le pouvoir autoritaire de V. Poutine, TikTok a modéré le contenu de façon évidente afin d’éviter toute possibilité, pour l’utilisateur d’accéder à des contenus internationaux critiques de la guerre en Ukraine.

Avec le DSA, **la plateforme est cependant tenue de mettre en place des mécanismes de partage de données avec des chercheurs**, permettant ainsi d’ouvrir la boîte noire de son algorithme. L’article 40 du DSA prévoit des explications sur la conception, le fonctionnement et la procédure de test des systèmes algorithmiques. L’accès aux données doit être facilité à travers des interfaces dédiées. Au regard de son statut de fournisseur de très grande plateforme, l’application est tenue à plus d’obligations encore. Nous reviendrons dans la deuxième partie du rapport sur ces éléments.

Enfin, **un autre point de vigilance particulièrement inquiétant concernant TikTok est celui de sa lutte contre la désinformation**. Le cadre légal français lui impose, depuis la loi du 22 décembre 2018 dite Loi Avia sur les fausses nouvelles, la mise en place d’un dispositif de signalement des contenus relatifs à la manipulation de l’information et le déploiement de mesures complémentaires en matière de transparence sur les actions menées contre le phénomène.

L’ARCOM joue un rôle, en lien avec ses homologues européens, dans la mise en œuvre du **code européen renforcé des bonnes pratiques contre la désinformation**. L’autorité administrative indépendante a jugé ⁽¹⁾ que les mesures mises en œuvre par l’entreprise étaient « *particulièrement imprécises* ».

Aucune information n’a été apportée concernant **les pratiques de manipulation identifiées sur l’application**. Il existe des dispositifs automatisés pour détecter, bloquer et supprimer les comptes considérés comme faux. Cependant, il n’est pas possible d’en juger de la pertinence au regard du peu d’informations données les concernant. L’ARCOM a également estimé que **le dispositif de signalement était caractérisé par un manque de visibilité**.

Des études complémentaires à celles de l’ARCOM ont mis en exergue la lutte relativement inefficace contre la désinformation menée par TikTok. Ainsi, la société américaine *NewsGuard* évaluant la fiabilité des contenus des sites d’information a souligné, en septembre 2022, **la présence massive de contenus manifestement faux**.

Son étude a également souligné que **la visibilité de ces contenus était élevée** puisque le délai au terme duquel ces contenus étaient proposés à l’utilisateur était particulièrement rapide. Cet élément est d’autant plus perturbant que TikTok

(1) *Bilan annuel des moyens et mesures mis en œuvre par les opérateurs de plateforme en ligne en 2021, ARCOM, Novembre 2022.*

constitue, pour une tranche conséquente de la population, de source d'information (75 % des utilisateurs américains de moins de 30 ans, selon une étude du *Pew Research Center*). Une étude réalisée en 2023 par l'Institut français d'opinion publique (IFOP) et la Fondation Jean-Jaurès a mis en exergue le lien de causalité entre la proportion du jeune public accreditant des théories conspirationnistes et leur mode d'information (TikTok).

Une étude américaine ultérieure a mis en avant le fait que TikTok était la plateforme la moins outillée pour lutter contre la désinformation et qu'elle présentait bien plus de contenus faux que Facebook, par exemple. Au regard du **nombre de personnes pratiquant la modération au sein de l'application** (600 selon la plateforme), il convient de se demander comment la première peut être aussi inefficace.

Le rapport de transparence de l'application, publié en 2022, renseigne sur le phénomène puisqu'il apparaît que **85 à 95 % des contenus retirés l'ont été par des interventions non-humaines** (intelligences artificielles). Il s'avère que l'intelligence artificielle est beaucoup moins efficace pour lutter contre la désinformation qu'un modérateur humain. L'algorithme mettant en avant des contenus à la plus grande viralité, il est porté à mettre en avant les contenus les plus problématiques.

En outre, **le Parlement européen a souligné** dans le rapport de la commission spéciale sur les ingérences étrangères de mai 2023 que **l'application était vulnérable aux ingérences étrangères** en pratiquant une politique de modération aussi peu dynamique.

La proportion de contenus signalés comme faux et effectivement retirés est négligeable pour l'année 2022 (1 %). Des comptes problématiques, et signalés à de multiples reprises, demeurent actifs sur la plateforme, à l'image du groupe Wagner. La labellisation des contenus est très imparfaite : des médias d'informations étatiques chinois ne sont pas étiquetés comme tels.

Enfin, **la politique assumée de TikTok consistant à s'adapter à la loi locale la conduit à pratiquer une censure** de certains contenus afin de pouvoir poursuivre ses activités. Il conviendrait que l'algorithme soit étudié aussi à travers cette dimension.

En définitive, l'application à travers sa conception et ses pratiques posent de sérieux questionnements quant à son encouragement à la désinformation et à sa vulnérabilité marquée face aux ingérences étrangères.

Il convient de souligner que **la pratique des affaires dans un régime dictatorial, celui en vigueur en Chine, interroge sur les intentions du pouvoir en place**. S'agit-il d'utiliser **TikTok comme un cheval de Troie** ?

DEUXIÈME PARTIE : LA LÉGISLATION SUR LE NUMÉRIQUE PROPOSE UN CADRE JURIDIQUE RENOUVELLE QUE VOS RAPPORTEURS SOUHAITENT AMÉLIORER

A. UNE NOUVELLE LÉGISLATION EUROPÉENNE SUR LE NUMÉRIQUE

1. Une nécessaire législation : remédier à l'obsolescence du règlement de 2000 et aller au-delà des simples codes de conduite

En dépit de la multiplication des législations nationales en matière de lutte contre les contenus illicites, **le constat de fragmentation juridique** rendait nécessaire une initiative européenne.

En effet, **le cadre européen en matière de réglementation sur les services numériques avait été fixé par la directive 2000/31/CE dite « directive sur le commerce électronique »** (directive e-commerce). Le texte de la directive avait fixé deux principes majeurs : **la liberté de fourniture de services électroniques et la liberté d'établissement.**

Un régime de responsabilité limité, évoqué précédemment, avait été instauré pour les hébergeurs, c'est-à-dire ceux qui stockent des informations fournies par un destinataire de service. Outre ce principe était posée **une interdiction de surveillance généralisée des contenus.**

Enfin, les prestataires de services de la société de l'information devaient se conformer à la législation de leur pays d'établissement en vertu du **principe dit du pays d'origine**. Ce principe constituait la **pièce angulaire du marché des services numériques.**

Ce cadre, pour structurant qu'il soit, **n'était cependant plus adapté à l'époque.** Considérons ainsi le fait que lors de l'adoption de la directive, Google était encore une jeune entreprise (créée en 1998), Amazon n'existait que depuis trois ans et plusieurs géants de l'Internet n'existaient pas encore à l'image de Facebook, Twitter ou même Instagram.

L'écosystème des fournisseurs de services en ligne a été profondément modifié avec l'arrivée de ces acteurs. De plus, le régime de responsabilité mis en place au nom de l'innovation et de la croissance a surtout bénéficié aux grandes entreprises américaines qui en sont venues à occuper l'essentiel du marché.

De même, **la Cour de Justice de l'Union européenne (CJUE)** est venue, à de multiples reprises, interpréter les dispositions de la directive qui étaient en discordance avec les nouveaux acteurs d'Internet.

La nouvelle législation sur le numérique a également été rendue nécessaire par **le constat d'insuffisance des codes de conduite.** Mis en place en **2016**, **un premier code vise à combattre les discours de haine illégaux en ligne.**

Initialement, quatre entreprises des technologies de l'information avaient adhéré à cette démarche - Facebook, Microsoft, Twitter et YouTube – afin de lutter contre la prolifération des discours de haine à caractère raciste et xénophobe en ligne.

L'objectif de ce code est de **veiller à la suppression rapide des contenus jugés illicites** au regard des règles d'utilisation de la plateforme voire des contenus contrevenaient aux lois nationales ou européennes en la matière.

En 2018, un nouveau code de conduite a été mis en place pour lutter contre la désinformation en ligne, à la suite du scandale de *Cambridge Analytica* (exploitation des données d'utilisateurs de Facebook) et de l'ingérence russe dans l'élection présidentielle américaine de 2016.

Le code fait le constat de campagnes de désinformation en ligne, à l'initiative d'une pluralité d'acteurs, et **instaure cinq engagements**. Il définit la désinformation comme des « *informations manifestement fausses ou trompeuses* » dans le but de tromper le public d'une part, et de causer des dommages à cette même opinion publique dans le cadre de processus politiques et démocratiques d'autre part.

Les cinq engagements énoncés consistent à contrôler les affectations publicitaires, à assurer la transparence en matière de publicité politique, à assurer l'intégrité des services (suppression des faux comptes notamment), à investir dans la hiérarchisation des contenus pertinents et à soutenir les efforts de recherche en matière de lutte contre la désinformation.

En dépit de la pertinence de la démarche, **il est vite apparu que ce code de conduite ne serait pas suffisant**. Les évaluations faites par la Commission européenne portant sur leur efficacité ont constaté des lacunes. Elles ont surtout démontré que **le principe facultatif d'adhésion aux engagements** du code rendait ces derniers peu appliqués.

Il convient toutefois de noter que **le code de conduite de lutte contre la désinformation est devenu opposable depuis la fin de janvier 2025**, comme l'a souligné le président de l'Autorité de régulation et de surveillance des contenus audiovisuelles et numériques (ARCOM) lors de son audition.

2. L'architecture de la nouvelle législation sur le numérique : des obligations contrôlées à l'échelon national et à l'échelon européen

Fort des constats précédemment faits, il a paru dès lors pertinent de **choisir l'échelon européen pour adopter une réglementation harmonisée** et susceptible de **fixer un cadre face aux géants américains**. En effet, une nouvelle législation permet d'afficher des valeurs et d'envoyer des signaux clairs aux autres acteurs, qu'ils s'agissent d'acteurs étatiques ou d'acteurs privés.

Ainsi, la garantie que ce qui est illégal hors ligne le serait également en ligne constitue le principe de base de la législation sur les services numériques. **La liberté**

pour les citoyens de disposer de leurs données constitue un autre aspect. Enfin, la double affirmation d'un principe de confiance et de transparence fixe le cadre général.

Il s'agit d'une reprise partielle des principes de la directive de 2000, et notamment du plus essentiel d'entre eux : **le principe de responsabilité limitée des fournisseurs de services en ligne**.

La mobilisation à l'échelle européenne évite une fragmentation du marché intérieur du numérique, écueil redoutable pour les entreprises opérant sur le sol européen, les conduisant à faire face à vingt-sept législations différentes avec des obligations non harmonisées.

Le DSA s'inscrit dans une stratégie globale de la Commission européenne visant à **créer un écosystème protecteur applicable aux citoyens et favorable aux entreprises**. Plusieurs textes font ainsi partie de cette stratégie : **le règlement sur les services numériques (DSA), le règlement sur les marchés numériques (Digital Markets Act, DMA)**, le règlement pour la gouvernance des données et la proposition de règlement sur l'intelligence artificielle (adoptée en 2024).

Le principe guidant le DSA est celui **d'une évaluation par le risque**. Afin de lutter contre les contenus illicites, un **renforcement des obligations de modération** est mis en place ainsi que des **obligations de vigilance** (*due diligence*) notamment en matière de transparence et de moyens.

Il convient ici de noter que **le texte ne comporte pas de définition des contenus illicites** renvoyant pour cela aux législations nationales. Le règlement se contente, à l'article 3, de définir ainsi : « *toute information qui, en soi ou par rapport à une activité [...] n'est pas conforme au droit de l'Union ou au droit d'un État membre [...]* ».

Les obligations prévues par le DSA varient en fonction de la nature et de la taille des fournisseurs de services en ligne concernés. Des prescriptions sont posées telles que la désignation d'un point de contact unique, des obligations minimales concernant les conditions générales d'utilisation (art. 12) et de retrait de contenus (art. 13), ou encore l'obligation de répondre aux injonctions d'agir contre les contenus illicites émanant d'autorités nationales administratives ou judiciaires (art. 8 et 9).

Le texte distingue une **nouvelle catégorie d'acteurs, les plateformes en ligne**, qui non seulement stockent des informations (hébergeurs) mais les diffusent aussi.

Les obligations communes à tous les fournisseurs de services et aux seuls hébergeurs se voient renforcées **d'obligations complémentaires pour les seules plateformes en ligne**. Parmi ces dernières, des obligations renforcées sont prévues pour **les très grandes plateformes**, « *qui ont un nombre mensuel moyen de destinataires actifs du service dans l'Union égal ou supérieur à 45 millions* »

(article 33 du DSA), dont il est estimé qu'elles pourraient représenter **un risque systémique**. S'agissant du **système de contrôle et de sanctions**, il se compose de deux niveaux. C'est une « *gouvernance en réseau* », pour reprendre les mots du président de l'ARCOM Martin Adjari.

Tout d'abord, au niveau national est instauré un **coordinateur pour les services numériques (CSN)** chargé de la coordination de l'application et du contrôle du règlement, et de la coopération avec la Commission européenne avec ses homologues au sein d'un comité européen des services numériques (arts 38 et 39).

Le CSN dispose de **pouvoirs d'enquête pour infractions supposées** au règlement, notamment des pouvoirs d'interrogatoires et d'inspection, d'accès aux données nécessaires ainsi que **des pouvoirs d'exécution** permettant la prise de mesures provisoires en cas de risques de préjudice grave.

Il peut également **prendre des mesures correctives** pour faire cesser une infraction et d'imposer des amendes et des astreintes. Le montant de celles-ci est déterminé par chaque État membre à hauteur de **6 % du chiffre d'affaires mondial annuel réalisé au cours de l'exercice précédent et 5 % du chiffre d'affaires quotidien** (art. 42).

En cas d'infraction pénale grave impliquant une menace pour la sécurité des personnes, **le CSN est habilité à saisir l'autorité judiciaire pour limiter temporairement l'accès des utilisateurs** concernés par l'infraction ou limiter l'accès aux services concernés par l'infraction.

En France, **l'ARCOM s'est vu confier le rôle de CSN par la loi visant à sécuriser et réguler l'espace numérique** (loi SREN). L'ARCOM est en lien avec la Commission nationale de l'informatique et des libertés (CNIL) et la Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF) participant également de la **supervision des acteurs** régulés par la Commission européenne.

Le pouvoir dont dispose l'ARCOM est conséquent puisqu'elle peut mettre en place une **politique active de lutte contre les contenus illicites**, en vertu des pouvoirs que lui confère l'article 9 du DSA. Cela lui permettrait ainsi de saisir les autorités administratives et judiciaires et d'adresser des injonctions à toutes les plateformes.

Le mécanisme étant relativement neuf, il doit être approprié pour reprendre les mots du Représentant permanent adjoint Cyril Piquemal. Déjà, **l'ARCOM a signé le 4 juillet 2024 une convention avec le service de lutte contre les ingérences numériques étrangères** – ou Viginum – afin d'analyser la mise en œuvre du DSA et disposer de données pour alimenter les enquêtes.

Au niveau européen, le système de contrôle et de sanctions est exercé par la Commission européenne. Elle joue un rôle essentiel dans le contrôle des

très grandes plateformes qui obéissent à des dispositions spécifiques en raison des risques systémiques qu'elles peuvent poser.

Un système de surveillance renforcée peut être mis en œuvre par le CSN compétent s'il juge qu'une très grande plateforme a enfreint une ou plusieurs des obligations spécifiques qu'elle est tenue de respecter. Si l'infraction perdure, la Commission peut prendre le relais du CSN.

La Commission peut également agir de son propre chef, sur recommandation du comité ou à la demande du CSN du pays d'établissement de la très grande plateforme.

La Commission se voit ainsi dotée de larges prérogatives concernant les pouvoirs d'enquête visant les très grandes plateformes. Plus spécifiquement, la Commission dispose de **pouvoirs d'accès aux données, aux algorithmes et systèmes informatiques** et aux explications de ces dernières.

Tout comme le CSN au niveau national, la Commission est compétente pour **prendre des mesures provisoires en cas de préjudice grave** et pour assurer la bonne application du règlement par les très grandes plateformes. Elle peut également infliger des amendes dont le calcul est identique à celui prévu pour les CSN nationaux.

Par ailleurs, le règlement relatif aux marchés uniques (*Digital Markets Act*, DMA) doit être examiné car la question des contenus illicites n'est pas détachée des questions de concurrence que vise le DMA.

L'objectif du DMA est de lutter contre les pratiques anti-concurrentielles des géants d'Internet et de **corriger les déséquilibres de leur domination** sur le marché numérique européen. Le DMA vise dix services de plateforme essentiels (moteurs de recherche, navigateurs web, services en nuage notamment).

La spécificité du DMA est de **cibler les entreprises considérées comme des contrôleurs d'accès (*gatekeepers*)**. Ces acteurs ont une incidence forte sur le marché intérieur et sont un point d'accès important pour les entreprises utilisatrices. Leur lieu d'établissement n'a pas d'importance.

Sont présumées contrôleurs d'accès les entreprises qui :

- fournissent un ou plusieurs services de plateforme essentiels dans au moins trois pays européens ;
- ont un chiffre d'affaires ou une valorisation boursière élevée (7.5 milliards d'euros de chiffre d'affaires annuel en Europe dans les trois dernières années ou une capitalisation boursière importante 75 milliards d'euros pour la dernière année) ;

- enregistrent un nombre d'utilisateurs dans l'Union de plus de 45 millions d'Européens par mois et 10.000 professionnels par an sur les trois dernières années.

Les entreprises atteignant ces chiffres devaient s'identifier auprès de la Commission européenne qui a publié une première liste de contrôleurs d'accès le 6 septembre 2023. Cette liste est révisable tous les trois ans.

En cas d'infraction, l'amende peut aller jusqu'à 10 % du chiffre d'affaires mondial total de l'entreprise contrevenante, et en cas de récidive jusqu'à 20 % du chiffre d'affaires. **Si trois violations interviennent en huit ans, la Commission peut ouvrir une enquête de marché et imposer des mesures correctives comportementales ou structurelles.** Parmi ces dernières figurent la cession d'activités ou l'interdiction d'acquisition d'entreprises de services dans le numérique.

3. Un équilibre à trouver entre la liberté d'expression et le modèle économique des plateformes

DSA et DMA constituent des textes structurants aux impacts conséquents notamment en ce qui concerne la mise en conformité des plateformes des conditions de la liberté d'expression et le fonctionnement respectueux des droits des utilisateurs.

S'agissant du DSA, **le mécanisme de notification et d'action par voie électronique permettant l'identification du contenu** et l'appréciation de son caractère illicite constitue un élément clé. **Il permet d'engager plus facilement la responsabilité de l'hébergeur** en cas de notification d'un contenu illicite qui ne serait pas traité avec diligence.

Par ailleurs, les utilisateurs disposent d'une meilleure information sur les services utilisés puisqu'ils se voient informer par les hébergeurs des motifs et circonstances du retrait de contenus et des voies de recours disponibles.

Les plateformes en ligne doivent mettre en place un système de traitement des réclamations et les utilisateurs, en cas de litige, pourront saisir des organes de règlement extrajudiciaire des litiges impartiaux et indépendants.

Un statut de « signaleurs de confiance » (*trusted flaggers*) est institué dont les plateformes devront **traiter les notifications prioritairement**. Ce statut sera accordé par les autorités du pays d'établissement de l'entité qui en fera la demande, sous conditions de critères d'expertise dans la détection, l'identification et la notification des contenus illicites, d'indépendance, et de représentation des intérêts collectifs.

Les plateformes sont autorisées à suspendre les comptes fournissant fréquemment des contenus manifestement illicites.

En matière de transparence, des obligations sont instaurées en fonction de la taille des opérateurs. La base commune consiste en des conditions générales d'utilisation (CGU), des politiques et outils de modération (art. 12) – en indiquant les modalités de celle-ci – ainsi qu'en la publication annuelle d'un rapport sur les modalités et les résultats de leurs activités de modération (art. 13).

Des exigences sont mises en place en matière d'information du caractère publicitaire des annonces diffusées avec une explication sur les paramètres de ciblage.

Eu égard aux risques systémiques qu'elles font peser, les très grandes plateformes sont soumises à des obligations rendues publiques évaluées annuellement, quant à la diffusion de contenus illicites, aux atteintes aux droits fondamentaux et à la manipulation intentionnelle de leurs services susceptibles d'impacter des domaines cruciaux ou des publics réputés vulnérables. Des mesures d'atténuation de ces risques doivent être mises en place (article. 27).

Les très grandes plateformes doivent **nommer un responsable de la conformité** et procéder à un **audit indépendant** pour s'assurer du respect des obligations prévues par le règlement mais aussi de leurs engagements dans le cadre de codes de conduite volontaires (art. 28).

Enfin, les très grandes plateformes doivent **indiquer à leurs utilisateurs les principaux paramètres de leurs systèmes algorithmiques de recommandation et permettre leur modification (art. 29)**. Elles sont également tenues de **rendre leurs données accessibles** aux autorités de régulation et de contrôle nationales et européennes compétentes, ainsi qu'aux chercheurs travaillant sur l'identification et la compréhension des risques systémiques posées par les très grandes plateformes.

Dans le cadre du DMA, les contrôleurs d'accès doivent permettre facilement le désabonnement ou l'abonnement, rendre interopérables les fonctionnalités de base de leurs services de messagerie instantanée et donner accès aux vendeurs à leurs données de performance *marketing* ou publicitaire sur leur plateforme.

Les contrôleurs d'accès ne peuvent plus imposer les logiciels les plus importants (navigateurs web, moteurs de recherche), favoriser leurs produits et services au détriment des vendeurs utilisant leur plateforme et réutiliser les données d'un utilisateur à des fins de publicité ciblée sans son consentement explicite.

Ainsi, les deux règlements de législation numérique viennent **poser un cadre exigeant et transparent** permettant aux utilisateurs d'en connaître l'architecture et les risques potentiels. Ils s'attaquent à **l'opacité du modèle économique de plateformes** (données personnelles utilisées, paramétrages des algorithmes). Enfin, plus spécifiquement dans le cadre du DSA, les modalités de la liberté d'expression sont précisées à travers les règles des plateformes (CGU) et tiennent compte des législations nationales et des codes de conduite volontaires.

B. LE RÈGLEMENT SUR LES SERVICES NUMÉRIQUES EST CONFRONTÉ A DIFFÉRENTES DIFFICULTÉS DANS SA MISE EN ŒUVRE

1. Des enquêtes européennes à la peine

Si la situation internationale couplée à la situation monopolistique des réseaux sociaux fait planer des menaces évidentes l'intégrité de nos démocraties, il convient de constater que **les pouvoirs d'enquête et de contrôle dont disposent la Commission européenne semblent insuffisamment utilisés.**

Interrogé sur ce point, le Représentant permanent adjoint (RPA) de la France auprès de l'Union européenne **Cyril Piquemal**, souligne la « *collision entre le temps d'application du DSA et le temps politique des États membres.* » La phase opérationnelle de mise en œuvre a été importante, indiquait-il et « *la mise sur rails* » par la Commission a fait l'objet d'un « *travail très intense* ».

Le président de l'ARCOM **Martin Adjari** a reconnu que le temps de mise en œuvre constitue un « *élément de frustration* ». C'est le « *temps de la sécurité juridique* » assure-t-il néanmoins. Il indique aux co-rapporteurs que le DSA est un outil de mise en conformité des plateformes, mais pas un outil de gestion de crise.

Questionné lui aussi sur l'outil que constitue le DSA, **David Chavalarias** a reconnu qu'il apporte de la régulation et qu'il peut être perçu comme une « *volonté de transparence* » et le signe d'une prise de conscience européenne de certains enjeux du numérique. Cependant, il souligne que « *la mise en œuvre est beaucoup plus longue que le temps de destruction de la démocratie* » du fait du comportement de certaines plateformes et leurs propriétaires.

Le chercheur a rappelé que les États-Unis avaient été confrontés à une tentative de coup d'État le 6 janvier 2021 au Capitole au cours de laquelle les partisans de Donald Trump – soutenus par ce dernier – ont failli renverser la démocratie. Quatre années après, les Démocrates au pouvoir n'ont pas réussi à mettre en place un outil à même de réguler les plateformes et à empêcher la dérive du débat politique qui s'y observe.

S'agissant de **la procédure d'enquête de la Commission, elle répond à plusieurs étapes.** Une enquête est ouverte **sur la base de l'évaluation des informations** obtenues au cours de la surveillance. Si la Commission continue de soupçonner une infraction à la législation sur les services numériques suite aux mesures d'enquête, elle peut ouvrir une procédure. Durant cette dernière, elle entend les grandes plateformes en ligne de façon contradictoire.

Si la Commission considère qu'il y a non-conformité, elle peut adopter une décision infligeant une amende et ordonner à la plateforme en ligne visée par la mesure de **prendre des mesures correctrices, le cas échéant sous peine d'astreintes.** Alternativement, la Commission peut aussi décider de **déclencher une période surveillance prolongée** afin de garantir le respect des mesures que le fournisseur a l'intention de prendre pour remédier à la violation.

Dans le cas où la Commission estime qu'il y a une urgence en raison du risque de préjudice grave pour les utilisateurs du service – et avant toute décision finale –, elle peut décider de l'adoption de mesures provisoires proportionnées et temporaires pour atténuer ce risque.

Cette procédure est donc un long cheminement avant que toute non-conformité soit prononcée. Cela questionne nécessairement sur l'efficacité du dispositif.

Il existe bien **la possibilité de suspension des activités du service** mais la plupart des personnes auditionnées ont, sur ce point, indiqué qu'il s'agissait d'une « arme » de dernier recours et que **la Commission européenne n'avait pas véritablement l'intention d'en faire usage.**

Le représentant permanent adjoint est conscient de l'aspect « *frustrant pour le citoyen* » d'une procédure aussi longue car « **plaider la confiance ne suffit pas** ». Il souligne, toutefois, que **la Commission** est « *très fermement engagée dans la mise en œuvre renforcée des capacités d'enquête et qu'elle fait face à une armée d'avocats envoyés par les plateformes issues des cabinets les plus prestigieux* ». L'enquête se doit d'être extrêmement « *minutieuse* » et robuste afin de pouvoir prouver les éventuelles infractions.

Les pouvoirs d'enquête de la Commission lui permettent d'envoyer une demande d'informations, d'ordonner l'accès aux données et aux algorithmes pour permettre d'évaluer son fonctionnement et sa gestion des contenus illicites, de mener des entrevues avec toute personne disposant d'informations utiles à l'enquête et de procéder à des inspections dans les locaux de la plateforme visée par l'enquête.

Plusieurs enquêtes ont été ouvertes par la Commission européenne et, plus spécifiquement, **une enquête est en cours contre X depuis le 19 décembre 2023.** Il lui est reproché de **manquer aux obligations du DSA en matière de modération des contenus**, facilitant ainsi la prolifération des fausses informations et de contenus illicites, ainsi qu'en matière de **gestion des risques, d'interfaces trompeuses** (article 24 du DSA), de **transparence de la publicité** et de **accès des chercheurs aux données.**

En mai 2024, une demande d'informations a été envoyée en vertu du DSA afin d'avoir **des détails sur les activités et les ressources de X en matière de modération de contenu**, sur l'évaluation des risques réalisée par X en ce qui concerne la **mise en œuvre d'outils d'intelligence artificielle générative** dans l'Union européenne, ainsi que sur d'autres domaines couverts par la procédure formelle ouverte en décembre 2023.

L'enquête a connu de nouveaux développements, le 17 janvier 2025, avec trois nouvelles demandes concernant son système de recommandation, notamment en **raison des élections générales allemandes** de février 2025 et de la diffusion de l'interview d'Alice Weidel.

Il lui a été demandé de **fournir des documents internes sur les changements apportés au système de recommandation**. De plus, une **injonction de conservation** a été imposée l'obligeant à conserver les documents relatifs à toute modification future de ses algorithmes de recommandation.

En considérant que l'enquête contre X est ouverte depuis plus de quatorze mois, ce délai apparaît comme excessivement long. La Commission n'a pu que **constater les interventions parasitaires d'Elon Musk** dans la vie politique allemande sans pour autant agir. M. Chavalarias abonde dans ce sens en précisant qu'il « *existe des armées de robots numériques chargés d'amplifier les messages d'Elon Musk et de l'AFD pendant l'élection législative allemande* ». **Votre rapporteur Jérémie Iordanoff a rappelé au RPA Piquemal que la contrainte du temps de l'élection devait être prise en compte pour éviter toute manipulation**. M. Piquemal en a la perception aiguë mais souligne que la procédure d'enquête nécessite une confidentialité – « *pour ne pas abattre ses cartes* » - face à des acteurs de la taille d'un État. C'est aussi, selon lui, l'intérêt de disposer d'une « *procédure centralisée et unifiée* ».

Votre rapporteur Thierry Sother considère néanmoins qu'il n'est pas envisageable que la procédure ne comporte aucune étape d'évaluation afin de disposer d'une publicité des débats et des motifs précis de l'enquête.

Une telle incapacité à prendre des mesures contre X questionne sur la volonté politique de la Commission d'agir. Le départ du commissaire Breton, défenseur constant du DSA, interroge sur la capacité à faire vivre le DSA. Si les pouvoirs d'enquête existent, il est nécessaire qu'une volonté politique soit affirmée pour leur donner du sens. La présidente actuelle de la Commission Ursula Von der Leyen n'a pas donné de signe laissant penser qu'il s'agissait d'une priorité.

Il est vrai, comme l'a indiqué votre rapporteur Thierry Sother au cours d'une audition, « *qu'il est difficile de négocier des questions économiques le mercredi et de sanctionner le jeudi*. »

Sur ce sentiment de lenteur, **le RPA a rappelé qu'il convient de s'interroger sur les finalités de la procédure**. S'agit-il de « *domestiquer les pratiques ou de faire payer* » ? Cette question se retrouve au cœur de l'article 74 du DSA dans la graduation des peines prévues en cas de manquement. Pour pouvoir tenir, la procédure doit être « *solide* » et « *étayée* ». **Si jamais elle devait être « bâclée », il y aurait alors des répercussions évidentes et une exploitation politique au détriment de la Commission**. Un risque qu'elle ne peut se permettre.

Les gouvernements des États membres n'ont d'ailleurs pas manqué de tirer la sonnette d'alarme à ce sujet, comme l'illustre le courrier envoyé aux commissaires européens Henna Virkkunen (souveraineté technologique) et Michaël McGrath (démocratie) par **douze États membres** dont l'Allemagne et la France.

Dans ce courrier signé des ministres chargés des affaires européennes, les signataires appellent la Commission européenne à utiliser d'urgence le DSA : « **Les**

menaces croissantes d'interférence étrangère et les interventions disruptives dans les débats publics à l'occasion d'évènements électoraux cruciaux constituent une menace directe à notre stabilité et notre souveraineté. »

Questionné sur le comportement du propriétaire de X, presque un « influenceur » selon votre rapporteur Thierry Sother, le RPA Piquemal a rappelé que les États membres avaient demandé « *d'aller aussi vite que possible* » et donné **l'exemple de l'initiative TikTok light** pour illustrer le caractère dissuasif des sanctions.

Cette initiative, qui consistait à rémunérer les utilisateurs, a suscité de multiples inquiétudes pour la santé de ces derniers avec des risques de comportements addictifs. Face à la possibilité de poursuites, TikTok y a renoncé en avril 2024.

2. Un cas d'école de détournement de la législation sur le numérique : le premier tour de l'élection présidentielle roumaine en novembre 2024

Outre les dérives constatées sur X depuis le rachat de la plateforme par Elon Musk, c'est **le stupéfiant premier tour de l'élection présidentielle en Roumanie en novembre 2024** qui a motivé la démarche de vos rapporteurs.

Ce n'est certes pas la première fois que les réseaux sociaux deviennent un moyen d'ingérence étrangère. **La Roumanie constitue après la Géorgie et la Moldavie « le troisième pays touché par des manipulations d'ampleur en contexte électoral.** » comme le souligne **Viginum** (Service de vigilance et de protection contre les ingérences numériques étrangères).

Ce service a été **créé en 2021** pour **détecter et caractériser les opérations d'ingérences numériques étrangères** en analysant les contenus publiquement accessibles sur les plateformes et les médias en ligne.

Il ne s'agit pas pour ce service, auditionné par vos rapporteurs, d'exercer une surveillance généralisée en exploitant des données personnelles, ni même de faire office de police judiciaire. Le travail se base sur des données publiques accessibles et ne cherche en aucune façon à **devenir une sorte de « ministère de la vérité » orwellien.**

Viginum a produit un **rapport au début du mois de février 2025** analysant de manière détaillée et argumentée le déroulement de ce qui constitue **une manipulation d'algorithmes et une instrumentalisation d'influenceurs.**

Les éléments d'analyse produits par Viginum reposent sur des notes déclassifiées de l'administration roumaine, des rapports d'observateurs, des enquêtes de médias et des éléments apportés par la plateforme TikTok mise en cause.

Le contexte de l'ingérence étrangère numérique est celui du premier tour de l'élection présidentielle roumaine qui se tenait le 24 novembre 2024 pour donner un successeur au président sortant Iohannis. **À la surprise générale, un candidat crédité entre 1 % et 10 % des voix** (entre fin octobre et fin novembre), Calin Georgescu, **est arrivé en tête** avec près de 23 % des voix (2 millions de votes).

Représentant un parti situé à l'extrême droite, **son résultat est apparu comme totalement déconnecté de la campagne qui venait de se dérouler**. Le candidat Georgescu n'a que tardivement présenté sa candidature – au mois d'octobre, il ne disposait d'aucun budget de campagne – et a **concentré quasi exclusivement sa campagne sur internet et les réseaux sociaux**, plus spécifiquement sur la plateforme *TikTok*.

TikTok occupe une place essentielle en Roumanie puisque **c'est près de 9 millions de Roumains qui disposent d'un compte sur la plateforme** pour une population totale de 19 millions d'habitants. Elle occupe une place prééminente dans le mode d'information des Roumains.

Troublés par les résultats, **des analystes ont rapidement pointé l'existence d'ingérences étrangères numériques** et des notes déclassifiées des renseignements ont fait état de manipulations observables sur la plateforme *TikTok* sur laquelle le candidat a basé sa campagne.

Au regard des éléments ainsi produits, **la Cour constitutionnelle roumaine a décidé d'annuler l'ensemble des opérations électorales pour irrégularités** le 6 décembre 2024.

Les analyses, dont rend compte le rapport de Viginum, ont montré **la croissance spectaculaire du candidat Georgescu sur TikTok dans les deux semaines précédant la tenue de l'élection**. Les hashtags du candidat ont vu leur popularité basculer en tête des classements. Ainsi, l'hashtag au nom du candidat aurait été vu près de 7.2 millions de fois en sept jours selon l'*European Digital Media Observatory*.

La visibilité exponentielle du candidat semble avoir été le fruit d'une campagne d'astroturfing ⁽¹⁾. Ce terme désigne une manipulation coordonnée de l'algorithme de recommandation via la publication massive de vidéos et commentaires comportant certains mots-clés. **Utiliser des méthodes d'astroturfing révèle une connaissance fine des dynamiques de la plateforme et plus encore une maîtrise des procédés de contournement des politiques de modération.**

(1) *Mode opératoire consistant à conférer de la visibilité à un sujet en faisant croire qu'il est un phénomène de masse alors qu'il provient uniquement de la coordination de quelques comptes produisant un volume important de publications sur un seul sujet.*

Les services de renseignements roumains ont pu prouver **l'usage d'adresses IP uniques pour la connexion** à la plateforme ne permettant ainsi pas de les rattacher à un seul réseau, et ainsi démasquer le caractère artificiel.

Le procédé a permis de tromper l'algorithme de recommandations et de le pousser à mettre en avant des contenus liés au candidat Georgescu générant une surreprésentation.

En outre, **des influenceurs ont également été utilisés**. Recrutés par des entreprises de marketing, **ces derniers ont été rémunérés** pour publier des contenus obéissant à un certain format. Les influenceurs diffusaient des vidéos avec certains hashtags, en apparence neutres, qui étaient ensuite repris par des comptes pro-Georgescu générant une viralité.

Il convient de souligner que **ces messages d'influenceurs ne répondent pas aux règles européennes relatives à la responsabilité des créateurs de contenus** sur la base de partenariats rémunérés, ni même à la réglementation roumaine relative à la publicité électorale.

Des enquêtes menées par différents médias, dont le journal *Le Monde*, ont démontré **qu'une entreprise étrangère serait à l'origine du recrutement de ces influenceurs**, entreprise qui serait une société écran gérée par une branche d'un groupe spécialisé dans le casino en ligne.

L'implication manifeste de puissances étrangères, étatiques ou tiers, n'a pas pu être prouvé à ce jour. Cependant, **les prises de position de Georgescu se distinguent par un tropisme pro-russe très marqué qui donne à voir quelle serait la puissance bénéficiaire de la campagne de manipulation réalisée sur TikTok**.

La Cour constitutionnelle roumaine constatant l'ensemble de ces éléments a annulé les opérations électorales mettant en avant des irrégularités et violations de la législation électorale faussant « *le caractère libre et équitable du vote* ». Par ailleurs, **la Commission européenne a ouvert une procédure formelle à l'encontre de TikTok dans le cadre des dispositions du DSA**.

Il est notamment reproché à la plateforme de **n'avoir pas identifié le caractère électoral de la manœuvre**. Celle-ci s'est déchargée de toute responsabilité soulignant que l'obligation de labellisation de contenus politiques ne relevait pas d'elle mais de l'auteur des contenus diffusés.

Il est néanmoins **très contestable de la part de TikTok de se désresponsabiliser** de cette situation puisque, comme l'étude de Viginum le souligne, un faisceau d'indices d'altération de la plateforme et de perturbation des algorithmes était à l'œuvre et perceptible dans les contenus que la plateforme affichait. **Elle était donc en mesure de lancer l'alerte** et d'enquêter sur le phénomène.

L'ensemble de cette séquence électorale a mis en exergue **la facilité avec laquelle les politiques de modération pouvaient être détournées** – de même que les algorithmes – ainsi que l'exemption de responsabilité dont un réseau social usait pour se décharger. Cette opération illustre donc puissamment les faiblesses du DSA.

L'opération de manipulation d'ampleur en Roumanie comporte des leçons pour d'autres démocraties alors même qu'en 2025 des élections doivent avoir lieu au Danemark (mars) et en Pologne (mai).

Elle a d'ailleurs été **l'occasion d'une propagation de fausses nouvelles**. Elon Musk, J. D. Vance – dans son discours de Munich – et **plusieurs autres figures versant dans le complotisme ont cru bon de répéter que la Commission européenne avait annulé les élections roumaines**. Outre **qu'elle ne dispose en aucun cas de ce pouvoir, il s'agit d'une décision d'une Cour constitutionnelle nationale**. Pourtant, le mensonge s'est répété et diffusé en dépit de son absence de fondement.

Il est permis de penser que ce type de manipulations reposant sur des techniques similaires pourrait avoir lieu en France, sachant que la plateforme *TikTok* compte dans notre pays 21 millions d'utilisateurs mensuels (1 français sur 3) et qu'en moyenne les utilisateurs de *TikTok* y passent 38 heures par mois (chiffre le plus important toutes plateformes de réseau social confondues).

Au regard des opérations de désinformation constatées sur des plateformes francophones (*Macron Leaks*, opérations *Doppelganger* et *Matriochka*), les événements survenus en Roumanie inquiètent légitimement sur la capacité française à se protéger contre ce qui constitue des assauts contre la démocratie. Et **le risque est grand pour « l'intégrité de l'espace informationnel et l'espace public »** reconnaît Martin Adjari au cours de son audition.

À l'évidence, le rempart que devait constituer le DSA est plutôt une digue fragilisée qui pourrait très facilement céder.

C. LES PRÉCONISATIONS PORTÉES PAR VOS RAPPORTEURS SONT DE DIFFÉRENTS NIVEAUX

1. La Commission européenne et les acteurs nationaux doivent assumer les pouvoirs que le règlement sur les services numériques leur confère

Vos rapporteurs ont pu constater dans leur travail de rédaction de la proposition de résolution, ainsi que dans les auditions menées dans le cadre du rapport l'accompagnant, les insuffisances dans la mise en œuvre du règlement sur les services numériques.

Il ne s'agit aucunement de décréter son inutilité : il constitue **un pas important en faveur de la régulation** et fixe des normes fortes pour l'Europe et

pour toutes les plateformes qui prétendent opérer sur un continent de plus de 500 millions.

Par ailleurs, il n'est pas anodin que le DSA fasse l'objet de tant d'attaques venant d'un même camp politique. Et il est assez ironique de constater que certains de ceux qui le critiquent en Europe, dans notre pays même, ont fait partie ceux qui l'ont voté au Parlement européen. **Plus de 90 % des députés européens l'ont approuvé.**

Ceci étant dit, vos rapporteurs ne peuvent donner un satisfecit à la Commission européenne dans la mise en œuvre du règlement.

Alors même que le texte du DSA lui donne de larges pouvoirs d'enquête et d'exécution, la Commission a engagé seize enquêtes formelles contre des plateformes et réseaux sociaux soupçonnés de ne pas conformer au DSA. Qu'en est-il de ces enquêtes ? **L'exemple de celles contre X, exposées précédemment, indiquent une lenteur très préjudiciable à l'efficacité du DSA.**

Au regard de la multiplicité d'analyses et de preuves manifestes tendant à montrer un usage détourné de la plateforme par son propriétaire, il est pertinent de se demander si l'article 16 a bien été analysé. Des interfaces qui trompent leurs utilisateurs, n'est-ce pas ce qu'Elon Musk a fait durant la campagne électorale américaine ?

Qu'en est-il de l'évaluation des risques systémiques pour les processus électoraux (art. 34 et 35) dont la campagne pour les élections législatives allemandes donne un piteux exemple ?

À ce titre, un **mécanisme de réponse à une crise** (art. 36) existe lorsque celle-ci entraîne une « *menace grave pour la sécurité publique ou la santé publique dans l'Union ou dans des parties importantes de celle-ci* ». Ce mécanisme est confirmé, dans une acceptation très restreinte à l'article 48 : « *Ces situations sont strictement limitées aux circonstances extraordinaires affectant la sécurité publique ou la santé publique.* »

Ce mécanisme n'est pas susceptible de permettre une censure des réseaux sociaux – contrairement à ce qu'une certaine désinformation pourrait le laisser penser – mais doit **permettre une analyse des risques liés à leurs services** et la mise en place de mesures temporaires pour les atténuer, accompagnées de garantie pour les droits fondamentaux.

Cet outil permet, en revanche, de **renforcer la modération et l'algorithme de recommandation** ainsi que le système de publicité. Il est hautement regrettable que la Commission ne s'en soit pas saisie considérant la réitération de situations dommageables intervenues sur le réseau X.

Vos rapporteurs rappellent que l'article 40 du DSA prévoit que les chercheurs peuvent avoir accès aux données de l'algorithme. Force est de

constater que **X ne respecte pas ces dispositions** en empêchant les chercheurs d’y accéder de façon large. X discrimine les centres d’expertise ayant accès à ces données alors que la lourdeur de la procédure d’un audit nécessite que cet accès soit aussi large que possible.

Le chercheur David Chavalarias a souligné lors de son audition qu’il lui avait été indiqué qu’il n’était pas « *légitime* » dans sa demande d’accès aux données et qu’à sa connaissance, aucun chercheur n’a reçu d’approbation. En aucune façon, il ne peut être attribué un pouvoir discrétionnaire aux plateformes leur permettant de décider qui est en droit d’obtenir les données ou quels sont les risques systémiques.

Vos rapporteurs s’interrogent également sur **l’efficacité des multiples rapports demandés aux plateformes en ligne** (transparence, audit) et les données qui en ressortent. À l’heure actuelle, a souligné le sociologue Romain Badouard, c’est près de **neuf milliards de données dont l’Union européenne dispose sur la base de ses obligations de transparence. L’exploitation d’une telle masse d’informations est évidemment complexe et nécessite des effectifs à la mesure.** Si l’Union européenne crée des mécanismes trop complexes, elle se trouvera elle-même dans l’impossibilité de les exploiter. La durée de l’enquête sur X en donne un aperçu.

La proposition de résolution transpartisane portée par vos deux rapporteurs ne peut que constater la place dominante des plateformes numériques devenus des mastodontes.

Elle constate que ces plateformes se nourrissent des aspects les plus néfastes des réseaux sociaux (fausses nouvelles monétisées) alors même que des politiques de modération sont censées prévenir de telles dérives.

Vos rapporteurs incitent donc la Commission européenne à muscler son dispositif en revenant à l’esprit du DSA et à sa recherche de normes effectives, en utilisant les larges pouvoirs de l’article 67 – quitte à **prendre des décisions radicales mais fondées en droit, à avancer dans l’exploitation des données et algorithmes et à faire preuve de transparence vis – à-vis des enquêtes menées.**

Comme la lettre des douze États membres envoyée à la Commission européenne le laissait deviner, comme le ministre français des affaires étrangères l’a indiqué à plusieurs reprises, **si la Commission n’est pas prête à mettre en œuvre les dispositions du DSA, elle doit alors laisser les États membres agir et obtenir des plateformes le respect strict de la loi votée.**

Vos rapporteurs souhaitent souligner l’exemple brésilien de l’été 2024. Au nom de la lutte contre la désinformation, un juge fédéral avait suspendu X dont il estimait qu’il ne respectait pas les lois brésiliennes en permettant à certains comptes de propager des fausses informations.

La reprise des activités de X n’a été possible que par la suspension des comptes litigieux, le paiement d’amendes et la désignation d’un nouveau

représentant légal au Brésil. La décision du juge se fondait sur l'estimation que les actions de X s'assimilaient à une entrave de la justice.

Suspendu un temps, X n'a pu être réactivé qu'en respectant la décision rendue par le collège des cinq juges le 5 octobre 2024 et cet après que Elon Musk ait diffamé l'auteur du jugement initial à travers un compte publiant de la désinformation.

La décision de se conformer à la justice brésilienne prouve bien qu'il est possible, pour les États, de s'opposer aux comportements délictueux et dangereux des plateformes et de les contraindre à rendre des comptes devant la justice.

Si le Brésil, qui ne dispose d'un dispositif similaire au DSA, a pu obtenir gain de cause, l'Union doit être en capacité de voir ses exigences respectées, ses réglementations appliquées et la lutte contre la désinformation et l'ingérence assumée.

Il est notable de constater que **le marché européen de 500 millions d'habitants représente un débouché majeur pour les plateformes en ligne**, et notamment X. Une absence de diligence donnant lieu à une suspension des activités pourrait être de nature à modifier les pratiques délictueuses.

D'ailleurs, **le RPA Piquemal a indiqué que « l'immense force du DSA est sa plasticité » et « qu'il sera ce que l'on en fait » tout en rappelant que le règlement ne constitue pas « la fin de l'histoire ».**

Derrière cette dernière expression, il convient de **comprendre que le régime de responsabilité limitée des hébergeurs de contenus n'est pas immuable** et qu'il est envisageable, un jour, de mettre en place un régime a priori plutôt que le régime actuel de réaction. C'est déjà ce qui est pratiqué pour les plateformes de ventes (*marketplaces*).

Sur ce point, le sociologue **Dominique Boullier** a émis dernièrement **l'hypothèse de faire évoluer le statut juridique des plateformes en ligne**, aujourd'hui simples hébergeurs. Un statut de médias pourrait leur être appliqué afin de reconnaître leurs lignes éditoriales et de responsabiliser leurs pratiques

Vos rapporteurs formulent, par ailleurs, **le souhait que les acteurs nationaux concernés par la mise en œuvre du DSA se saisissent pleinement des pouvoirs qui leur ont été attribués.** Il s'agit spécifiquement ici de l'ARCOM.

David Chavalarias, chercheur au CNRS auditionné par vos rapporteurs, fait observer que le DSA doit pouvoir être utilisé dans toutes ses dispositions et que **l'ARCOM devrait user du principe de subsidiarité** en se saisissant des nouveaux pouvoirs qui lui ont été octroyés.

Comme a pu le confirmer la DG Connect lors de son audition, « *La Commission européenne n'intervient pas au niveau des contenus individuels, c'est la mission des régulateurs nationaux et cadrés par les droits nationaux. Un magistrat national peut ordonner le retrait précis des contenus* ». Ainsi, face à la menace d'ingérence qui pèse sur nos démocraties, il semble nécessaire de renforcer les effectifs et capacités de l'ARCOM afin de lui conférer une capacité à analyser et agir en justice pour supprimer immédiatement tout contenu contraire au droit français et sanctionner les auteurs.

Au-delà de ces constats et demandes, vos rapporteurs souhaitent engager une réflexion – et par la suite une action – sur les modèles des plateformes en ligne.

2. Repenser le modèle des plateformes : la rentabilité du modèle économique doit aller de pair avec des architectures numériques éthiques

Il ressort du travail de vos rapporteurs que **la question de la lutte contre la désinformation et les ingérences doit tenir compte des lois du marché. Le modèle économique des plateformes, basé sur la publicité et la mise en avant de contenus viraux, est un impensé des tentatives de régulation.**

Le sociologue Dominique Boullier a souligné à plusieurs reprises que le danger provient surtout de **la viralité qui règne sur les réseaux sociaux** qui active un phénomène de propagation des contenus.

La théorie de la propagation d'Adam Kucharski ⁽¹⁾ (durée, opportunités, transmissibilité, susceptibilité) s'applique ici pour partie. Un élément perturbateur surgit grâce à une opportunité et crée une épidémie. Celle-ci perdure en fonction de la durée de vie de l'élément perturbateur et de sa capacité à être transmissible au sein d'une population.

La monétisation des réseaux sociaux, à partir de 2008-2009, leur a permis de **générer des revenus colossaux tout en pratiquant l'opacité** dans la construction de l'algorithme et en créant des mécanismes de captation de l'attention largement prédateurs.

Un exemple parlant de **l'impact du marché publicitaire sur internet** est celui du moteur de recherche Google et de son classement des sites en fonction de leur notoriété sur internet. Cette classification a donné lieu au dépôt du brevet de la formule de l'algorithme appelé PageRank en 1998.

Un système proche a été créé quelques années après visant cette fois-ci les créateurs de site et les vidéastes de la plateforme YouTube pour leur permettre de monétiser leurs contenus.

(1) *Épidémiologiste spécialisé dans les modèles mathématiques et statistiques.*
« *Les lois de la contagion, fake news, virus, tendances* ». 2021.

À titre d'illustration, **Facebook générerait 70 milliards d'euros de revenus pour l'année 2019 dont 98 % provenaient de la seule publicité.**

À l'ère des *big data* (mégadonnées), **les plateformes en sont venues à utiliser les données des utilisateurs en les revendant au plus offrant.** Au-delà de l'absence de respect des données personnelles, la concrétisation politique du phénomène a été rapide avec le scandale *Cambridge Analytica*.

Le législateur est là pour impulser des dynamiques et poser des règles mais la rapidité des évolutions technologiques le contraint à une agilité permanente. Désormais, des règles ont été posées s'agissant de la publicité politique ou de l'usage des données personnelles (règlement général sur la protection des données personnelles) mais de nouvelles opportunités se dessinent.

Ainsi, **l'intelligence artificielle**, existante depuis les années 1950, a fait des progrès colossaux au point de pouvoir être utilisé par le grand public et non plus seulement les chercheurs. **Les robots conversationnels nourris d'algorithmes entraînés en permanence produisent un contenu qui nécessite une régulation.**

Le règlement sur l'intelligence artificielle (IA), adopté en 2024 par l'Union, est un premier pas indispensable en instaurant des normes éthiques et en interdisant certaines pratiques (notation sociale, identification biométrique, exploitation des vulnérabilités).

Il fait pourtant l'objet de coups de butoirs de la part d'acteurs étrangers étatiques ou tiers. **Nous croyons qu'il est indispensable de le soutenir car fixe le niveau du débat démocratique. Nous n'ignorons pas l'effet des *deepfakes* lors des processus électoraux et la désinformation qu'ils engendrent.**

Il convient également de souligner que **l'IA pourrait modifier le mode informationnel actuel**, hypothèse formulée par le sociologue Romain Badouard auditionné par vos rapporteurs. Soulignant que les réseaux sociaux étaient devenus la source principale d'information de la population, il indique **qu'une utilisation de l'IA pour s'informer via le robot conversationnel** peut modifier la pratique des réseaux sociaux pour le futur : « *Nous n'utiliserons plus les réseaux sociaux de la même façon* ».

La monétisation qui a lieu sur les plateformes passe également par l'architecture (*design*) de ces dernières. L'algorithme, en fonction des recommandations qu'il opère, est susceptible d'influer sur le comportement de l'utilisateur. Plus ce dernier est captif et plus son comportement sera dicté par les contenus qu'il voit.

Le sociologue Boullier soulignait que **le *free speech*** (la liberté d'expression) n'est pas un problème mais que **le *free reach*** (l'inondation des esprits) en est un.

Une initiative utile avait été le partenariat entre des rédactions de presse et certains réseaux sociaux en vue de contrecarrer l'effet de viralité et l'emprise

de la désinformation. Les choix idéologiques opérés par Musk et désormais par Mark Zuckerberg, le dirigeant de Facebook, ont remis en cause ce travail de conscientisation de l'information.

Les informations sont calibrées en fonction des outils qui les rendent possibles. L'exemple de X et ses 280 caractères en est une juste illustration. Il crée des réactions identiques, tout comme les *reaction buttons* sur Facebook. Il encourage des mécanismes émotionnels particulièrement nocifs contre lesquels il faut se prémunir.

Pour agir sur le modèle des plateformes et les effets insidieux qu'elles suscitent, **il convient de repenser leur fonctionnement** et de lutter contre le « *réchauffement médiatique* » (Boullier).

Les « machines à réplication » que sont devenus les réseaux sociaux (notifications incessantes, simplification du partage d'informations) accélèrent les flux créant de phénomènes en chaîne. La désinformation et les ingérences se nourrissent de ces dynamiques pour se déployer.

Remettre en cause le modèle des plateformes, c'est **agir sur leur construction en freinant les partages** pour permettre aux utilisateurs d'être conscients des informations dont ils se font les relais.

Si le modèle économique des plateformes pourrait en être altéré (baisse des recettes publicitaires), il est néanmoins possible de le faire comme l'application *Instagram* en a donné l'exemple en 2019 en supprimant, dans certains pays, le nombre de *likes* sous les publications. L'application *WhatsApp* limite le partage de messages de groupes pour lutter contre la propagation des fausses informations.

D'autres modèles d'applications sont envisageables à l'instar de l'application Mastodon, alternative libre et décentralisée de X, qui empêche la possibilité de citer un tweet dans son propre message. Cette fonctionnalité est en effet un vecteur d'humiliation publique dans le but d'obtenir une reconnaissance de ses pairs.

Mastodon et Bluesky sont deux alternatives à X tout en posant les mêmes questions de modèles économiques et de choix technologiques à long terme. Les deux applications se veulent des alternatives plus éthiques que le réseau social X dans sa forme actuelle.

La particularité de ces réseaux sociaux est de reposer sur un modèle de décentralisation où une constellation d'entités existe indépendamment l'une de l'autre, et appliquant leurs propres règles de modération. **Ce modèle permet aux personnes de choisir les informations qu'elles souhaitent voir et les données qu'elles choisissent de partager.**

La difficulté à laquelle se heurtent ces réseaux reste cependant le modèle économique. La publicité permet à Bluesky d'exister et de poursuivre sa croissance

et de rentabiliser l'investissement initial d'avoir créé son propre protocole. Mastodon a repris un protocole déjà existant limitant ainsi ses coûts mais demeure tributaire des dons pour poursuivre sa croissance.

À titre informatif, Bluesky revendique 30 millions d'utilisateurs et Mastodon plus d'un million quand X dispose de plusieurs centaines de millions d'utilisateurs.

L'exemple de Bluesky et Mastodon permet également **d'introduire le débat de l'interopérabilité** comme manière de bouleverser la nocivité de certains réseaux sociaux. *La Quadrature du Net*, auditionnée par vos, rapporteurs, a soulevé le débat au cours de son audition, de même que le sociologue Romain Badouard.

La difficulté à quitter certains réseaux sociaux se trouve dans l'effet de réseau créé : les plateformes ont atteint une taille critique et forgé des communautés dont les utilisateurs devraient se priver s'ils souhaitaient quitter les plateformes en question.

Avec un droit à l'interopérabilité, tel que promu par le canadien Cory Doctorow dans son dernier ouvrage ⁽¹⁾, **l'utilisateur est en mesure d'« exporter » ses données avec lui**. C'est d'ailleurs grâce au DSA que cette possibilité est devenue réelle.

Les utilisateurs lassés par les dérives de X ont pu migrer vers Bluesky et Mastodon grâce à la portabilité de leurs données leur permettant ainsi de ne pas perdre des années d'interactions. C'est ce qui a permis **le relatif succès de l'initiative HelloQuitteX propulsée avec l'aide des travaux de David Chavalarias**.

La portabilité est une mesure prometteuse qui est d'ailleurs défendue par le conseil national du numérique (CNNum) a indiqué Romain Badouard. Pour ce sociologue, **la difficulté** est cependant la capacité à **emmener une taille critique d'utilisateurs/consommateurs qui se sont habitués à un mode d'interaction à travers les plateformes qu'ils utilisent**. La difficulté étant alors de trouver une force de motivation suffisante sans quoi les utilisateurs migrant s'apercevraient qu'ils sont peu suivis et reviendraient sur la plateforme d'origine. Romain Badouard souligne, malgré tout, qu'il s'agit d'une option peu coûteuse économiquement puisqu'elle ne nécessite pas d'infrastructures physiques particulières. Il s'agit principalement d'une question technique et sur ce point, l'Union européenne ne fait pas face à un obstacle insurmontable.

En encourageant l'interopérabilité, l'Union européenne permettrait le développement d'initiatives indépendantes portées par une éthique, à l'image du *Front Porch Forum*, et de créer un nouvel écosystème informationnel bienveillant.

Cette initiative développée dans l'État américain du Vermont consiste en un réseau social local (240 000 utilisateurs) où les échanges sont pacifiés et, plus

(1) *Le rapt d'internet*, C&F éditions, 2025.

encore, où certains méfaits de la viralité sont contrés : pas de *like* possible des commentaires, ni de commentaires instantanés pour permettre une réflexion.

La portabilité est un moyen facile et efficace pour permettre le développement de plateformes françaises et européennes conséquentes. Tant que ce principe ne sera pas garanti et rendu opposable, les plateformes pourront continuer à jouir de leur monopole et des gains obtenus par les innovations technologiques sans être contraintes d'ouvrir la porte à de nouveaux acteurs. Cette réflexion a été soulignée par David Chavalarias au cours de son audition.

3. La création d'une véritable souveraineté numérique européenne

Être souverain, c'est disposer de la capacité à édicter des règles applicables à tous sans être contraint par des insuffisances techniques.

Cela est d'autant plus essentiel en période de crise, à l'instar d'une pandémie, où les informations qui circulent déterminent la vision du public qui utilise un réseau social.

Alors que l'administration Trump est en fonction depuis cinquante jours, **votre rapporteur Thierry Sother considère que « face aux réveils matinaux pendant quatre ans, il faut une réponse politique », pour Jérémie Iordanoff : “L'Europe doit agir fermement pour que les plateformes respectent les règles et garantissent un débat public équitable et transparent”.**

Cette réponse est d'autant plus nécessaire **qu'en comparant les attitudes des différentes plateformes en ligne**, ainsi que l'ont souligné Viginum et M. Badouard, il y a des différences de diligence importantes. **TikTok présente de véritables problématiques** de données personnelles, d'opacités et d'ingérences mais adopte, malgré tout, une approche ouverte et **tend à modifier ses pratiques** ainsi qu'à se mettre en conformité avec les demandes européennes.

X ne suit absolument pas cette direction et, pour reprendre les mots de Romain Badouard, « *on passe un cap* » en comparant les pratiques des deux plateformes avec un choix politique affirmé et **un refus de se soumettre à la législation européenne assumée par Elon Musk.**

En établissant une législation numérique ambitieuse, l'Union s'est dotée de la capacité de réguler les plateformes et de formuler un début de réponse aux excès constatés notamment en matière de désinformation et d'ingérences étrangères.

Le règlement du DSA et son pendant anti-monopolistique DMA ne pourront être efficaces que si chacune des dispositions qui les composent sont pleinement utilisées. À ce titre, vos rapporteurs estiment qu'au regard de la position X un nouvel examen pour **déterminer un possible statut de contrôleur d'accès** serait judicieux. Sa position parmi les réseaux sociaux en fait aujourd'hui un acteur incontournable.

S'agissant de la clause de revoyure, vos rapporteurs jugent également que l'architecture du DSA **pourrait être revue de manière anticipée**. Le présent rapport dresse un constat plus que nuancé de certaines des dispositions et de la manière dont la Commission européenne s'en saisit. Une modification des équilibres des pouvoirs entre États membres et Commission européenne serait envisageable.

L'hypothèse de réexamen précoce de la clause de revoyure du DSA serait aussi l'opportunité de tenir compte des dernières innovations technologiques. Le règlement sur l'IA a proscrit un ensemble de pratiques, nous l'évoquions précédemment. Il serait justifié de prendre en compte les détournements des dernières innovations pour s'assurer de la pertinence technologique de l'instrument du DSA.

Au-delà du DSA, **la question fondamentale qui se pose à l'Union en termes de souveraineté est la constitution de géants du numérique**. Trop longtemps, **la politique de la concurrence a fixé des normes drastiques empêchant l'émergence de champions européens** tout en laissant d'autres puissances occuper le terrain.

Les géants du numérique en sont l'illustration. Le règlement de 2000 était censé favoriser l'éclosion d'un écosystème d'entreprises bénéficiant des innovations technologiques et permettant l'affirmation de l'Europe dans ce domaine. L'outil n'a pas été approprié, sans doute par manque d'incitations économiques également.

L'Union pourra affirmer d'autant plus fortement son influence qu'elle disposera, outre son corpus normatif, d'entreprises favorables à ces dernières et s'inscrivant idéologiquement dans l'esprit de régulation et de modération de la liberté d'expression qui nous caractérise.

Laisser les géants du numérique, essentiellement américains et chinois, occuper l'espace européen, c'est continuer de confier les règles de la modération et de la censure à des structures privées dont les règles extra-judiciaires sont difficilement contestables, sauf en dernier ressort comme le DSA le permet.

À cet égard, **votre rapporteur Jérémie Iordanoff est partisan d'envisager le levier de la cession de capital de géants du numérique étrangers à des entreprises européennes**. Cette proposition figure parmi les dispositions du DMA en cas de comportements contrevenant au règlement. En cas de violations répétées, la Commission peut envisager des « *mesures correctives comportementales et structurelles* ».

Votre rapporteur soutient la proposition de cession de parts dans une plateforme dont le propriétaire se trouve en situation de conflit d'intérêts. En l'espèce, **le rôle de M. Musk dans l'administration Trump, sa stratégie de privatisation sauvage à travers le DOGE et ses intérêts capitalistiques en jeu**

doivent faire envisager ce levier. Il ne s'agit nullement d'exproprier mais de permettre à un acteur tiers d'agir librement sans mélanger des intérêts contraires.

Cet instrument peut être puissamment incitatif à l'égard des plateformes pratiquant des écarts répétés avec la législation nationale et européenne. À défaut, la question se posera de la pérennité de leurs activités au sein de l'espace européen. **Le droit américain pratique une extraterritorialité exorbitante : l'Union est fondée à permettre sur son sol l'application de son droit.**

Interrogé sur cette hypothèse, le président de l'ARCOM a répondu que l'état du droit national et européen ne semble pas permettre sa concrétisation. **Votre rapporteur considère que le cadre juridique peut être amené à évoluer et n'est pas figé.** Sur une question différente mais actuelle, celle de la confiscation des avoirs russes gelés depuis le lancement de la guerre en Ukraine, le droit actuel ne la permet pas ce qui n'empêche pas les gouvernements des États membres de l'envisager très sérieusement. **Là où il y a une volonté, il y a un chemin.**

En outre, **considérer que l'arme de la sanction (6 % du chiffre d'affaires mondial) serait dissuasive, c'est oublier, dans le cas de X, qu'Elon Musk a pu acheter une plateforme en ligne - ne faisant aucun bénéfice – pour 44 milliards de dollars !** Avec de tels moyens financiers, l'amende de la Commission européenne paraît beaucoup moins en mesure de modifier les pratiques.

Par ailleurs, **la montée en puissance de l'IA et de son usage – notamment dans l'exercice de la politique de modération – fait craindre une complexification du processus et une opacification des règles pour l'utilisateur.**

À cet égard, l'Union n'a pas investi collectivement sur l'IA pour rivaliser avec l'américain *ChatGPT* ou le chinois *DeepSeek*. La France a bien saisi l'opportunité mais il est certain que sa puissance de frappe ne peut pas être aussi importante que celle des États-Unis ou de la Chine. Cela questionne une fois de plus la capacité de l'Union à mettre en actes ses intentions.

Si la souveraineté numérique s'exerce à travers des structures, elle se réalise également à travers des mécanismes de protection de nos démocraties et notamment par la capacité à interpréter les actes et les stratégies de nos partenaires commerciaux souvent concurrents, c'est-à-dire la Chine, la Russie – dans une moindre mesure depuis la guerre en Ukraine - et les États-Unis.

En constituant entre 2020 et 2023 une commission spéciale sur les ingérences (INGE 1 et 2), présidée par le député Raphaël Glucksmann, le Parlement européen a pris conscience de la menace que constituent l'ingérence et son exercice à travers les technologies.

La « *Commission spéciale sur l'ingérence étrangère et l'ensemble des processus démocratiques de l'Union européenne, y compris de la désinformation* » a dressé un portrait complet de la menace de l'ingérence et de ses manifestations. Si son travail a essentiellement porté sur la législation électorale et le financement

des partis politiques, **la place des réseaux sociaux dans l'ingérence a largement été débattue.**

Les modalités de l'ingérence (guerre hybride, infiltration de rédactions de presse, publicité, modalités de lutte contre la désinformation par les plateformes) rejoignent l'analyse de vos rapporteurs sur les dérives constatées sur plusieurs plateformes en ligne, et spécifiquement sur X.

Le large travail accompli a permis de **prendre conscience de l'ampleur du phénomène et de consolider la législation européenne sur ces sujets.** Il s'agit d'un chantier encore en cours.

À cet égard, le Parlement européen s'est à nouveau saisi de la question de la protection de la démocratie et des processus électoraux à travers le « **bouclier démocratique européen** », commission spéciale constituée au début du mois de février 2025 et présidée par la députée Nathalie Loiseau.

Les travaux de la commission n'ont pas encore débuté mais **il s'agit d'un projet voulu comme une riposte de l'Union aux ingérences étrangères** en luttant contre les « *potentielles attaques malveillantes* » extérieures via la modification de la réglementation européenne.

Le projet n'a pas de lien avec la législation du DSA mais il en rejoint l'objet en partie en cherchant à lutter contre les ingérences sur les plateformes en ligne et leur impact sur la démocratie, les cyberattaques ou encore les contenus générés par l'IA visant à manipuler l'information.

Enfin, il importe de **tenir compte d'une « fracture sociale » dans l'information** (Romain Badouard) avec une **capacité différentielle à être convaincu par la désinformation selon l'origine sociale et les études secondaires** effectuées. Il s'agit d'un sujet de politique publique. Une **éducation aux médias**, à leur contenu et à un esprit critique est indispensable pour créer un bouclier intellectuel. Apprendre à identifier l'information et à la décrypter permet aussi de s'armer contre la désinformation et ses manifestations.

Comme le sociologue le fait observer lors de son audition, la pandémie de Covid – avec le confinement répété qu'elle a engendré – a vu un rebond des médias traditionnels et une volonté de nombreux citoyens de disposer d'informations sûres et vérifiées dans un contexte inquiétant et incertain.

Sur ce volet-là, **l'Union européenne peut aussi agir à travers certains de ses programmes** à l'image du programme MEDIA.

CONCLUSION

Le règlement sur les services numériques était attendu par les acteurs du milieu et nécessaire pour répondre aux profondes mutations technologiques intervenues depuis le premier règlement de 2000 consacré aux services numériques.

Le DSA constitue une avancée certaine et réaffirme la vision portée par l'Union européenne en matière de liberté d'expression qui concilie liberté et respect de la dignité humaine, loin de toute vision maximaliste donnant lieu à des excès dans lesquels nous ne pouvons-nous retrouver.

Les bouleversements intervenus sur X en matière de modération, les pratiques opaques et addictives de *TikTok* ainsi que les invariants du modèle économique de X nous incitent cependant à **formuler de nouvelles propositions** en vue d'améliorer la législation en vigueur et de **s'assurer du respect des données personnelles et des droits fondamentaux**.

L'Union européenne ne doit pas seulement édicter des normes éthiques : elle doit se donner les moyens de leur donner une concrétisation réelle par des structures et surtout rester en alerte face aux menaces qui l'entourent et cherchent à perturber notre modèle démocratique.

EXAMEN EN COMMISSION

La Commission s'est réunie le mercredi 19 mars 2025, sous la présidence de M. Pieyre-Alexandre Anglade, président, pour examiner la présente proposition de résolution européenne.

M. le président Pieyre-Alexandre Anglade. L'ordre du jour appelle l'examen de la proposition de résolution européenne relative à l'urgence démocratique d'appliquer pleinement et entièrement le règlement européen sur les services numériques, dont Thierry Sother et Jérémie Iordanoff sont les co-rapporteurs.

M. Thierry Sother, co-rapporteur. Lénine a écrit : « Il y a des décennies où rien ne se passe, et des semaines où des décennies se produisent ». Nous y sommes. Une heure et quarante-huit minutes par jour, c'est le temps moyen des Français passés sur les réseaux sociaux. Ils occupent une place non-négligeable dans notre vie et notre démocratie. Un Français sur deux déclare s'y informer. C'est certes un lieu de débats et d'actualités politiques, mais aussi un lieu où l'opinion se forge. Ce temps passé, cette place dans nos vies, c'est la raison économique des plateformes qui déploient leurs efforts pour développer leur centralité dans notre société. Car rien n'est gratuit : pour les plateformes, il faut bien avoir conscience que les citoyens sont des produits. C'est aussi un objet d'intérêt, un point d'entrée pour des puissances étrangères qui voudraient déstabiliser notre vie politique.

Nous nous souvenons, avec la crise du Covid, des dégâts que les théories conspirationnistes et la désinformation peuvent causer et causent encore. Ces pratiques, elles sont aussi orchestrées et dirigées contre nos démocraties. Nous vivons déjà dans une ère où les puissances étrangères remettent en cause notre souveraineté nationale. Dans ce rapport, nous dressons un état de la menace très préoccupant. Par leur fonctionnement et par leur négligence, les réseaux sociaux exposent des pays européens à de graves déstabilisations.

VIGINUM, notre service de lutte contre les ingérences étrangères à la pointe dans le monde, a identifié 230 phénomènes inauthentiques sur les réseaux sociaux, dirigés contre la France en 2023. Ils avaient l'ambition claire de troubler le débat public numérique français. Une douzaine était clairement identifiée comme des ingérences étrangères. Le constat de VIGINUM est plus édifiant encore en ce qui concerne les élections présidentielles roumaines, en novembre 2024. 25 000 comptes, parfois non-humains, et aux affinités pro-russes, se sont fait l'écho d'un candidat jusqu'ici inexistant, via une attaque coordonnée. Des influenceurs étaient rémunérés par des entreprises opaques, en dépit de la loi roumaine. Pire : la plateforme n'a pas considéré que le contenu diffusé par le candidat était de nature politique, lui accordant une place dans l'algorithme que n'avaient pas ses concurrents. Ces manipulations étaient massives, alors qu'un roumain sur deux

s'informe sur Tiktok. La plateforme n'a lancé aucune alerte et n'a pris aucune mesure au moment du scrutin.

Quant à X, Elon Musk a licencié depuis son arrivée à la tête du réseau social la moitié des effectifs en charge de la plateforme. Les insultes, les contenus violents, les contre-vérités s'y répondent désormais sans contrôle. Sur X, on supprime environ 14 000 publications par mois, ce qui peut sembler important, mais c'est 283 fois moins que Tiktok, et 800 fois moins que Facebook. X est devenu une zone de non-droit, et la toxicité qui y règne n'a rien à voir avec la liberté d'expression. C'est un reflet tronqué par le fonctionnement des plateformes et leur besoin de viralité. Le CNRS a prouvé que X propose des recommandations 50 fois plus toxiques que les abonnements des utilisateurs : ils ne choisissent pas la violence, on leur impose. Ce biais est gravissime, car il est démontré que les sentiments négatifs peuvent décourager un électeur d'aller voter, et influencer ses convictions politiques.

Nous pensons pourtant avoir les outils juridiques nécessaires, au niveau européen, pour agir. Le Parlement européen a très largement adopté le règlement sur les services numériques qui comprend des dispositions de bon sens.

Premièrement, le DSA dispose que ce qui est interdit hors-ligne, doit être interdit en ligne, selon les propos qui étaient ceux du commissaire européen Thierry Breton. Comment comprendre qu'un propos insultant, diffamatoire, ou négationniste, puisse ne jamais être supprimé quand, dans la vie réelle, il été empêché, enfermé et son auteur poursuivi et certainement condamné ? Cette lutte pour l'identification et la suppression des contenus illicites incombe clairement aux plateformes, et nos auditions font la démonstration qu'elles ne se conforment pas à cette responsabilité.

Deuxièmement, le DSA prévoit que les plateformes doivent mettre en place des outils efficaces pour identifier et supprimer les contenus non-humains. Or, il n'en est rien. Là encore, la présidentielle roumaine en est un exemple frappant.

Troisièmement, le DSA prévoit que les chercheurs peuvent accéder aux données des plateformes pour nous informer sur la manière dont sont sélectionnés les contenus que nous voyons, par le biais que les réseaux peuvent présenter. Là encore, cette obligation n'est pas respectée. X n'a encore jamais répondu positivement à une réponse faite par un chercheur.

Nous sommes aujourd'hui face à une pièce sombre. Nous pouvons constater la présence de robots, de contenus mensongers ou offensants, ou encore des manœuvres étrangères. Mais nous avons confié aux plateformes l'obligation d'agir et elles ne le font pas. Les infractions sont claires, et pourtant : quelle est la réaction européenne ?

Alors que nous devrions appliquer un principe de précaution démocratique, c'est-à-dire évaluer le risque des atteintes que nous constatons sur notre modèle et ses potentiels dégâts, nous peinons à nous coordonner. La Commission européenne, elle, a lancé des enquêtes, mais n'en achève aucune. Tiktok, Facebook, Instagram,

Meta, X : toutes ces plateformes sont épinglées et aujourd’hui assujetties à une enquête. Mais aucune conclusion n’arrive, même après plus d’un an et demi d’enquête : aucune communication de la part de la Commission européenne qui se retranche derrière le secret de l’instruction. Or, c’est à cause de notre passivité que des étapes sont franchies : je pense là aux ingérences assumées d’Elon Musk qui menacent l’intégrité territoriale des États européens, mais sur lesquels je vais laisser mon collègue Jérémie Iordanoff revenir.

L’absence de modération n’encourage pas à la liberté d’expression, elle ruine le débat en l’ensevelissant sous des manœuvres qui sont parfois d’origine étrangère. Viendra un jour où le second tour de notre élection présidentielle se jouera à quelques dizaines de milliers de voix qui seront peut-être obtenues avec le concours de manœuvres coordonnées par des puissances étrangères. Ce jour-là, il sera trop tard pour se demander si notre démocratie ne valait pas la peine d’être protégée ! C’est pourquoi je vous invite dès aujourd’hui à appeler la Commission européenne et le Gouvernement à prendre les mesures de sanction et de prévention nécessaires pour réguler les réseaux sociaux et nous protéger des ingérences étrangères.

M. Jérémie Iordanoff, co-rapporteur. L’ère du numérique, vu un temps comme celle de la liberté et de l’accès universel à l’information, prend depuis quelques années un tournant préoccupant. Certains analystes qualifient l’évolution récente de la situation de passage dans l’ère de la post-vérité, c’est-à-dire une période où les faits et la vérité n’ont plus de poids face à la multiplicité des discours alternatifs et à l’essor des appels aux sentiments et aux ressentiments. Une période où les assertions s’entrechoquent, où la rumeur est reine, et le mensonge comme un poisson dans l’eau.

En déformant la réalité, et en brouillant les repères factuels, la désinformation détruit le fondement même du débat d’idées et donc de la démocratie. Mon collègue Thierry Sother l’a dit, les réseaux sociaux sont devenus des vecteurs de diffusion à grande échelle de ces faits alternatifs. Ils ne sont pas que cela, évidemment, mais ils sont aussi cela. Certains deviennent même de véritables acteurs de déstabilisation, et d’ingérences étrangères : c’est le cas de la dérive de X, anciennement Twitter, orchestrée par son propriétaire Elon Musk, l’homme le plus riche du monde et compagnon de fortune de Donald Trump. Ce cas illustre parfaitement les évolutions possibles d’un réseau social à l’influence planétaire, soumis aux décisions unilatérales de son propriétaire, dont les intentions sont claires : s’en prendre à la presse indépendante, à l’Union européenne, aux démocraties libérales, et à un corpus de valeurs qui sont les nôtres.

Nos démocraties, construites sur le débat éclairé et la confiance dans les institutions ne peuvent rester sourdes à cette interférence. Nous devons agir collectivement et fermement pour défendre notre souveraineté et la qualité du débat public. Depuis le rachat de ce réseau social, Elon Musk a substantiellement modifié les règles de modération, licencié la plus grande partie des équipes chargées de lutter contre la désinformation et rétabli des milliers de comptes autrefois suspendus pour

incitation à la haine, notamment ceux des personnes ayant participé à la tentative de coup d'État au capitol le 6 janvier 2021.

Plus récemment, nous avons vu comment ces choix éditoriaux ont contribué à amplifier des thèses complotistes, et favorisé la diffusion de fausses informations. Le milliardaire est même intervenu dans l'élection législative allemande en appelant à voter pour l'AFD depuis son compte X, intervention relayée par un algorithme qui met en avant ses propres messages, ainsi qu'une armée de robot qui pullulent sur la plateforme. C'est évidemment illégal, mais c'est la réalité. Un réseau social de cette ampleur, utilisé par des millions d'utilisateurs à travers le monde, ne peut être laissé à la seule main d'un individu, quel qu'il soit. Nous devons mettre un terme à cette manipulation et exiger des garde-fous clairs et transparents pour encadrer ces plateformes : c'est tout l'objet de cette proposition de résolution européenne.

Face à ces menaces, l'Arcom – le régulateur national du numérique – joue un rôle essentiel dans le cadre de l'application du DSA (*Digital Services Act*). Cette autorité indépendante est chargée de surveiller les contenus illicites sur les réseaux sociaux. Elle peut ainsi exiger leur suppression et saisir la justice lorsque que des infractions sont constatées. Toutefois ces moyens d'action restent très insuffisants face à l'ampleur des défis. Il est impératif de la soutenir, de renforcer ses pouvoirs d'enquête et d'accroître ses capacités de sanction en cas d'attaque de grande ampleur nuisant à notre souveraineté nationale.

L'Arcom doit pouvoir bénéficier d'un accès renforcé aux données d'entrée et de sortie des plateformes via des API (interface de programmation d'application). Ces interfaces numériques permettent de connecter des logiciels aux plateformes afin de pouvoir extraire les données d'entrée et de sortie sans impérativement nuire à la santé des algorithmes de mise en avant des contenus. Ainsi, le régulateur national pourrait mieux appréhender les enjeux relatifs à la diffusion de contenus sur les plateformes, imposer des régulations strictes en matière de modération et agir avec une réactivité accrue contre la désinformation et les contenus haineux.

De plus, cette situation met en lumière un débat crucial, celui de la responsabilité des plateformes numériques. Jusqu'à présent elles se sont abritées derrière leur statut d'hébergeur – simple prestataire technique assurant la mise à disposition d'un serveur et d'une interface. Elles se défendent ainsi de tout contrôle sur le contenu et rejettent la responsabilité sur les individus à l'origine de la publication de ces contenus. Pourtant, leur fonctionnement les rapproche de la définition juridique d'un éditeur. Elles sélectionnent, classent, mettent en avant ou rendent invisibles certains contenus via leurs algorithmes, influençant ainsi massivement l'information qui atteint les utilisateurs. Nous pouvons considérer qu'elles ont une ligne éditoriale. Même si elles ne produisent pas elles-mêmes le contenu, il faut considérer leur impact réel sur l'opinion publique pour appréhender cette question.

Au-delà de leur statut, laisser des géants du numérique, essentiellement américains et chinois, occuper l'espace européen revient à confier les règles de la

modération et de la censure à des structures privées dont les pratiques sont difficiles à contester devant la justice. À cet égard, nous vous proposons d'envisager un levier : la cession du capital des géants du numérique à des entités européennes. À titre de comparaison, et comme le dispose la loi relative à la liberté de la communication de 1986, « l'autorisation relative à un service de radio ou une télévision par voie hertzienne terrestre assurée en langue française ne peut être accordée à une société dans laquelle plus de 20 % de capital social ou des droits de vote sont détenus directement ou indirectement par des personnes de nationalité étrangère ». Appliquée aux personnes, cette mesure limiterait donc la concentration des réseaux sociaux par des intérêts étrangers et contribuerait à agir pour maintenir les conditions de notre souveraineté.

Un autre grand sujet pour les utilisateurs est de pouvoir sortir de la captivité des plateformes dominantes sur lesquelles chacun a construit sa communauté. C'est la question de l'interopérabilité. Cette architecture technique est soutenue par le Conseil national du numérique. Elle permettrait à l'utilisateur de changer de plateforme tout en conservant ses contacts et ses contenus. En l'imposant ou en l'encourageant, la Commission européenne briserait l'oligopole des géants du secteur en permettant une concurrence et l'émergence d'initiatives européennes.

Chers collègues, ce rapport montre que nous sommes à un tournant décisif. Nos démocraties ne peuvent plus se permettre d'être des spectatrices passives face à la montée de la manipulation numérique orchestrée par des puissances étrangères et par des intérêts privés.

La Commission européenne dispose de moyens conséquents de contrôle et de sanctions. Elle doit les utiliser rapidement. Il est temps de se saisir pleinement des instruments du DSA et de ne plus craindre les rapports de force avec ces plateformes. Il faudra également envisager de renforcer le DSA et de le refonder pour aller plus loin notamment sur la question des interventions préventives. Il ne faut pas oublier que le régulateur national peut toujours agir en cas de carence au niveau européen. Pour l'instant, l'Arcom ne se saisit pas de ses prérogatives à ce niveau-là.

Face au danger, chacun doit prendre ses responsabilités. Il en va de la préservation de la confiance de nos concitoyens dans le débat public et dans le modèle démocratique. Nous avons les moyens d'agir, il est temps de le faire avec détermination.

L'exposé des co-rapporteurs a été suivi d'un débat.

M. Charles Sitzenstuhl (EPR). Cette résolution européenne appelle la Commission européenne à appliquer avec rigueur le DSA et le DMA (*Digital Markets Act*). Ces textes ont été adoptés sous la présidence française de l'Union européenne afin de s'assurer que les grandes plateformes respectent pleinement les règles établies. Il ne s'agit pas d'une question théorique : depuis des années, nous constatons l'influence croissante des plateformes numériques dans nos vies, mais

aussi sur la vie politique et les élections. Or cette influence n'est pas neutre. Elle peut être exploitée par des puissances étrangères pour manipuler l'opinion publique, fausser le débat démocratique, déstabiliser nos institutions et in fine détruire nos démocraties.

Un évènement récent l'illustre : les ingérences numériques qui ont marqué l'élection présidentielle en Roumanie en 2024. Une vaste opération de manipulation de l'algorithme de Tiktok, appuyée par des milliers de comptes inauthentiques et des influenceurs mobilisés à des fins politiques a conduit la Cour constitutionnelle de Roumanie à annuler les résultats du scrutin. Pour la première fois en Europe, une élection a été annulée en raison d'une ingérence numérique. Face à cela, nous devons être intransigeants. C'est pourquoi notre groupe a déposé un amendement visant à intégrer explicitement cette réalité dans la proposition de résolution. Il est essentiel que l'Union européenne prenne en compte ce précédent et agisse en conséquence pour prévenir de tels scénarios à l'avenir. Le risque n'est pas lointain : il nous concerne directement. Comme l'a rappelé le président de la République lors de son adresse du 5 mars dernier, certains États, en particulier la Russie, cherchent à manipuler nos opinions via la diffusion de fausses informations. Cette stratégie de désinformation combinée à des cyberattaques visant nos infrastructures critiques, constitue une menace directe pour notre souveraineté.

L'Europe ne peut pas rester passive face à ces attaques. Il ne suffit pas d'avoir des textes ambitieux : encore faut-il les appliquer avec fermeté. Cette résolution rappelle à la Commission européenne qu'elle doit utiliser pleinement ses pouvoirs pour contraindre et sanctionner les plateformes qui ne respectent pas les règles. L'impunité des géants du numérique doit cesser.

C'est pourquoi le groupe EPR soutien avec force cette proposition de résolution, enrichie des amendements portés par notre groupe. J'invite l'ensemble des collègues à se mobiliser avec la même détermination.

M. Thierry Sother (SOC). Merci pour votre soutien. J'apporte une information complémentaire. En rédigeant cette proposition de résolution, je pensais également que l'algorithme avait été modifié dans le cas roumain. Dans les échanges que nous avons pu avoir pendant les auditions, il apparaît que cela a été assez peu le cas. En réalité, il n'y a pas de contrôle de ce qui se passait. Je conseille de lire sur ce point le rapport de Viginum dont je salue le travail exemplaire. Viginum accomplit un travail méconnu et pas assez visible. En dépit de faibles moyens, cet organe réalise un travail d'étude et de suivi de l'ensemble des plateformes. Je suggère que son responsable soit auditionné.

Mme Marietta Karamanli (SOC). Cette proposition de résolution européenne est très importante. Elle vise à accélérer l'application du dispositif européen assurant la régulation des plateformes numériques. Notre commission a eu déjà à plusieurs reprises l'occasion d'évoquer la réglementation des plateformes numériques. Leur nécessaire régulation nous permet de rappeler ici que leur responsabilité, en tant que diffuseur de contenu, dans le respect des droits de

propriété intellectuelle et dans la protection des droits des citoyens, est un grand sujet. Elles peuvent être un moyen aussi de privatisation, au sens d'une prise de contrôle par les grandes entreprises privées d'un nombre significatif de services, et ce hors de toute régulation. Leur responsabilité dans l'information de l'opinion est devenue une question politique et démocratique. S'ajoute à cela l'insuffisance de modération, l'absence de lutte contre les fausses nouvelles et la création de réflexes par la répétition d'images ainsi que la sollicitation quasi automatisée : tout ceci est de nature à fortement inquiéter.

Toutefois, nous ne sommes pas découragés. Nous appelons donc les autorités de l'Union et le gouvernement français à accélérer la mise en œuvre des mesures déjà adoptées. Le DMA vise aussi à renforcer la contestabilité des positions dominantes acquises par les géants du numérique. Notre groupe a déjà fait des observations pour dire que ces instruments sont complexes, souvent à la main de la Commission : ils offrent des possibilités, mais cela ne garantit pas toujours l'effectivité des droits créés. L'approche européenne est le bon échelon : elle consiste à privilégier une régulation *ex ante* et asymétrique, c'est-à-dire proportionnée à la taille des acteurs. Lors de l'examen de ces deux textes par l'Assemblée nationale, notre commission avait porté déjà un certain nombre de suggestions d'amélioration de ces dispositifs, tels que la possibilité pour plusieurs États membres de saisir la Commission pour ouvrir une enquête. Il est important que la résolution permette que l'on puisse hâter le pas et dresser un bilan des textes adoptés. Nous soutenons donc votre proposition.

M. Thierry Sother, co-rapporteur. Un processus de contrôle du DSA-DMA est prévu en son sein et doit intervenir en 2027, ce qui est peut-être trop tardif. Le DSA-DMA est pleinement opérationnel depuis le mois de février 2024. Il a donc un peu plus d'un an d'existence, mais cela n'empêche pas de faire pression pour qu'il y ait des communications d'étapes de la part de la Commission sur les travaux menés qui sont parfois sujets à une certaine opacité.

Par exemple, la première procédure enclenchée au titre du DSA l'a été en décembre 2023. Or nous n'avons toujours pas d'informations quant à la suite de cette procédure.

Mme Sophie Taillé-Polian (EcoS). Le groupe Écologiste et Social partage la nécessité d'appliquer pleinement le règlement européen sur les services numériques. La position de l'Union européenne doit être ferme et volontariste face aux plateformes. L'enjeu est de sanctionner les récalcitrants dans l'intérêt de nos sociétés et des citoyens européens. Nous soutenons donc cette proposition de résolution européenne.

Depuis plusieurs semaines, le président de la République et son Premier ministre préparent les esprits à un effort budgétaire pour le réarmement de notre pays. Le 4 mars dernier, la Commission européenne a dévoilé son plan « réarmer l'Europe » pour soutenir l'Ukraine et assurer la défense de l'Union européenne. Ce

sujet s'est également invité dans notre assemblée. Cependant, il me semble que nous ne pouvons limiter notre réflexion à la question militaire.

Une stratégie de défense complète et cohérente dans une société démocratique comme la nôtre passe par une politique offensive d'affirmation de la liberté d'expression, conjuguée au droit des citoyennes et citoyens à accéder à une information fiable et indépendante.

La maîtrise de la production et de la diffusion de l'information est une arme essentielle pour l'agresseur russe en Ukraine et elle fragilise nos démocraties européennes. Cependant, la Russie n'est pas la seule ennemie de l'Union européenne sur ce sujet, comme l'illustrent les ingérences récentes de M. Musk dans les élections nationales britanniques et allemandes. M. Musk n'est plus seulement un milliardaire qui rachète un réseau social à des fins politiques, il est également l'un des plus proches conseillers du président américain, un artisan de la politique qui est menée.

Aussi regrettons-nous que la présidente de la Commission européenne n'affirme pas avec plus de force la défense de l'Union européenne dans cette guerre culturelle qu'assument de mener contre nous les États-Unis.

Mme Isabelle Rauch (HOR). Les grandes plateformes en ligne sont obligées en application du règlement européen sur les services numériques – DSA – d'éviter la diffusion de contenus illicites comme les appels à la haine, l'apologie du terrorisme ou les propos pédopornographiques. C'est pour cela que la Commission européenne a lancé plusieurs enquêtes visant la plateforme X mais aussi d'autres plateformes très utilisées par nos concitoyens comme TikTok, Meta, Temu et Shein.

Ces enquêtes sont nécessaires pour s'assurer que ces plateformes respectent les normes européennes visant à protéger nos concitoyens contre les contenus illicites. Elles sont d'autant plus nécessaires qu'il y a un vrai manque de transparence dans le fonctionnement de ces plateformes, dont on doit déterminer la part de responsabilité dans les tentatives de désinformation, de manipulation et d'ingérence.

Il ne s'agit pas ici, chers collègues, de remettre en cause la liberté d'expression. Cette dernière est garantie par notre Constitution, par la Charte européenne des droits fondamentaux, et par le DSA lui-même. Au contraire, c'est parce que nous voulons une expression libre et indépendante que nous ne pouvons pas accepter que nos concitoyens soient exposés à de la désinformation et à des manipulations.

À plus long terme, si nous voulons durablement protéger nos démocraties, il faut que l'Union européenne développe des plateformes et infrastructures numériques souveraines. En conséquence, nous voterons en faveur de cette proposition de résolution européenne.

M. Thierry Sother, co-rapporteur. Je partage pleinement la nécessité de se doter d'outils adaptés à l'échelle européenne.

Les auditions menées ont permis de comprendre que l'un des défis principaux est celui de l'interopérabilité. L'utilisateur d'une plateforme doit pouvoir assurer le transfert de ses contacts dans une autre plateforme de son choix, comme on peut transférer ses contacts de téléphone lorsque l'on change d'opérateur.

L'interopérabilité est ainsi l'une des conditions *sine qua non* d'une concurrence juste entre les plateformes, de nature à faire émerger des champions européens.

M. Matthieu Marchio (RN). Cette proposition de résolution européenne, bien qu'ayant pour objectif de protéger la démocratie, est le symptôme d'un système qui finit par menacer lui-même nos libertés fondamentales.

Le règlement européen sur les services numériques, que l'on nous presse d'appliquer fermement, risque de nous conduire à plus de censure, avec des amendes colossales pouvant atteindre 6 % du chiffre d'affaires mondial des plateformes. Ce règlement pousse inévitablement les plateformes à une censure préventive et excessive.

L'hypocrisie démocratique de l'Union européenne atteint ici son paroxysme. Cette même Europe qui prétend défendre la démocratie n'a-t-elle pas systématiquement ignoré la volonté des peuples exprimée par référendum ? Le Traité de Lisbonne imposé après le rejet du traité constitutionnel européen par les Français et les Néerlandais en 2005 en est l'illustration parfaite.

Et que dire de cette Commission, composée de commissaires non élus, qui s'érige en ministère de la vérité avec une extension de ses pouvoirs de contrôle au travers du DSA ? Le double standard est flagrant : Meta annonce la fin de l'hypocrite *fact checking* aux États-Unis mais le maintien en Europe sous la pression de la Commission par l'intermédiaire du DSA.

L'Europe devient ainsi le laboratoire d'une censure où des bureaucrates décident de ce qui est vrai ou de ce qui est faux. Nous avons vu en Roumanie jusqu'où peut aller cette ingérence. Si une telle ingérence de la part de la Russie est peut-être survenue – ce que ne confirme ni le rapport Viginum, ni la commission de Venise – faire pression pour l'annulation d'une élection présidentielle est aussi de l'ingérence.

Ma question concerne l'article 36 § 2 du DSA, qui introduit ce que l'on appelle un mécanisme de réaction aux crises. Ce mécanisme permet d'analyser l'impact des activités des VLOP (*Very large online platforms*) et des VLOSE (*Very large online search engines*) sur une crise et de décider des mesures à prendre pour garantir le respect des droits fondamentaux.

Quand on sait que l'article 56 confère à la Commission un pouvoir exclusif de surveillance et d'exécution et que le terme de « crise » n'est pas strictement défini, comment pouvons-nous nous assurer qu'il n'y aura pas d'excès ou de censure ?

M. Thierry Sother, co-rapporteur. Je ne partage pas du tout votre analyse de la situation. La modération, ce n'est pas la censure. Le DMA-DSA vise à assurer la mise en conformité de l'action des plateformes à la réglementation européenne et aux lois que nous avons adoptées. Ce cadre européen a d'ailleurs été très largement soutenu par les parlementaires européens.

Le DMA-DSA ne remet pas en cause la liberté d'expression mais vise à assurer une symétrie : ce qui est interdit dans la vie réelle doit aussi l'être en ligne.

M. Jérémie Iordanoff, co-rapporteur. Je pensais que notre proposition de résolution européenne ferait l'unanimité, mais finalement, ce ne sera pas le cas ! Il faut répondre aux grossièretés de l'analyse de M. Matthieu Marchio car il ne faut pas laisser dire n'importe quoi ! Vous avez fait une attaque en règle contre l'Union européenne, mais en fait vous auriez dû demander à l'Arcom de résoudre le problème.

À propos du DSA, l'application stricte de ce règlement est demandée. Il existe une variété de sanctions possibles, et les sanctions financières ne sont pas dissuasives parce qu'elles arrivent tardivement. Compte tenu de la rapidité et de l'efficacité des actes d'ingérences dans les élections, le DSA ne peut pas régler seul ce problème. Dans trois ans, il sera trop tard. La question de la célérité des procédures est à l'ordre du jour.

Il existe une spécificité de X qui le démarque des autres réseaux sociaux. Habituellement, ces derniers peuvent être à l'origine de perturbations de nature commerciale qui concernent l'opinion publique, en proposant du contenu qui cherche à retenir l'attention des utilisateurs. Pour X, il y a un propriétaire d'un réseau social lié au pouvoir américain qui utilise sa plateforme pour promouvoir sa propre parole, au détriment de son modèle économique. Nous observons une ingérence directe d'un pays étranger, avec une personne qui attaque le premier ministre du Royaume-Uni et qui supporte des candidats d'extrême droite lors des élections en Allemagne. Si cette pratique n'est pas de l'ingérence, alors qu'est-ce c'est ?

Lorsque les Russes font des opérations en Roumanie, en Allemagne, en France, ou en Pologne, de quoi s'agit-il ? Les autorités russes payent des personnes pour organiser des opérations physiques, qui sont ensuite relayées sur les réseaux sociaux grâce à des armées de robots qui multiplient le contenu. Les algorithmes rendent possible des phénomènes d'emballlement à partir d'une trentaine de personnes. L'information qui arrive aux utilisateurs est biaisée. Si cette pratique n'est pas de l'ingérence, alors qu'est-ce que c'est ?

Le Rassemblement national parle constamment de souveraineté nationale. Quelle est la souveraineté des citoyens d'un État dont le débat public démocratique serait piloté depuis les États-Unis ou la Russie ?

Concernant la censure, c'est bien M. Donald Trump qui interdit un certain nombre de vocabulaires, de mots dans les universités, qui coupe des financements. Cela est de la censure. Lorsque sont interdits des contenus haineux parce qu'ils seraient des insultes racistes ou homophobes, est-ce que c'est de la censure pour vous ?

Il est nécessaire de mettre le DSA en œuvre le plus fermement possible. D'ailleurs, ce règlement ne suffira pas et il faudra aller plus loin.

Mme Sandrine Rousseau (EcoS). Le texte est absolument indispensable puisque les algorithmes des réseaux sociaux sont de nature à influencer notre capacité à réfléchir et à avoir des informations indépendantes ou fictives. Il est néanmoins important de rajouter un élément : les réseaux sociaux ont une influence sur l'état psychique notamment de nos jeunes. Une augmentation est constatée du taux de suicide chez les jeunes filles depuis 2006 avec un accroissement de plus de 570 %. Une partie de cette augmentation tient à l'addiction, à la dépendance aux réseaux, et à la non-modération des contenus présentés. La question des algorithmes est aussi une question de santé publique.

M. le président Pierre-Alexandre Anglade. Nous en venons à l'examen de la proposition de résolution européenne et des amendements qui ont été déposés.

Amendement n° 4 de Mme Constance Le Grip

Mme Constance Le Grip (EPR). Cet amendement vise à mentionner l'existence d'un ensemble de travaux parlementaires déjà effectué sur la détection et la prévention des ingérences en France. Il fait référence à un rapport d'information écrit pour le compte de la commission des affaires européennes ainsi qu'à un rapport d'information portant observation sur une proposition de loi.

M. Thierry Sother, co-rapporteur. Avis favorable.

M. Jérémie Iordanoff, co-rapporteur. Avis de sagesse, je n'ai pas lu le rapport d'information mentionné mais je ne m'y opposerai pas.

L'amendement n° 4 est adopté.

Amendement n° 5 de Mme Constance Le Grip

Mme Constance Le Grip (EPR). Le volet détection prévention et lutte contre les ingérences étrangères est important dans les prises de paroles faites par les co-rapporteurs et dans les écrits du rapport d'information. Il semblait nécessaire de renforcer la présence dans le texte de la PPRE d'autres travaux parlementaires récents. L'amendement n° 5 évoque le rapport de la commission d'enquête relative aux ingérences politiques, économiques et financières portant sur les puissances

étrangères. Il fait état de la dangerosité des ingérences étrangères à l'œuvre contre nos démocraties européennes.

M. Thierry Sother, co-rapporteur. Je donne un avis favorable pour cet amendement. Ces travaux d'enquête ont porté pour la première fois à notre attention la question des ingérences. L'évolution de la menace est constante, et les différents types et actions d'ingérence possibles sont également très fréquents.

M. Charles Sitzenstuhl (EPR). Une audition particulièrement importante s'est tenue, et je vous invite à en prendre connaissance afin de préparer la suite de vos travaux ou de renforcer votre argumentaire. Il s'agit de celle du secrétaire général à la défense et à la sécurité nationale, M. Bouillon, qui était accompagné du directeur de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI). Cette audition s'est déroulée à huis clos, mais son compte rendu a été rendu public, comme toutes les auditions à huis clos menées dans le cadre des commissions d'enquête. Je vous encourage à le consulter, car il contient de nombreuses informations qui n'ont pas toujours été relayées dans la presse. Notamment, elle met en évidence le fait que 2017 marque le début des problèmes numériques liés à des ingérences extérieures en France, avec l'épisode des *Macron Leaks* et une présomption très forte d'une opération organisée depuis la Russie. Cette affirmation a été formulée par de hauts fonctionnaires de l'État.

L'amendement n° 5 est adopté.

Amendement n° 1 de M. Charles Sitzenstuhl

M. Charles Sitzenstuhl (EPR). Cet alinéa vise à ajouter une mention explicite concernant la Roumanie. La Cour constitutionnelle de Roumanie a annulé les élections. Nos collègues qui expliquent que cette annulation relève d'une ingérence étrangère ont peut-être une vision de la démocratie où toute intervention du pouvoir judiciaire constituerait une ingérence.

M. Thierry Sother (rapporteur). Malheureusement, les collègues qui assimilaient l'annulation des élections roumaines à une ingérence bruxelloise ou européenne ne sont plus présents. Je ne suis pas opposé à l'amendement que vous proposez, mais je propose un sous-amendement afin de le compléter avec des éléments de citation issus du rapport de Viginum.

M. Charles Sitzenstuhl (EPR). J'y suis favorable et je pense que l'amendement est plus solide en faisant référence aux travaux de Viginum.

Mme Constance Le Grip (EPR). Je suis favorable à cet amendement ainsi qu'au sous-amendement qui vient le compléter. Je souligne la nécessité de nous saisir de la question des ingérences étrangères dans les processus électoraux partout en Europe, notamment en Moldavie et en Géorgie. La France, à la faveur de la récente venue de la présidente Maia Sandu à Paris, a signé un accord renforcé de coopération et d'accompagnement très solide, qui, je l'espère, sera durable. Cet accord associe l'ANSSI, Viginum et plusieurs organismes moldaves en prévision

des futurs scrutins prévus au début de l'automne. Je fais également écho à la commission spéciale récemment reconstituée par le Parlement européen, qui s'est vu attribuer un cadre de travail très large. Cette commission, dédiée au bouclier européen pour la démocratie et présidée par Nathalie Loiseau, entre clairement en résonance avec vos travaux et les préoccupations fortes que vous exprimez.

Le sous-amendement n° 1 est adopté

L'amendement ainsi modifié n° 1 est adopté

Amendement n° 6 de Mme Constance Le Grip.

Mme. Constance Le Grip (EPR). Il s'agit de renforcer, dans le texte même de votre proposition de résolution européenne, l'importance que revêt la menace d'ingérence étrangère pour nos processus électoraux, ainsi que pour nos souverainetés nationales et européennes. À juste titre, le DSA constitue une avancée, mais il faudra sans doute aller plus loin. Des pistes de réflexion, tant nationales qu'européennes, restent à explorer.

M. Thierry Sother, co-rapporteur. Avis favorable.

L'amendement n° 6 est adopté

Amendement n° 3 de M. Jérémie Iordanoff (co-rapporteur).

M. Jérémie Iordanoff, co-rapporteur. Cet amendement vise à insister sur la question de la propriété de ces plateformes, étant entendu qu'aujourd'hui, elles sont principalement américaines et chinoises. Il s'agit de permettre une forme de sanction et d'imposer le transfert de leurs parts à des entités européennes.

M. Charles Sitzenstuhl (EPR). Nous voterons contre cet amendement, non pas par opposition sur le fond, mais parce que nous avons des doutes sur la manière dont il est rédigé, notamment dans son I qui vise une personne en particulier. Il faudrait peut-être le retravailler pour s'assurer qu'il soit solide juridiquement.

M. Jérémie Iordanoff, co-rapporteur. Je vous propose de supprimer le I et, au grand II, de supprimer les références à la plateforme X pour que cela concerne l'ensemble des plateformes numériques.

M. Charles Sitzenstuhl (EPR). Nous souscrivons à cette proposition

L'amendement n° 3 rectifié est adopté

Amendement n° 2 de M. Charles Sitzenstuhl

M. Charles Sitzenstuhl (EPR). Cet amendement vise à faire mention de l'adresse du président de la République du 5 mars dernier qui évoque explicitement le sujet des ingérences.

M. Thierry Sother, co-rapporteur. Je ne suis pas opposé à votre amendement dont je comprends le sens.

M. Jérémie Iordanoff, co-rapporteur. Je comprends que vous vouliez rajouter cette référence. Il est très utile que le président de la République ait ainsi évoqué la question des ingérences étrangères.

L'amendement n° 2 est adopté.

Amendement n° 7 de Mme Constance Le Grip

Mme Constance Le Grip (EPR). Cet amendement fait écho à la déclaration du 21 janvier 2025 du Conseil et de la Commission européenne devant le Parlement européen qui vise à réaffirmer l'urgence à appliquer strictement le DSA. Hier après-midi, dans cette même salle, à la faveur de la discussion d'une proposition de résolution européenne visant à renforcer notre lutte européenne contre l'antisémitisme, nous avons également appelé à un renforcement et à une accélération du DSA.

M. Jérémy Iordanoff, co-rapporteur. Avis défavorable car cet amendement s'adresse non seulement à la Commission mais aussi au Conseil qui n'a pas de pouvoir d'initiative. Je demande le retrait de l'amendement.

M. Charles Sitzenstuhl, EPR. Je souhaite profiter de cet amendement pour demander aux deux rapporteurs si un recours en carence ne pourrait pas être introduit contre la Commission pour défaut de mise en œuvre du DSA. Pourrait-on faire expertiser ce sujet ?

M. Pierre Pribetich (SOC). En marge de ces discussions, il serait utile d'étudier *l'hyper-trading* et les robots qui permettent de faire des fluctuations financières et déstabilisent les gouvernements. Il s'agit d'un élément qui risque de déstabiliser des économies fragilisées par des conflits internationaux.

M. Thierry Sother, co-rapporteur. Je partage l'avis de mon co-rapporteur sur l'amendement. Pour répondre à la question de Charles Sitzenstuhl, nous n'en sommes pas encore au point de considérer qu'il y a carence de la Commission européenne. Lors de son audition, la Commission européenne a invoqué le temps mis pour se mettre en place. Toutefois, si la Commission européenne continue à ne pas agir, il ne faut pas exclure de recourir à de nouveaux moyens pour faire pression sur elle.

Mme Constance Le Grip (EPR). Je retire mon amendement. J'entends ce que disent les co-rapporteurs et je ne veux pas créer de malentendu.

L'amendement n° 7 est retiré.

Amendement n° 9 de M. Jérémy Iordanoff et M. Thierry Sother

M. Thierry Sother, co-rapporteur. À travers les auditions, nous avons réalisé que le DSA est avant tout un outil de mise en conformité au droit européen. Il doit être un outil de gestion de crise adapté pour pouvoir agir en cas d'infraction grave.

L'amendement n° 9 est adopté.

Amendement n° 8 de M. Jérémy Iordanoff et M. Thierry Sother

M. Thierry Sother, co-rapporteur. Pour donner davantage de lisibilité à la proposition de résolution européenne, nous proposons une modification de son titre.

L'amendement n° 8 est adopté.

L'article unique de la proposition de résolution européenne est adopté.

La proposition de résolution ainsi modifiée est par conséquent adoptée.

M. Thierry Sother, co-rapporteur. Nous nous situons à des instants cruciaux sur ces questions de réseaux sociaux, d'information et d'ingérence. Il faut être vigilant, maintenir la pression et poursuivre la réflexion sur les outils nécessaires, tant sur le plan législatif que réglementaire.

M. Jérémy Iordanoff, co-rapporteur. J'espère que cette résolution va prospérer en séance et aboutir. Des sujets émergent, il s'agit d'une matière nouvelle, tous les outils ne sont pas encore disponibles. Sur l'idée d'introduire une procédure en carence, je ne pense pas que ça puisse actuellement aboutir mais si l'Union européenne n'est pas assez rapide, les États et les régulateurs nationaux en seront aussi responsables.

M. Charles Sizenstuhel (EPR). Il s'agit d'un débat majeur. Je demande au président d'user de son pouvoir d'influence au sein de la conférence des présidents pour que ce texte puisse être examiné en séance lors d'une journée et à un horaire, décents. Il me semble fondamental que l'ensemble de la représentation nationale prenne le temps de débattre d'une question essentielle pour l'avenir de notre démocratie.

PROPOSITION DE RÉSOLUTION EUROPÉENNE INITIALE

Article unique

- ① L'Assemblée nationale,
- ② Vu l'article 88-4 de la Constitution,
- ③ Vu l'article 151-5 du Règlement de l'Assemblée nationale,
- ④ Vu l'article 3 du Traité sur l'Union européenne,
- ⑤ Vu la Charte des droits fondamentaux de l'Union européenne et notamment son article 11, article 21, article 22, article 23, et article 38,
- ⑥ 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,
- ⑦ Vu le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828, entré en vigueur le 1^{er} août 2024,
- ⑧ Vu la communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions du 19 février 2020 intitulée « Façonner l'avenir numérique de l'Europe » COM(2020) 67 final et le programme d'action pour la décennie numérique de l'Europe à l'horizon 2030,
- ⑨ Vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions du 26 mai 2021, intitulé « Orientations de la Commission européenne visant à renforcer le code européen de bonnes pratiques contre la désinformation », COM(2021) 262 final,
- ⑩ Vu la loi n° 2024-449 du mardi 21 mai 2024 visant à sécuriser et à réguler l'espace numérique,
- ⑪ Vu le rapport du Sénat n° 75 (2018-2019) de Mme Catherine Morin-Desailly, fait au nom de la commission de la culture, de l'éducation et de la communication, sur la proposition de loi relative à la lutte contre les fausses informations, déposé le 24 octobre 2018,

⑫ Vu la résolution européenne du Sénat n° 31 (2018-2019) du 30 novembre 2018, sur la responsabilisation partielle des hébergeurs de services numériques,

⑬ Vu le rapport d'information du Sénat n° 274 (2021-2022) de Mmes Florence Blatrix Contat et Catherine Morin-Desailly, fait au nom de la commission des affaires européennes, sur la proposition de législation européenne sur les services numériques, déposé le 8 décembre 2021,

⑭ Vu l'étude annuelle du Conseil d'État de 2022 « Les réseaux sociaux : enjeux et opportunités pour la puissance publique », publiée le 27 septembre 2022,

⑮ Vu l'étude de l'Observatoire de l'audience des plateformes en ligne de l'Autorité de régulation de la communication audiovisuelle et numérique au 1^{er} semestre 2024, publiée le 8 novembre 2024,

⑯ Considérant la position ultra-dominante des très grandes plateformes numériques, devenues de véritables infrastructures de communication, à l'heure où environ trois quarts des citoyens européens se déclarent utilisateurs réguliers des réseaux sociaux ;

⑰ Considérant que le modèle économique de ces plateformes, fondé sur une gratuité d'accès et des recettes publicitaires proportionnelles au trafic généré par les utilisateurs, constitue un cadre favorable non seulement à la propagation de nouvelles fausses, contestables ou fallacieuses, mais également à des tentatives de manipulation menées par des personnes ou des États tiers, en particulier en période électorale ;

⑱ Considérant que l'évolution de la politique éditoriale et de modération de ces très grandes plateformes et l'usage qui en fait par certains de leurs propriétaires n'en font plus de simples fournisseurs d'un service de la société de l'information qui ne serait pas responsable des informations transmises ou de l'accès fourni au sens de l'article 4 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 susmentionné ;

⑲ Considérant que par ces évolutions et face à l'inefficacité des actions mises en œuvre par certaines de ces très grandes plateformes pour évaluer et atténuer les risques systémiques sur les processus électoraux, celles-ci représentent une menace pour les droits fondamentaux des citoyens non-européens, la qualité du débat public et plus largement la souveraineté politique et démocratique des États membres de l'Union ;

⑳ Considérant qu'il est indispensable de mettre en œuvre des normes de sécurité dès la conception des systèmes régissant ces très grandes plateformes, afin de favoriser le respect des droits fondamentaux ;

㉑ 1. Appelle la Commission européenne à appliquer fermement et sans délai le règlement européen et ce faisant, à faire usage de l'intégralité des pouvoirs qui

lui sont conférés par les articles 67 et suivants du règlement sur les marchés numériques, non pas seulement en matière d'investigation, mais aussi, en cas de non-conformité avérée d'une très grande plateforme numérique, pour contraindre et sanctionner ladite plateforme ;

22

2. Appelle la Commission européenne à communiquer sans attendre aux parlements nationaux l'état d'avancement des différentes procédures formelles qu'elle a ouvertes à l'encontre des très grandes plateformes numériques et les résultats des procédures ouvertes depuis plus d'un an ;

23

3. Invite la Commission européenne à un nouvel examen de la détermination de X comme contrôleur d'accès au marché numérique au titre du règlement sur les marchés numériques ;

24

4. Se félicite de la décision de la Commission européenne prise le 17 janvier 2025 d'approfondir son enquête sur X afin d'obtenir du réseau social des informations supplémentaires sur la conception et le fonctionnement de ses algorithmes de recommandation mais souhaite une investigation rapide et transparente ;

25

5. Invite le Gouvernement à relayer ces appels auprès de la Commission et à œuvrer pour un usage déterminé par l'Union européenne de tous les outils réglementaires, économiques et diplomatiques à sa disposition pour contraindre les très grandes plateformes numériques au respect de ses règles dans l'espace numérique européen ;

26

6. Appelle la Commission européenne à élaborer une stratégie de développement de plateformes et infrastructures numériques souveraines au sein de l'Union.

AMENDEMENTS EXAMINÉS PAR LA COMMISSION

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÈGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 4

présenté par
Mme Constance Le Grip

ARTICLE UNIQUE

Après l'alinéa 13, ajouter l'alinéa suivant :

« Vu le rapport d'information de Mme Constance Le Grip déposé par la commission des affaires européennes portant observations sur la proposition de loi visant à prévenir les ingérences étrangères en France (n° 2150), n° 2385, du mercredi 20 mars 2024 ; »

EXPOSÉ SOMMAIRE

L'Union européenne est confrontée à une guerre hybride croissante, marquée par des cyberattaques, des campagnes de désinformation et des ingérences étrangères visant à fragiliser ses démocraties. Le rapport d'information du 20 mars 2024 met en évidence ces menaces, en s'appuyant notamment sur les travaux de la commission spéciale INGE du Parlement européen.

En intégrant la référence à ce rapport dans ce texte, cet amendement rappelle que la protection de la démocratie européenne passe par une application rigoureuse du DSA et un engagement renforcé contre la guerre hybride, qui menace directement l'intégrité des processus électoraux et la souveraineté démocratique.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÉGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 5

présenté par
Mme Constance Le Grip

ARTICLE UNIQUE

Après l'alinéa 13, ajouter l'alinéa suivant :

« Vu le rapport de l'Assemblée nationale fait au nom de la commission d'enquête *relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français*, n° 1311, du 1^{er} juin 2023 ; »

EXPOSÉ SOMMAIRE

Cet amendement vise à intégrer dans cette PPRE une référence au rapport de l'Assemblée nationale du 1er juin 2023 de la commission d'enquête sur les ingérences étrangères, en particulier la section intitulée « Médias, plateformes numériques, nouvelles technologies : principaux points de vulnérabilité ». Cette partie du rapport souligne que les médias numériques et les nouvelles technologies constituent des vecteurs privilégiés pour les ingérences étrangères, notamment par le biais de la diffusion de fausses informations et de la manipulation de l'opinion publique.

En renforçant la transparence des algorithmes, en promouvant les contenus issus de sources fiables et en luttant contre les comptes propageant massivement de fausses informations, le Règlement sur les services numériques (DSA) offre des outils essentiels pour protéger l'intégrité du débat public et préserver la souveraineté démocratique. Cet amendement souligne ainsi l'urgence d'une application rigoureuse du DSA pour combattre les vulnérabilités identifiées et assurer la résilience de nos institutions face aux ingérences étrangères.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

RAPPELANT L'URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTièrement LE RÈGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

SOUS-AMENDEMENT

N° 1

présenté par

MM. Thierry Sother, Jérémie Jordanoff

à l'amendement n°1 de M. Charles Sitzenstuhl

ARTICLE UNIQUE

Remplacer l'alinéa suivant :

« Considérant l'implication des plateformes numériques dans les ingérences étrangères affectant les scrutins démocratiques en Europe, et plus particulièrement les manipulations ayant visé l'élection présidentielle roumaine de 2024, lesquelles ont conduit la Cour constitutionnelle de Roumanie à annuler les résultats du scrutin. »

Par l'alinéa suivant :

« Considérant l'implication des plateformes numériques dans les ingérences étrangères affectant les scrutins démocratiques en Europe, et notamment les manipulations ayant visé l'élection présidentielle roumaine de 2024, telles que décrites par le rapport de VIGINUM du 04 février 2025, lesquelles ont conduit la Cour constitutionnelle de Roumanie à annuler les résultats du scrutin. »

EXPOSÉ SOMMAIRE

Les récentes discussions parlementaires ont été le théâtre de débats sur le fait de savoir si l'élection présidentielle roumaine avait été l'objet ou non de déstabilisations et d'ingérences étrangères. Or, un rapport de VIGINUM rendu le 04 février 2025 apporte une expertise factuelle et fiable s'agissant des événements, établissant clairement la manipulation du scrutin.

Il attribue notamment la popularité du candidat pro-russe Călin Georgescu à une « manipulation coordonnée de l'algorithme de recommandation, via la publication massive de vidéos et de commentaires comportant certains hashtags et mots-clés. En effet, cette campagne a reposé, d'une part, sur l'action coordonnée de réseaux de comptes, et d'autre part, sur l'instrumentalisation de la popularité d'influenceurs rémunérés de manière dissimulée. »

Parce que le rapport vient établir des faits clairs et attestés d'une campagne de manipulation tout en évaluant les risques de tels agissements contre notre pays, les rapporteurs souhaitent en faire mention.

Enfin, les rapporteurs proposent de substituer « notamment » à « plus particulièrement » pour ne pas laisser penser que la proposition de résolution serait plus attentive aux dérives d'une plateforme par rapport à une autre.

Ce sous-amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÉGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 1

présenté par

M. Charles Sitzenzstuhl, M. Pieyre-Alexandre Anglade, Mme Liliana Tanguy, M. David Amiel,
Mme Céline Calvez, M. Sébastien Huyghe, M. Jean Laussucq, Mme Constance Le Grip

ARTICLE UNIQUE

Après l'alinéa 17 :

Insérer l'alinéa suivant :

« Considérant l'implication des plateformes numériques dans les ingérences étrangères affectant les scrutins démocratiques en Europe, et plus particulièrement les manipulations ayant visé l'élection présidentielle roumaine de 2024, lesquelles ont conduit la Cour constitutionnelle de Roumanie à annuler les résultats du scrutin. »

EXPOSÉ SOMMAIRE

Les récentes manipulations observées lors de l'élection présidentielle roumaine de 2024, principalement sur la plateforme TikTok, marquent un tournant majeur dans l'analyse des ingérences numériques dans les processus électoraux en Europe. Cette campagne sophistiquée, impliquant la manipulation de l'algorithme de TikTok et l'instrumentalisation d'influenceurs, a révélé l'ampleur et la complexité des nouvelles formes d'ingérence numérique. Des milliers de comptes inauthentiques ont été activés de manière coordonnée pour promouvoir artificiellement un candidat, modifiant ainsi les dynamiques de la campagne électorale et faussant la perception publique de son soutien.

L'impact de ces manipulations a été tel que la Cour constitutionnelle roumaine a annulé les résultats de l'élection présidentielle, pointant les irrégularités liées à la manipulation de l'information et à la violation des lois électorales. Ce précédent constitue le premier cas en Europe où des résultats électoraux ont été annulés en raison de l'ingérence numérique, soulignant l'importance de renforcer la protection contre ces pratiques.

Les autorités roumaines ont suggéré que ces manipulations étaient le fait d'acteurs étrangers malveillants, une hypothèse qui mérite une attention particulière. La transposition de ces méthodes en France et en Europe représente une menace tangible pour l'intégrité des processus démocratiques.

En particulier, la manipulation des plateformes sociales telles que TikTok, qui comptent un nombre croissant d'utilisateurs et d'influence, est facilement reproductible et pourrait être

exploitée pour perturber les débats publics, influencer les résultats électoraux et semer la méfiance parmi les électeurs.

Les plateformes numériques, en l'absence de mesures adéquates de modération, facilitent la propagation de contenus inauthentiques et l'instrumentalisation des influenceurs. Cette dynamique met en lumière une vulnérabilité croissante des démocraties européennes face à des acteurs extérieurs qui cherchent à déstabiliser les élections en exploitant la visibilité en ligne et les biais des algorithmes des réseaux sociaux.

Ainsi, il est impératif de rappeler que ces ingérences ne se limitent pas à un événement isolé en Roumanie, mais s'inscrivent dans une tendance plus large d'actions visant à manipuler l'opinion publique via les outils numériques. Le rapport des autorités roumaines et les analyses menées par VIGINUM démontrent la nécessité d'une vigilance accrue face à ces risques, tant pour la France que pour l'ensemble de l'Europe. Ce contexte appelle à des actions concertées pour prévenir de telles ingérences, protéger le débat public et assurer la transparence et l'intégrité des processus électoraux dans un environnement numérique de plus en plus complexe et interconnecté.

Cet amendement modifié par le sous-amendement n°1 est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÉGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 6

présenté par
Mme Constance Le Grip

ARTICLE UNIQUE

Après l'alinéa 17, ajouter l'alinéa suivant :

« Considérant que les ingérences étrangères constituent une menace grave pour la souveraineté nationale et européenne, en exploitant les vulnérabilités informationnelles, économiques et politiques des démocraties, et que ces stratégies hostiles, souvent orchestrées par des puissances étrangères, s'inscrivent dans une logique de guerre hybride visant à affaiblir l'Union européenne en combinant manipulation de l'information, financement occulte d'acteurs d'influence et exploitation des failles numériques, rendant indispensable une réponse coordonnée entre les États membres et les institutions européennes pour garantir la résilience démocratique du continent ; »

EXPOSÉ SOMMAIRE

Cet amendement insiste sur la dimension européenne des ingérences étrangères, qui ne menacent pas seulement la France mais l'ensemble des démocraties de l'Union européenne. Il s'appuie sur les travaux du rapport d'information du 20 mars 2024, qui met en évidence une guerre hybride croissante, marquée par des cyberattaques, des campagnes de désinformation et des tentatives de manipulation électorale.

Face à ces risques, le rapport souligne l'importance d'une application stricte du Règlement sur les services numériques (DSA), visant à limiter la propagation des fausses informations et à imposer un contrôle accru des grandes plateformes numériques. Il insiste également sur la nécessité d'un renforcement de la coopération entre les États membres et les institutions européennes, notamment via des outils comme le Service européen d'action extérieure (SEAE) et Viginum, afin de détecter et contrer ces ingérences en temps réel.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÉGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 3 rect

présenté par

MM. Jérémie IORDANOFF et Thierry SOTHER, co-rapporteurs

ARTICLE UNIQUE

I - Après l'alinéa 25, insérer les alinéas suivants :

« Appelle la Commission européenne à édicter toute décision visant à imposer aux propriétaires des plateformes numériques de céder les parts de capital qu'ils détiennent dans ces plateformes, correspondantes à leurs activités européennes, à un tiers n'étant pas placé en situation de conflit d'intérêts et, à défaut, à décider la suspension ou l'interdiction des plateformes dans l'Union européenne » ;

« . Invite le Gouvernement à proposer à la Commission européenne l'édiction de toute décision utile visant à imposer aux propriétaires des plateformes numériques de céder les parts de capital qu'ils détiennent dans ces plateformes, correspondantes à leurs activités européennes, à un tiers n'étant pas placé en situation de conflit d'intérêts et, à défaut, à décider la suspension ou l'interdiction des plateformes dans l'Union européenne ».

EXPOSÉ SOMMAIRE

Cet amendement vise à considérer l'impact spécifique de la plateforme X sur les échanges d'informations et d'opinions est considérable de par le monde. L'Europe n'échappe pas à cette règle. Cette plate-forme a pour caractéristique d'être la propriété de M. Elon Musk, milliardaire également placé à la tête d'une agence fédérale des États-Unis par le Président nouvellement élu de cet État fédéral, M. Donald Trump. Cette situation conduit à un conflit d'intérêts patent qui n'est pas sans conséquence.

Force est de constater que cette plate-forme numérique peut désormais être considérée de manière particulière, notamment par les prises de position de son propriétaire, mais également par l'absence de régulation appropriée des contenus qui y sont postés, de nombreuses modifications de l'algorithme de mise en avant des messages postés sur la plateforme, le recours à des robots numériques amplifiant les contenus, et l'invisibilisation volontaire des contenus postés par les médias traditionnels.

Cette plateforme est devenue un véritable outil de déstabilisation de l'Union Européenne et de ses États membres piloté par M. Elon Musk. Ce dernier agissant en soutien des mouvements d'extrême-droite, fragilisant ainsi les gouvernements en place et polluant le débat public à des degrés encore jamais atteints depuis la création de l'Union et dans un contexte inédit de conflit avec la Russie.

Il est aujourd'hui nécessaire que l'Union européenne réagisse par des décisions proportionnées à la menace à laquelle elle fait face. C'est la raison pour laquelle cet amendement propose d'étudier tous les mécanismes utiles permettant de contraindre la plateforme X à céder les parts de ses filiales européennes à un tiers public.

Cet amendement rectifié est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÉGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 2

présenté par

M. Charles Sitzenzstuhl, M. Pieyre-Alexandre Anglade, Mme Liliana Tanguy, M. David Amiel,
Mme Céline Calvez, M. Sébastien Huyghe, M. Jean Laussucq, Mme Constance Le Grip

ARTICLE UNIQUE

Après l'alinéa 19 :

Insérer l'alinéa suivant :

« Considérant l'adresse aux Français du président de la République le 5 mars 2025, dans laquelle il affirme que certains États, en tête desquels la Russie, cherchent à manipuler nos opinions par la diffusion de mensonges sur les réseaux sociaux. »

EXPOSÉ SOMMAIRE

La menace d'ingérence numérique à travers les plateformes sociales constitue une réalité tangible et caractérisée, comme en témoignent les récentes manipulations observées, notamment lors des élections présidentielles en Roumanie en 2024. Ces ingérences, impliquant l'utilisation coordonnée de comptes inauthentiques et l'exploitation des algorithmes de recommandation, ont non seulement perturbé le processus démocratique dans ce pays, mais ont également soulevé de vives préoccupations quant à la vulnérabilité des démocraties européennes face à des acteurs extérieurs malveillants.

Dans ce contexte, le Président de la République française a, dans son discours du 5 mars 2025, souligné avec clarté et vision l'ampleur de cette menace. Il a mis en lumière les attaques numériques russes visant à paralyser des infrastructures sensibles telles que les hôpitaux, tout en mettant en garde contre les tentatives de manipulation de l'opinion publique via des mensonges diffusés sur les réseaux sociaux. Cette prise de position démontre la conscience aiguë du président de la République française de la nécessité de se prémunir contre de telles menaces et de protéger l'intégrité de l'espace numérique, essentiel à la préservation des processus démocratiques et de la souveraineté nationale.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTIÈREMENT
LE RÉGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 7

présenté par
Mme Constance Le Grip

ARTICLE UNIQUE

Après l'alinéa 24, ajouter l'alinéa suivant :

« Invite le Conseil et la Commission à donner une suite concrète à leur déclaration du 21 janvier 2025 devant le Parlement européen, réaffirmant l'urgence d'une application stricte du DSA afin de préserver la démocratie en ligne face aux ingérences étrangères et aux manipulations de l'information ; »

EXPOSÉ SOMMAIRE

Cet amendement souligne l'importance de traduire en mesures concrètes les engagements pris dans la déclaration du 21 janvier 2025 du Conseil et de la Commission européenne devant les parlementaires européens, en renforçant les obligations des grandes plateformes numériques. Il appelle à une mise en œuvre rigoureuse du DSA, garantissant plus de transparence algorithmique et un contrôle accru des campagnes de désinformation, afin de préserver l'intégrité du débat public et des processus démocratiques en Europe.

Cet amendement est retiré.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

RAPPELANT L'URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTièrement LE RÈGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 9

présenté par
MM. Thierry Sother, Jérémie Jordanoff

ARTICLE UNIQUE

Après l'alinéa 24, insérer l'alinéa suivant :

« Appelle la Commission européenne à mettre en place un dispositif d'urgence harmonisé entre les États membres permettant de prendre des mesures provisoires en cas d'infractions graves aux règlement sur les services numériques risquant de conduire à une crise systémique ».

EXPOSÉ SOMMAIRE

Les auditions menées dans le cadre du présent rapport ont mis en lumière la difficulté, tant de la Commission européenne que du régulateur national, à répondre efficacement et rapidement aux infractions commises envers le règlement sur les services numériques.

En effet, le président de l'ARCOM M. Martin Adjari tout comme le Représentant permanent adjoint (RPA) de la France auprès de l'Union européenne M. Cyril Piquemal ont reconnu la lenteur des procédures tout en les justifiant par le « temps de la sécurité juridique ».

Néanmoins, surtout au regard des événements roumains, il est difficilement concevable que nous n'ayons pour protection de nos démocraties qu'un dispositif de mise en conformité dont l'application ne peut jamais être vérifiée qu'après le déroulement des processus électoraux et donc, possiblement, des ingérences étrangères.

Ainsi, en s'inspirant du référé du droit français, les rapporteurs proposent d'appeler la Commission européenne à construire un nouveau dispositif d'urgence. Cet alinéa additionnel contient plusieurs garde-fous (le fait que la décision revient au régulateur national, qu'il faille des infractions graves et que celles-ci risquent de conduire à une crise systémique) pour indiquer clairement la portée du dispositif.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

19 MARS 2025

RAPPELANT L'URGENCE DÉMOCRATIQUE D'APPLIQUER PLEINEMENT ET ENTièrement LE RÈGLEMENT EUROPÉEN SUR LES SERVICES NUMÉRIQUES (N° 876),

AMENDEMENT

N° 8

présenté par
MM. Thierry Sother, Jérémie Jordanoff

ARTICLE UNIQUE

Dans le titre, substituer aux mots :

« rappelant l'urgence démocratique d'appliquer pleinement et entièrement le règlement européen sur les services numériques »

les mots :

« appelant à la régulation des réseaux sociaux face aux ingérences étrangères »

EXPOSÉ SOMMAIRE

Les auditions menées dans le cadre de cette proposition de résolution ont fait la démonstration que si le règlement sur les services numériques (DSA) était une norme européenne de première importance, contenant de nombreuses dispositions permettant de lutter contre les ingérences étrangères et ayant de réelles traductions nationales, il ne saurait être considéré comme un outil complet et efficace en lui-même.

Il s'agit en effet d'une norme de mise en conformité des plateformes avec les conditions de la liberté d'expression et le cas de l'élection présidentielle annulée en Roumanie tout comme la lenteur des enquêtes diligentées par la Commission européenne illustre ses limites en matière de gestion de crise.

Enfin, le titre d'origine de la proposition de résolution propose une lecture limitée du rôle qu'a à jouer la législation nationale et en particulier l'ARCOM, ou encore le règlement sur les marchés numériques.

Cet amendement est adopté.

PROPOSITION DE RÉOLUTION ADOPTÉE PAR LA COMMISSION

Article unique

- ① L'Assemblée nationale,
- ② Vu l'article 88-4 de la Constitution,
- ③ Vu l'article 151-5 du Règlement de l'Assemblée nationale,
- ④ Vu l'article 3 du Traité sur l'Union européenne,
- ⑤ Vu la Charte des droits fondamentaux de l'Union européenne et notamment son article 11, article 21, article 22, article 23, et article 38,
- ⑥ 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,
- ⑦ Vu le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828, entré en vigueur le 1^{er} août 2024,
- ⑧ Vu la communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions du 19 février 2020 intitulée « Façonner l'avenir numérique de l'Europe » COM(2020) 67 final et le programme d'action pour la décennie numérique de l'Europe à l'horizon 2030,
- ⑨ Vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions du 26 mai 2021, intitulé « Orientations de la Commission européenne visant à renforcer le code européen de bonnes pratiques contre la désinformation », COM(2021) 262 final,
- ⑩ Vu la loi n° 2024-449 du mardi 21 mai 2024 visant à sécuriser et à réguler l'espace numérique,

- ⑪ Vu le rapport du Sénat n° 75 (2018-2019) de Mme Catherine Morin-Desailly, fait au nom de la commission de la culture, de l'éducation et de la communication, sur la proposition de loi relative à la lutte contre les fausses informations, déposé le 24 octobre 2018,
- ⑫ Vu la résolution européenne du Sénat n° 31 (2018-2019) du 30 novembre 2018, sur la responsabilisation partielle des hébergeurs de services numériques,
- ⑬ Vu le rapport d'information du Sénat n° 274 (2021-2022) de Mmes Florence Blatrix Contat et Catherine Morin-Desailly, fait au nom de la commission des affaires européennes, sur la proposition de législation européenne sur les services numériques, déposé le 8 décembre 2021,
- ⑭ Vu le rapport d'information de Mme Constance Le Grip déposé par la commission des affaires européennes portant observations sur la proposition de loi visant à prévenir les ingérences étrangères en France (n° 2150), n° 2385, du mercredi 20 mars 2024 ;
- ⑮ Vu le rapport de l'Assemblée nationale fait au nom de la commission d'enquête *relative aux* ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, n° 1311, du 1^{er} juin 2023 ;
- ⑯ Vu l'étude annuelle du Conseil d'État de 2022 « Les réseaux sociaux : enjeux et opportunités pour la puissance publique », publiée le 27 septembre 2022,
- ⑰ Vu l'étude de l'Observatoire de l'audience des plateformes en ligne de l'Autorité de régulation de la communication audiovisuelle et numérique au 1^{er} semestre 2024, publiée le 8 novembre 2024,
- ⑱ Considérant la position ultra-dominante des très grandes plateformes numériques, devenues de véritables infrastructures de communication, à l'heure où environ trois quarts des citoyens européens se déclarent utilisateurs réguliers des réseaux sociaux ;
- ⑲ Considérant que le modèle économique de ces plateformes, fondé sur une gratuité d'accès et des recettes publicitaires proportionnelles au trafic généré par les utilisateurs, constitue un cadre favorable non seulement à la propagation de nouvelles fausses, contestables ou fallacieuses, mais également à des tentatives de manipulation menées par des personnes ou des États tiers, en particulier en période électorale ;
- ⑳ Considérant l'implication des plateformes numériques dans les ingérences étrangères affectant les scrutins démocratiques en Europe, et notamment les manipulations ayant visé l'élection présidentielle roumaine de 2024, telles que

décrites par le rapport de VIGINUM du 04 février 2025, lesquelles ont conduit la Cour constitutionnelle de Roumanie à annuler les résultats du scrutin.

⑳ Considérant que les ingérences étrangères constituent une menace grave pour la souveraineté nationale et européenne, en exploitant les vulnérabilités informationnelles, économiques et politiques des démocraties, et que ces stratégies hostiles, souvent orchestrées par des puissances étrangères, s'inscrivent dans une logique de guerre hybride visant à affaiblir l'Union européenne en combinant manipulation de l'information, financement occulte d'acteurs d'influence et exploitation des failles numériques, rendant indispensable une réponse coordonnée entre les États membres et les institutions européennes pour garantir la résilience démocratique du continent ;

㉑ Considérant que l'évolution de la politique éditoriale et de modération de ces très grandes plateformes et l'usage qui en fait par certains de leurs propriétaires n'en font plus de simples fournisseurs d'un service de la société de l'information qui ne serait pas responsable des informations transmises ou de l'accès fourni au sens de l'article 4 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 susmentionné ;

㉒ Considérant que par ces évolutions et face à l'inefficacité des actions mises en œuvre par certaines de ces très grandes plateformes pour évaluer et atténuer les risques systémiques sur les processus électoraux, celles-ci représentent une menace pour les droits fondamentaux des citoyens non-européens, la qualité du débat public et plus largement la souveraineté politique et démocratique des États membres de l'Union ;

㉓ Considérant l'adresse aux Français du président de la République le 5 mars 2025, dans laquelle il affirme que certains États, en tête desquels la Russie, cherchent à manipuler nos opinions par la diffusion de mensonges sur les réseaux sociaux.

㉔ Considérant qu'il est indispensable de mettre en œuvre des normes de sécurité dès la conception des systèmes régissant ces très grandes plateformes, afin de favoriser le respect des droits fondamentaux ;

㉕ 1. Appelle la Commission européenne à appliquer fermement et sans délai le règlement européen et ce faisant, à faire usage de l'intégralité des pouvoirs qui lui sont conférés par les articles 67 et suivants du règlement sur les marchés numériques, non pas seulement en matière d'investigation, mais aussi, en cas de non-conformité avérée d'une très grande plateforme numérique, pour contraindre et sanctionner ladite plateforme ;

㉖ 2. Appelle la Commission européenne à communiquer sans attendre aux parlements nationaux l'état d'avancement des différentes procédures formelles qu'elle a ouvertes à l'encontre des très grandes plateformes numériques et les résultats des procédures ouvertes depuis plus d'un an ;

- ⑳ 3. Invite la Commission européenne à un nouvel examen de la détermination de X comme contrôleur d'accès au marché numérique au titre du règlement sur les marchés numériques ;
- ㉑ 4. Se félicite de la décision de la Commission européenne prise le 17 janvier 2025 d'approfondir son enquête sur X afin d'obtenir du réseau social des informations supplémentaires sur la conception et le fonctionnement de ses algorithmes de recommandation mais souhaite une investigation rapide et transparente ;
- ㉒ 5. Appelle la Commission européenne à mettre en place un dispositif d'urgence harmonisé entre les États membres permettant de prendre des mesures provisoires en cas d'infractions graves aux règlements sur les services numériques risquant de conduire à une crise systémique ;
- ㉓ 6. Invite le Gouvernement à relayer ces appels auprès de la Commission et à œuvrer pour un usage déterminé par l'Union européenne de tous les outils réglementaires, économiques et diplomatiques à sa disposition pour contraindre les très grandes plateformes numériques au respect de ses règles dans l'espace numérique européen ;
- ㉔ 7. Appelle la Commission européenne à édicter toute décision visant à imposer aux propriétaires des plateformes numériques de céder les parts de capital qu'ils détiennent dans ces plateformes, correspondantes à leurs activités européennes, à un tiers n'étant pas placé en situation de conflit d'intérêts et, à défaut, à décider la suspension ou l'interdiction des plateformes dans l'Union européenne » ;
- ㉕ 8. Invite le Gouvernement à proposer à la Commission européenne l'édiction de toute décision utile visant à imposer aux propriétaires des plateformes numériques de céder les parts de capital qu'ils détiennent dans ces plateformes, correspondantes à leurs activités européennes, à un tiers n'étant pas placé en situation de conflit d'intérêts et, à défaut, à décider la suspension ou l'interdiction des plateformes dans l'Union européenne ;
- ㉖ 9. Appelle la Commission européenne à élaborer une stratégie de développement des plateformes et infrastructures numériques souveraines au sein de l'Union.

ANNEXES :

LISTE DES PERSONNES AUDITIONNÉES PAR LES RAPPORTEURS

- **La Quadrature du Net**
 - M. Bastien Le Querrec, juriste
- **Représentation Permanente de la France auprès de l'Union européenne**
 - M. Cyril Piquemal, représentant permanent adjoint
 - Mme Ségolène Milaire, conseillère politique industrielle et innovation
- **Viginum (Service de vigilance et protection contre les ingérences numériques étrangères)**
 - M. Marc-Antoine Brillant, chef de service
- **Experts**
 - M. David Chavalarias, mathématicien et directeur de recherche au CNRS et à l'EHESS
 - M. Romain Badouard, maître de conférences en sciences de l'information et de la communication à Paris II-Panthéon Assas
- **ARCOM (Autorité de régulation et de communication audiovisuelle et numérique)**
 - M. Martin Adjari, président
 - M. Alban de Nerveaux, directeur général
 - Mme Lucile Petit, directrice des plateformes en ligne
- **Commission européenne (Direction générale des réseaux de communication, du contenu et des technologies)**
 - M. Prabhat Agarwal, chef d'unité