

N° 881

SÉNAT

SESSION EXTRAORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 8 juillet 2026

RAPPORT D'INFORMATION

FAIT

au nom de la commission des affaires européennes (1)
*sur le **bouclier européen de la démocratie**,*

Par M. Didier MARIE et Mme Catherine MORIN-DESAILLY,

Sénateur et Sénatrice

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

SOMMAIRE

	<u>Pages</u>
L'ESSENTIEL.....	5
AVANT PROPOS.....	15
I. LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE : RAPPEL DU CONTEXTE DE SA MISE EN ŒUVRE ET PREMIER BILAN	19
A. LES DÉFIS STRUCTURELS MENAÇANT LES DÉMOCRATIES EUROPÉENNES AUXQUELS LE BOUCLIER TENTE D'APPORTER UNE RÉPONSE.....	19
B. COMMENT APPRÉCIER LA ROBUSTESSE DU BOUCLIER EUROPÉEN DE LA DÉMOCRATIE ?	23
C. UN BOUCLIER CRITIQUÉ DÈS SA PUBLICATION ET QUI RESTE MIS EN QUESTION AUJOURD'HUI	27
1. Dès sa publication, des critiques de plusieurs parties prenantes quant à la solidité du bouclier	27
2. La position du gouvernement français sur le bouclier européen de la démocratie	28
3. Un avis réservé de la commission spéciale du Parlement européen sur la portée effective du bouclier	30
4. Un bouclier en papier ?.....	33
II. UN BILAN D'ÉTAPE DÉCEVANT DE LA MISE EN ŒUVRE DU CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE.....	35
A. CARTOGRAPHIE DES INITIATIVES EUROPÉENNES DÉJÀ EXISTANTES.....	35
1. Le modèle français de VIGINUM, un exemple performant à répliquer dans l'Union européenne	36
a) Le mandat de VIGINUM.....	36
b) Des réalisations concrètes et opérationnelles	37
c) L'ambition du renforcement de la résilience de la société civile : l'Académie de la lutte contre les manipulations de l'information (LMI).....	39
2. Une diversité d'acteurs aux approches hétérogènes implantés sur le territoire européen	41
a) Le modèle suédois : l'Agence de défense psychologique	41
b) L'exemple du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO).....	42
c) Le Centre d'excellence pour la cybersécurité en coopération, adossé à l'OTAN..	43
d) Le centre d'excellence européen pour la lutte contre les menaces hybrides, une initiative commune de l'UE et de l'OTAN	44
B. DANS CET ENVIRONNEMENT DÉJÀ DENSE, QUELLE PLACE ET QUEL RÔLE POUR LE CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE ?	44
1. Le risque d'une désorganisation des initiatives sans une coopération stratégique	44
a) Une vigilance nécessaire dans l'association au centre de pays tiers	44
b) Quelle articulation avec le Nouveau pacte démocratique du Conseil de l'Europe ?	46
2. Une feuille de route encore peu lisible pour le Centre européen pour la résilience démocratique	48
3. Le Centre a-t-il abouti à des résultats tangibles à ce stade ?	50

C. TRANSFORMER L'ESSAI DU CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE : LA NÉCESSITÉ D'UN MANDAT CLAIR ET D'UN PORTAGE POLITIQUE FORT	52
III. PASSER D'UN BOUCLIER DE PAPIER À UN BOUCLIER D'ACIER : COMMENT RENFORCER LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE ?..	56
A. RENFORCER LE CADRE JURIDIQUE ET LES OBLIGATIONS INCOMBANT AUX GRANDES PLATEFORMES.....	56
B. FAUT-IL RENFORCER LA DIMENSION COERCITIVE DU BOUCLIER ?	61
C. CONTRIBUER À RÉTABLIR UNE HIÉRARCHIE DE L'INFORMATION	64
D. RENFORCER L'EFFICACITÉ DES MÉCANISMES D'ALERTE PRÉCOCE (<i>RAPID ALERT SYSTEM</i>) ET DES PROTOCOLES DE CRISE PRÉVUS PAR LE RÈGLEMENT SUR LES SERVICES NUMÉRIQUES (DSA)	69
E. AMÉLIORER LA LITTÉRATIE DES CITOYENS EN MATIÈRE NUMÉRIQUE	70
LISTE DES RECOMMANDATIONS.....	73
EXAMEN EN COMMISSION.....	77
LISTE DES PERSONNES ENTENDUES	87
LISTE DES CONTRIBUTIONS ÉCRITES.....	89
DÉPLACEMENT	91

L'ESSENTIEL

Le 12 novembre 2025, la Commission européenne a présenté, conjointement avec la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, une communication intitulée « **bouclier européen de la démocratie** ». Cette initiative entend apporter une réponse européenne coordonnée aux défis croissants que soulèvent la **désinformation** et les **autres tentatives de manipulations de l'information**, notamment en ligne.

L'espace public informationnel est aujourd'hui en effet articulé autour de l'activité de **quelques très grandes plateformes numériques**, dont les modèles économiques et les algorithmes, opaques, conduisent à **brouiller la frontière entre vraie et fausse information**.

Dans cet écosystème complexe, des puissances étrangères ou des entités privées malveillantes instrumentalisent les outils numériques pour conduire des activités d'ingérence. Or **les ingérences numériques étrangères (INE) vont croissant** ; elles s'inscrivent de plus en plus dans des **stratégies hybrides, numériques**, mêlant parfois d'autres leviers d'attaque ciblant les **infrastructures critiques** tels les câbles sous-marins, les ports, les aéroports ou encore les réseaux énergétiques. Ces stratégies hybrides exploitent largement les vulnérabilités numériques : utilisation de l'intelligence artificielle -IA- (hypertrucages ou *deepfakes*, contenus synthétiques, etc.), de comptes fictifs ou inauthentiques sur les réseaux sociaux et effet d'amplification algorithmique de contenus polarisants.

Les ingérences numériques étrangères **ciblent surtout de manière accrue les processus électoraux**, aux fins de déstabilisation des institutions démocratiques. Outre les exemples européens récents fortement médiatisés, telles les ingérences russes à l'occasion de l'élection présidentielle en Roumanie en 2024, la menace apparaît d'ores et déjà matérialisée en France, comme le démontre un récent rapport du service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM).

Dès lors, le bouclier européen de la démocratie apparaît comme une réponse bienvenue pour lutter contre les manipulations de l'information et les ingérences étrangères (FIMI) mais **la solidité de ce bouclier résiste mal à l'analyse**. La commission des affaires européennes formule donc **plusieurs recommandations pour le renforcer**.

LES PRINCIPALES RECOMMANDATIONS

1. **Renforcer par tous moyens la souveraineté numérique européenne**, laquelle est un vecteur intrinsèque de résilience démocratique.
2. **Doter le Centre européen pour la résilience démocratique** d'un mandat clair, lui permettant de coordonner le partage des bonnes pratiques entre États membres et avec les institutions de l'Union européenne, dans le respect des compétences des États membres et notamment de leurs capacités de détection et de riposte souveraines. Le doter d'une équipe compétente, d'un format adapté aux missions qui lui sont attribuées.
3. **Mettre à jour les lignes directrices** relatives à l'atténuation des risques systémiques menaçant les processus électoraux, adoptées sur la base de **l'article 35 du règlement sur les services numériques (DSA)**, en renforçant les exigences d'**encadrement des systèmes et algorithmes de recommandation, la lutte contre les comptes et contenus inauthentiques, la transparence publicitaire en période électorale**, le financement des contenus de manipulation de l'information, et des indicateurs quantitatifs sur la performance des outils mis en œuvre.
4. **Publier dans les meilleurs délais des lignes directrices sur les registres publicitaires**, prévues par **l'article 39 du règlement sur les services numériques (DSA)**, afin d'assurer la transparence des plateformes en la matière, y compris hors période électorale.
5. **Préciser, dans les lignes directrices relatives à l'application de l'article 39 du règlement sur les services numériques (DSA)**, les exigences en matière de **transparence des annonceurs** ainsi que les fonctionnalités qui devraient être mises à disposition dans le cadre des registres publicitaires et des interfaces de programmation d'application (APIs) des très grandes plateformes et des grands moteurs de recherche.
6. **Demander aux grandes plateformes numériques de ne pas modifier leurs algorithmes en période électorale** afin d'éviter tout soupçon de biais en faveur de certains partis politiques.

7. Sans attendre une révision du DSA, mettre en œuvre, au niveau de la Commission européenne, les moyens nécessaires pour **réaliser les enquêtes permettant d'attester le nombre d'utilisateurs réels de Telegram** afin qu'il soit requalifié comme très grande plateforme et incombe au contrôle direct de la Commission européenne.
8. Imposer aux très grandes plateformes de prendre en compte dans leurs algorithmes un objectif de **visibilité prioritaire** des contenus issus de médias **certifiés de la norme Journalism Trust Initiative (JTI)** ou d'une norme équivalente.
9. Intégrer dans le cadre de régulation européen du numérique des **mesures d'incitation à la publicité dans des médias fiables**, afin de soutenir le modèle économique d'une presse de qualité.
10. Engager une réflexion sur **l'utilisation par l'IA des contenus médiatiques pour aboutir à une solution permettant la juste rémunération des médias traditionnels** et la pérennité de leur modèle économique.

I. UN BOUCLIER EUROPÉEN DE LA DÉMOCRATIE NÉCESSAIRE MAIS FRAGILE

A. ALORS QUE LES DÉFIS STRUCTURELS MENAÇANT L'ESPACE INFORMATIONNEL EUROPÉEN VONT CROISSANT...

La **démocratie constitue le socle historique de l'Union européenne**, garantissant la paix, la sécurité, la prospérité économique et la cohésion sociale. Elle repose sur des valeurs et des principes fondamentaux : élections libres et équitables, médias indépendants, institutions solides et participation citoyenne.

Pourtant, dans un contexte marqué par les tensions géopolitiques, les conflits régionaux et les bouleversements technologiques, **les démocraties européennes font face à des pressions internes et externes croissantes, ciblant notamment les processus électoraux.**

4 **ingérences numériques étrangères (INE) ciblant spécifiquement les élections municipales françaises** des 15 et 22 mars 2026 ont été détectées et caractérisées par VIGINUM, dont deux sont attribuables à des modes opératoires informationnels pro-russes.

*Source : Rapport de VIGINUM, publié le 11 juin 2026,
« Protection du débat public contre les ingérences numériques étrangères durant les élections
municipales des 15 et 22 mars 2026 »*

Or l'écosystème informationnel européen est confronté à des défis majeurs : perte de hiérarchie de l'information par le truchement des algorithmes des grandes plateformes et grands moteurs de recherche en ligne, recul des médias traditionnels éditorialisés au profit d'autres sources d'information.

20 % **des Français, et 54 % des moins de 25 ans, s'informent désormais principalement par les outils d'IA.**

Source : Baromètre du numérique de l'Arcom (édition 2026)

B. ... LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE APPARAÎT À CE STADE FRAGILE

Prenant la forme d'une simple communication de la Commission européenne et du Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, le bouclier européen de la démocratie, en cours de mise en œuvre, se structure autour de trois « piliers » : **la préservation de l'intégrité de l'espace informationnel ; la protection des institutions, des processus électoraux et de la liberté des médias ; le renforcement de la résilience de la société et de l'engagement citoyen.**

Les trois « piliers » du bouclier européen de la démocratie

Préservation de l'intégrité de l'espace informationnel	Protection des institutions, des élections de la liberté des médias	Renforcement de la résilience de la société et de l'engagement citoyen
• Renforcement du code de conduite contre la désinformation et du réseau européen de vérificateurs de faits • Création d'une liste de critères communs pour guider les régulateurs nationaux des médias • Création d'un Centre européen pour la résilience démocratique coordonnant les moyens des États membres et de la Commission européenne face aux FIMI	• Coopération renforcée dans le cadre du Réseau européen de coopération électorale (ECNE) • Création d'un réseau européen d'influenceurs volontaires • Actualisation de la boîte à outils pour les élections issue du règlement sur les services numériques (DSA)¹ • Révision des directives sur les services de médias audiovisuels et sur le droit d'auteur	• Mesures d'éducation à la citoyenneté et aux médias, y compris hors milieu scolaire, <i>via</i> l'actualisation de lignes directrices • Publication d'un guide de l'UE sur la démocratie • Soutien aux technologies civiques européennes

¹ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

Or ce bouclier **s'appuie pour l'essentiel sur des structures et des textes existants**. Il ne consiste donc pas tant en la mise en place de nouvelles mesures qu'en l'activation de dispositifs déjà en place, sans que des budgets supplémentaires soient nécessairement alloués.

« La plupart de ces mesures consistent en des engagements de la Commission européenne visant à renforcer les structures volontaires de coordination et de partage d'informations, à élaborer des lignes directrices non contraignantes ou à renforcer la législation existante, sans fournir beaucoup de détails sur la manière dont elle compte les mettre en œuvre ni sur le calendrier prévu. »

Source : Note d'orientation « Le « bouclier de la démocratie européenne » : masquer les failles », Luise Quaritsch, Hertie School, Centre Jacques Delors, 12 décembre 2025

Cet avis est d'ailleurs partagé par la **commission spéciale du Parlement européen sur le bouclier européen de la démocratie, qui a adopté le 23 juin 2026¹ un rapport mitigé, plaidant pour son renforcement**.

II. UN BILAN D'ÉTAPE DÉCEVANT DE LA MISE EN ŒUVRE DU CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE

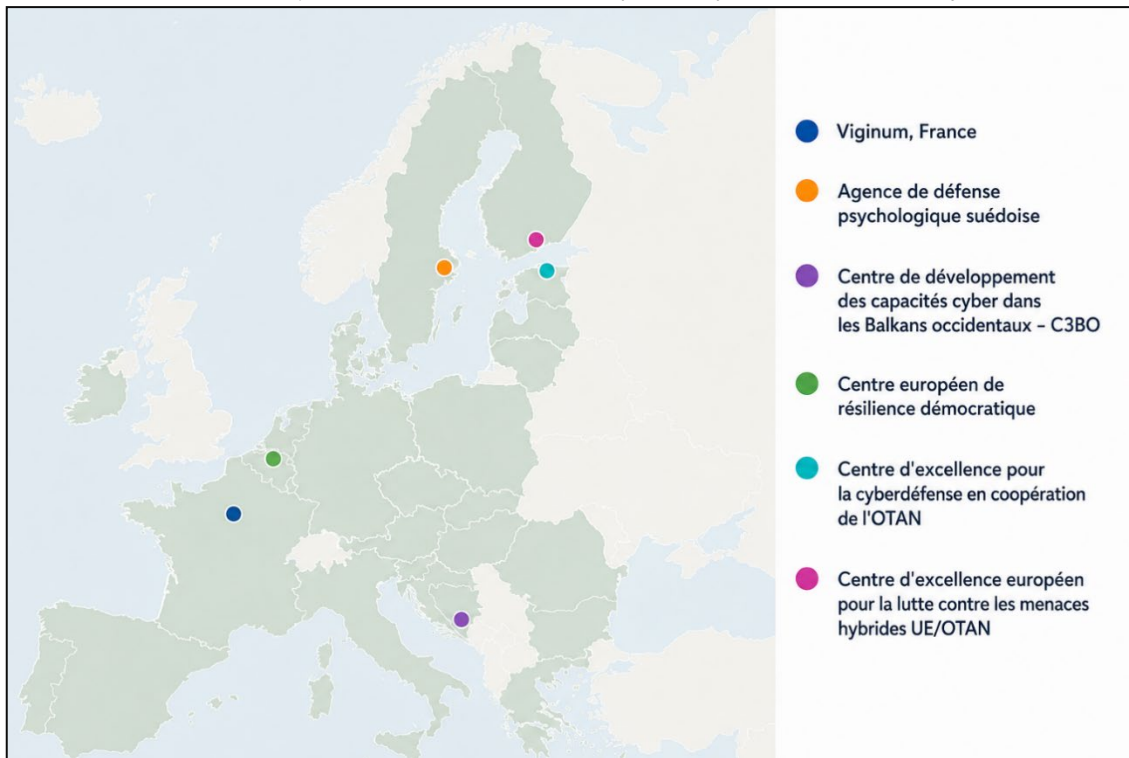
De manière pratique, le bouclier est **essentiellement axé sur la création d'une nouvelle structure - le Centre européen pour la résilience démocratique**, dont la feuille de route reste imprécise et le degré de mise en œuvre près de six mois après sa création, incertain.

A. PLUSIEURS INITIATIVES EUROPÉENNES DÉJÀ EXISTANTES

Alors qu'à travers l'Europe existent déjà différentes initiatives pour renforcer les capacités de résilience démocratie, soit au niveau national (**VIGINUM en France, l'Agence de défense psychologique en Suède, s'agissant des plus avancées**), soit dans une logique de coopération internationale (Centre d'excellence pour la cyberdéfense en coopération adossé à l'OTAN, Centre de développement des capacités cyber dans les Balkans occidentaux ou C3BO...), le Centre européen pour la résilience démocratique doit pouvoir jouer un rôle de coordination, sans nuire à la capacité des États membres.

¹ Conclusions et recommandations de la commission spéciale sur le « bouclier européen de la démocratie » (2025/2069(INI)), Tomas Tobé, 23 juin 2026.

Centres européens de résilience et de défense informationnelle et cyber



Source : Infographie générée avec l'aide de l'IA

B. LA NÉCESSITÉ D'UN MANDAT CLAIR ET D'UN PORTAGE POLITIQUE FORT

Pour ne pas risquer de devenir une autre plateforme ou un centre parmi d'autres, ce qui aggraverait la fragmentation des efforts européens et réduirait l'efficacité des outils existants, ce centre a besoin d'**un mandat clair, axé sur la seule coordination des initiatives nationales et la coopération en vue du partage des bonnes pratiques et du renforcement des capacités des pays les moins avancés en la matière.**

Aujourd'hui hébergé au sein de la direction générale pour la communication (DG COMM) de la Commission européenne et doté de ressources humaines incertaines (il **serait composé de 5 à 6 personnes** dont on ne connaîtrait à ce stade pas l'organigramme précis), le Centre – inauguré officiellement le 24 février 2026 – ne bénéficie pas d'une feuille de route claire et n'a pas encore abouti à des résultats tangibles.

Il convient donc de le doter, d'une part, d'une **équipe compétente**, d'un format adapté aux missions qui lui sont attribuées, et d'autre part, d'un **mandat clair**, lui permettant de coordonner le partage des bonnes pratiques entre États membres et avec les institutions de l'Union européenne, dans le respect des compétences des États membres et notamment de leurs capacités de détection et de riposte souveraines.

III. PASSER D'UN BOUCLIER DE PAPIER À UN BOUCLIER D'ACIER : COMMENT RENFORCER LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE ?

A. RENFORCER LE CADRE JURIDIQUE ET LES OBLIGATIONS INCOMBANT AUX GRANDES PLATEFORMES NUMÉRIQUES

Concernant la lutte contre les ingérences numériques étrangères, notamment pendant les périodes électorales, les **plateformes en ligne jouent désormais un rôle majeur dans les mécanismes d'information et de formation de l'opinion publique.**

Dès lors, le renforcement du bouclier européen de la démocratie passe également par **l'application stricte et le renforcement du cadre réglementaire des grandes plateformes numériques et de l'IA**, notamment au titre du règlement sur les services numériques (DSA) de 2022¹, qui devrait être soumis à révision fin 2027.

Dans ce cadre, le rapport fait plusieurs propositions. Il invite notamment la Commission européenne à publier ou **mettre à jour les lignes directrices prévues au titre du DSA relativement à l'atténuation des risques systémiques menaçant les processus électoraux ou encore concernant les registres publicitaires.**

Considérant que la transparence des plateformes en matière publicitaire, mais aussi de manière générale, leur responsabilité au titre des contenus qu'elle héberge, doit être reconnue, le rapport appelle la Commission européenne à appliquer sans trembler, voire à renforcer, le cadre juridique ambitieux que l'UE a développé en matière numérique, y compris par l'application des sanctions prévues au titre du DSA dès qu'elles sont nécessaires pour préserver l'espace informationnel numérique.

B. CONTRIBUER À RÉTABLIR UNE HIÉRARCHIE DE L'INFORMATION

La fiabilité de l'information est au cœur des questionnements sur la résilience démocratique. En effet, pour pouvoir prendre des décisions éclairées, les citoyens doivent pouvoir se reposer sur des informations vérifiées, sans pour autant porter atteinte à la liberté d'expression.

¹ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

Le rapport fait plusieurs propositions pour renforcer les médias d'information, notamment locaux, à travers les divers instruments envisagés au sein du prochain cadre financier pluriannuel, afin de lutter contre les déserts d'information et la désinformation. Il appelle également à imposer aux grandes plateformes numériques des obligations pour **garantir la visibilité de contenus journalistiques qualifiés** ou encore **pour encourager les annonceurs à insérer leurs publicités dans des médias éditorialisés, afin de soutenir leur modèle économique.**

Enfin, outre l'encouragement des médias paneuropéens, le rapport souligne que, pour améliorer la résilience démocratique, **doit être renforcée la littératie du numérique pour les citoyens européens** – c'est à dire leur capacité à lire, comprendre et traiter l'information en ligne, sur les réseaux sociaux et l'information produite par l'IA –, afin de repérer plus facilement les contenus trompeurs ou inauthentiques.

AVANT PROPOS

Face à des défis nombreux et renouvelés dans un contexte géopolitique incertain, **la Commission européenne multiplie les initiatives en lien avec les orientations annoncées par sa présidente, Ursula von der Leyen¹, en matière de protection de la démocratie et des valeurs de l'Union européenne (UE), notamment au travers du renforcement de sa souveraineté numérique vis-à-vis des tentatives d'ingérences étrangères** et des nouveaux enjeux soulevés par le développement de l'intelligence artificielle (IA).

En matière de régulation du numérique, de lutte contre les risques *cyber* et d'accompagnement législatif et stratégique des nouveaux usages numériques dans la société européenne, les **propositions récemment adoptées ou en cours d'examen sont nombreuses**.

Afin d'objectiver ce phénomène d'inflation, on peut citer, entre autres, depuis 2022, les initiatives suivantes :

- **en matière numérique** : le règlement sur les services numériques (DSA) de 2022² qui encadre les activités des plateformes, en particulier celles des GAFAM, et le règlement sur les marchés numériques (DMA), de 2022³ également, qui prévoit des obligations et interdictions opposables aux géants du numérique dans l'objectif de lutter contre les pratiques anticoncurrentielles dans ce secteur ;

- **en matière de cybersécurité** : le règlement sur la résilience cyber de 2022⁴ et le règlement sur la cyber-solidarité de 2023⁵, destinés à améliorer la préparation, la détection et la réaction aux incidents de cybersécurité dans l'ensemble de l'UE. En complément, le projet de refonte du règlement sur la cybersécurité est en cours de discussion⁶ ;

¹ « Le choix de l'Europe », orientations pour la prochaine Commission européenne, 18 juillet 2024.

² Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

³ Règlement (UE) 2022/1925 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques).

⁴ Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

⁵ Règlement (UE) 2025/38 visant à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir (règlement sur la cybersolidarité).

⁶ Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2) – COM(2026) 11 et proposition de directive du Parlement européen et du conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2] – COM(2026) 13.

- **en matière d'IA** : le règlement sur l'IA de 2024¹, lui-même en cours d'amendement au travers de l'examen de l'omnibus numérique, avec son train de mesures sur l'IA², lequel est également composé d'un volet sur les données en cours d'examen³ ;

- incidemment, **en matière de télécommunications** : la Commission européenne a présenté une proposition de règlement sur les réseaux numériques⁴, destinée à remplacer le code des communications électroniques de l'Union européenne de 2018⁵ ;

- enfin, **de manière générale, concernant l'industrie numérique** : le règlement sur les infrastructures gigabit de 2024⁶ et le règlement européen sur les semi-conducteurs (*Chips Act*) de 2023⁷. Un nouveau paquet de mesures vient d'être proposé par la Commission européenne pour renforcer la souveraineté technologique de l'Europe. Présenté le 3 juin 2026, ce paquet comprend deux propositions législatives : une proposition de règlement sur les semi-conducteurs 2.0 (dit « *Chips Act 2.0* »⁸) et une proposition de règlement sur le développement de l'informatique en nuage et de l'intelligence artificielle⁹. Il comprend aussi deux communications : la stratégie de l'Union européenne en faveur de l'*open source*¹⁰ et une feuille de

¹ Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle).

² Proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2024/1689 et (UE) 2018/1139 en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l'intelligence artificielle.

³ Proposition de règlement du Parlement européen et du Conseil COM(2025)837 modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024, dite « règlement omnibus numérique ».

⁴ Proposition de règlement du Parlement européen et du Conseil relatif aux réseaux numériques, modifiant le règlement (UE) 2015/2120, la directive 2002/58/CE et la décision n° 676/2002/CE et abrogeant le règlement (UE) 2018/1971, la directive (UE) 2018/1972 et la décision n° 243/2012/UE (règlement sur les réseaux numériques) – COM(2026)16.

⁵ Directive (UE) 2018/1972 établissant le code des communications électroniques européen.

⁶ Règlement (UE) 2024/1309 du Parlement européen et du Conseil du 29 avril 2024 relatif à des mesures visant à réduire le coût du déploiement de réseaux gigabit de communications électroniques, modifiant le règlement (UE) 2015/2120 et abrogeant la directive 2014/61/UE (règlement sur les infrastructures gigabit).

⁷ Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et modifiant le règlement (UE) 2021/694 (règlement sur les puces).

⁸ Proposition de règlement du Parlement européen et du Conseil relatif à un cadre de mesures visant à renforcer l'écosystème des semi-conducteurs de l'Union, abrogeant le règlement (UE) 2023/1781 (*Chips Act 2.0*, COM/2026/504 final, non encore traduit en français).

⁹ Proposition de règlement du Parlement européen et du Conseil établissant un cadre de mesures pour le renforcement de l'écosystème européen du cloud et de l'IA (loi sur le développement du cloud et de l'IA, COM/2026/502 final, non encore traduit en français).

¹⁰ Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la souveraineté technologique européenne, accompagnée d'une stratégie de l'UE en matière de logiciels libres, COM/2026/503 final, en date du 3 juin 2026, non encore traduite en français.

route stratégique pour la numérisation et l'intelligence artificielle dans le secteur de l'énergie¹.

C'est dans ce contexte foisonnant que s'inscrit la création du bouclier européen de la démocratie, présenté le 12 novembre 2025 par la Commission européenne et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, dans le cadre d'une communication conjointe².

L'ensemble des actes législatifs ou propositions d'actes précités entend en effet **participer à la logique souhaitée par les institutions européennes d'une transformation numérique qui soit à la fois vecteur de croissance, mais également conforme aux valeurs européennes – dont la démocratie est un pilier structurant – et à l'impératif stratégique de résilience et de sécurité**. Cette logique, qui croise mesures de régulation économique et déclarations de principes sur les valeurs européennes, se retrouve notamment dans la récente feuille de route « Une Europe, un marché³ », cosignée par le Parlement européen, le Conseil de l'Union européenne et la Commission européenne.

Fidèle à cette logique, le bouclier européen de la démocratie, en cours de mise en œuvre, se structure autour de trois « piliers » :

1. la préservation de l'intégrité de l'espace informationnel, avec notamment le renforcement du code de conduite contre la désinformation et du réseau européen de vérificateurs de faits, la création d'une liste de critères communs pour guider les régulateurs nationaux des médias et, surtout, **la mise en place d'un Centre européen pour la résilience démocratique** qui coordonnerait les moyens des États membres et de la Commission européenne face aux ingérences et aux manipulations de l'informations étrangères ;

2. la protection des institutions, des processus électoraux et de la liberté des médias, à travers une coopération renforcée dans le cadre du réseau européen de coopération électorale (ECNE), la constitution d'un réseau européen d'influenceurs volontaires, l'actualisation de la boîte à outils pour les élections issue du règlement sur les services numériques (DSA)⁴ ainsi qu'une évaluation et **une révision des directives sur les services de médias audiovisuels et sur le droit d'auteur dans le marché unique numérique** ;

¹ Communication de la Commission au Parlement européen, au Conseil, au Comité Économique et Social Européen et au Comité des Régions « Feuille de route stratégique pour la transition numérique et l'IA dans le secteur de l'énergie », COM(2026) 501 final, en date du 3 juin 2026.

² Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions JOIN/2025/791 final intitulée « bouclier européen de la démocratie : renforcer la position de démocraties fortes et résilientes », 12 novembre 2025.

³ Feuille de route « Une Europe, un marché » du Parlement européen, du Conseil de l'Union européenne et de la Commission européenne, 23 avril 2026, 8473/26.

⁴ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

3. le renforcement de la résilience de la société et de l'engagement citoyen, qui s'appuierait sur des **mesures d'éducation à la citoyenneté et aux médias**, y compris hors milieu scolaire, *via* l'actualisation de lignes directrices, la publication d'un guide de l'UE sur la démocratie, un soutien aux technologies civiques européennes, etc.

Pour autant, selon la communication conjointe précitée, **le bouclier européen de la démocratie s'appuie pour l'essentiel sur des structures et des textes existants**. Il ne consiste donc pas tant dans la mise en place de nouvelles mesures que dans l'activation de dispositifs déjà en place, sans que des budgets supplémentaires ne soient nécessairement alloués.

Dans sa résolution européenne sur le programme de travail de la Commission européenne pour l'année 2026¹, le Sénat a affirmé son **soutien à la mise en œuvre de ce bouclier de la démocratie, jugé utile et nécessaire, tout en appelant à le renforcer**.

En conséquence, s'inscrivant dans le cadre du programme de contrôle de la commission des affaires européennes du Sénat au titre de l'année 2026, le présent rapport d'information entend **dresser un bilan de la mise en œuvre en cours de ce bouclier**, afin d'apprécier s'il se traduit bien par des mesures concrètes et des résultats mesurables, au bénéfice du renforcement de la résilience de la société civile et d'un écosystème médiatique de qualité.

Les rapporteurs estiment que **la lutte contre les ingérences étrangères doit relever d'un équilibre entre subsidiarité et interopérabilité des capacités et réponses européennes**. La France s'est en effet dotée de d'un cadre national particulièrement abouti, avec la création du **service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM)**, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN). Il s'agit de la structure la plus avancée de l'Union européenne en la matière, notamment dans sa composante de vigilance du secteur numérique, véritable clé de la lutte contre la désinformation et les ingérences étrangères. Les rapporteurs ont notamment souhaité **s'assurer que les bonnes pratiques françaises développées par VIGINUM sont correctement prises en compte** pour la mise en œuvre du Centre européen pour la résilience démocratique, seule véritable nouveauté annoncée par la Commission européenne et la haute représentante, et que ce centre contribue de manière concrète à l'amélioration des capacités opérationnelles des États membres.

¹ *Résolution européenne du Sénat n° 42 (2025-2026) du 23 janvier 2026.*

I. LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE : RAPPEL DU CONTEXTE DE SA MISE EN ŒUVRE ET PREMIER BILAN

A. LES DÉFIS STRUCTURELS MENAÇANT LES DÉMOCRATIES EUROPÉENNES AUXQUELS LE BOUCLIER TENTE D'APPORTER UNE RÉPONSE

La **démocratie constitue le socle historique de l'Union européenne**, garantissant la paix, la sécurité, la prospérité économique et la cohésion sociale. Elle repose sur des valeurs et des principes fondamentaux : élections libres et équitables, médias indépendants, institutions solides et participation citoyenne.

Pourtant, dans un contexte marqué par les tensions géopolitiques, les conflits régionaux et les bouleversements technologiques, **les démocraties européennes font face à des pressions internes et externes croissantes**. Divers acteurs étatiques ou privés, au premier rang desquels les régimes autoritaires tels que la Russie, déploient des stratégies hybrides pour affaiblir les démocraties, à travers la manipulation de l'information, notamment en ligne, mais aussi des tentatives d'ingérence (on parle communément de **FIMI** pour « *foreign information manipulations and interference* » ou, en français, de **MIIE** pour « manipulation de l'information et ingérence étrangères »).

Ces stratégies hybrides exploitent les vulnérabilités numériques : utilisation de l'IA (hypertrucages ou *deepfakes*, contenus synthétiques, *etc.*), de comptes fictifs ou inauthentiques sur les réseaux sociaux et de l'amplification algorithmique de contenus polarisants.

Elles **ciblent également de manière accrue les processus électoraux**, aux fins de déstabilisation des institutions démocratiques. Outre les exemples européens récents fortement médiatisés, telles les ingérences russes à l'occasion de l'élection présidentielle en Roumanie en 2024, ou plus récemment lors des élections législatives moldaves en septembre 2025, la menace apparaît d'ores-et-déjà matérialisée en France.

La notion de mode opératoires informationnels (MOI), développé par VIGINUM

Il s'agit d'un concept développé par VIGINUM pour décrire spécifiquement un ensemble de comportements, d'outils, de tactiques, techniques et procédures (TTP) et de ressources adverses présumés liés au même acteur malveillant ou groupe d'acteurs malveillants.

Un MOI doit réunir deux conditions cumulatives : la clandestinité et des efforts de coordination pour éviter que ne puisse lui être imputée son activité.

La clandestinité désigne les opérations techniques de dissimulation de l'acteur malveillant, afin d'éviter l'imputation.

La coordination correspond au recours à des infrastructures numériques différentes, présumées administrées par le même acteur, travaillant pour le même commanditaire.

Ce concept est la clé de voûte des méthodologies d'analyse mises en œuvre par VIGINUM pour caractériser les ingérences numériques étrangères en ligne. Selon VIGINUM, *« l'approche par les modes opératoires informationnels permet non seulement d'avoir une appréhension technique et donc objective de la menace, mais aussi de mieux détecter de nouvelles opérations informationnelles »*.

Ainsi, **quatre ingérences numériques étrangères (INE) ciblant spécifiquement les élections municipales françaises des 15 et 22 mars 2026 ont été détectées et caractérisées par VIGINUM¹**. Deux de ces ingérences numériques étrangères sont attribuables à des modes opératoires informationnels pro-russes (Storm-1516, CopyCop, Storm-1679 et Matriochka), pour lesquels VIGINUM précise qu'ils sont connus et ont déjà mené des activités numériques malveillantes contre la France par le passé. Deux nouvelles INE ont été caractérisées par VIGINUM :

- la première, à finalité lucrative, a été conduite au moyen d'un nouveau mode opératoire informationnel impliquant **un acteur non-étatique localisé au Vietnam**. Elle s'est articulée autour de plus de 100 pages Facebook inauthentiques et 73 sites internet francophones impliqués dans la **diffusion de contenus polarisants autour des enjeux électoraux**. Selon VIGINUM, la finalité lucrative repose sur la monétisation publicitaire des actifs numériques administrés dans le cadre de cette ingérence numérique étrangère, notamment les sites internet promus par les pages Facebook, qui se présentent comme des blogs d'actualités ou des médias d'information ;

¹ Rapport de VIGINUM, publié le 11 juin 2026, « Protection du débat public contre les ingérences numériques étrangères durant les élections municipales des 15 et 22 mars 2026 ».

- la seconde, impliquant un **acteur non-étatique localisé en Israël, a ciblé plusieurs candidats du parti La France Insoumise (LFI)**. Le nouveau mode opératoire informationnel utilisé consistait en un réseau de plusieurs sites web et de comptes de réseaux sociaux inauthentiques, combinant des fausses accusations (par exemple de pédophilie) de certains candidats et des tentatives de polarisation du débat public en ligne, en particulier en accusant le parti LFI de communautarisme musulman.

Si le volume et l'effet potentiel des campagnes d'ingérence numérique étrangères détectées par VIGINUM doivent être relativisés s'agissant des élections municipales de 2026, elles démontrent toutefois la tendance à l'accroissement des menaces numériques ainsi induites et de leurs conséquences potentielles pour les institutions démocratiques, auxquelles s'ajoutent des défis structurels en France, comme dans d'autres pays européens : la montée des extrémismes et la polarisation de la société, ainsi que l'érosion de la confiance envers les institutions démocratiques.

En complément, la **transformation numérique de l'espace public modifie les dynamiques du débat démocratique et expose les citoyens à un risque accru de « bulles informationnelles »** ou « bulles de filtrage », de surcroît dans un contexte de fragilisation des médias indépendants et traditionnels, notamment sous l'effet de la domination des plateformes numériques sur les revenus publicitaires et du développement des IA génératives.

La notion de « bulle informationnelle »

Issue originellement de l'ouvrage *The Filter Bubble : What The Internet is Hiding from You* (Eli Pariser, Penguin Press, non traduit), la notion de « bulle informationnelle » ou « bulle de filtrage » désigne l'enfermement intellectuel d'un citoyen qui, lorsqu'il utilise des services internet ou réseaux sociaux, se voit proposer de manière automatique des contenus conformes à ses préférences, par le biais des algorithmes exploitant des biais cognitifs usuellement reconnus par les sciences sociales et la micro-économie en matière de recueil d'information, tels les biais de renforcement et de sélection.

Du risque induit par les « bulles informationnelles » pour la polarisation de l'information, les tentatives d'ingérences numériques étrangères voire l'amplification des radicalités en ligne, découle **une nécessité de formation des citoyens, notamment les plus jeunes et les plus fragiles, aux usagers numériques, aux médias et à l'information.**

Concernant l'identification et la mesure des risques et menaces qui pèsent sur l'espace informationnel français, les rapporteurs renvoient **aux travaux en cours de la mission d'information sur la régulation de l'information dans l'espace numérique, intitulée « les zones grises de l'information », engagée par la commission de la culture, de l'éducation, de la communication et du sport**, dont les rapporteurs sont Mme Agnès Evren, M. Laurent Lafon et Mme Sylvie Robert¹.

Dans le cadre de la communication sur le bouclier européen de la démocratie, un Eurobaromètre spécial intitulé « protéger et promouvoir la démocratie »² a été publié pour objectiver ce défi. Selon ce sondage, **près de trois Européens sur dix (28 %) disent se sentir exposés quotidiennement à la désinformation**, 24 % considèrent qu'ils le sont au moins une fois par semaine.

Les systèmes éducatifs et la vérification indépendante des faits sont considérés comme les moyens les plus efficaces pour aider les citoyens à lutter contre la désinformation et la manipulation de l'information (44 % des répondants).

Viennent ensuite la vérification des faits assurée par des organisations indépendantes et fiables (41 %) et les campagnes de sensibilisation du public visant à aider les citoyens à identifier la désinformation et la manipulation de l'information (40 %).

Selon ce même Eurobaromètre, les répondants européens dressent **un lien fort et négatif entre désinformation et risques pour des élections libres**. Les personnes interrogées dans l'ensemble des pays membres s'inquiètent notamment que les électeurs fondent leurs décisions sur de la désinformation (79 %), que des cyberattaques influencent les élections (71 %) et que des pays étrangers influencent les élections (70 %).

Sur le principe, les rapporteurs partagent les constats et l'analyse de la présidente de la Commission européenne, Mme Ursula von der Leyen, laquelle a souligné que *« la démocratie est le fondement de notre liberté, de notre prospérité et de notre sécurité. Le bouclier européen de la démocratie renforcera les éléments essentiels qui permettent aux citoyens de vivre quotidiennement nos valeurs démocratiques communes, à savoir la liberté d'expression, l'indépendance des médias, la résilience des institutions et le dynamisme de la société civile. Il s'agit de la force de l'Europe, et nous devons accroître notre capacité collective à la protéger à tout moment³. »*

¹ Voir : <https://www.senat.fr/travaux-parlementaires/commissions/commission-de-la-culture-de-l-education-et-de-la-communication/contrôle-en-clair/les-zones-grises-de-l-information.html>

² Eurobaromètre spécial n° 568, mai 2025.

³ Discours à l'occasion de la présentation du Bouclier européen de la démocratie, le 12 novembre 2025.

B. COMMENT APPRÉCIER LA ROBUSTESSE DU BOUCLIER EUROPÉEN DE LA DÉMOCRATIE ?

Face aux risques de déstabilisation de l'espace informationnel européen, l'Union européenne a entendu mettre en place un cadre politique et juridique pour renforcer la « résilience démocratique », notamment par le biais :

- du **plan d'action pour la démocratie européenne** de décembre 2020¹ ;

- du **train de mesures intitulé « défense de la démocratie »**, présenté par la Commission européenne le 12 décembre 2023, dont l'élément central consiste en une proposition de directive sur les activités de représentation d'intérêts menées pour le compte de pays tiers². Ce paquet comprend également une recommandation relative à des processus électoraux inclusifs et résilients dans l'Union, au renforcement du caractère européen des élections au Parlement européen et à une meilleure garantie de leur bon déroulement³, ainsi qu'une recommandation relative à la promotion de l'implication des citoyens et des organisations de la société civile dans les processus d'élaboration des politiques publiques et de leur participation effective à ces processus⁴.

Le bouclier européen de la démocratie, présenté dans le cadre d'une communication de la Commission européenne du 12 novembre 2025⁵, s'inscrit dans cette continuité. Il vise à **renforcer la résilience démocratique via trois axes prioritaires** :

- renforcer la conscience situationnelle et la capacité de réponse pour protéger l'intégrité de l'espace informationnel ;
- consolider les institutions démocratiques, les élections libres et les médias indépendants ;
- stimuler la résilience sociétale et l'engagement citoyen.

¹ Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur le plan d'action pour la démocratie européenne, 3 décembre 2020, COM(2020) 790 final.

² Proposition de directive du Parlement européen et du Conseil établissant des exigences harmonisées dans le marché intérieur en matière de transparence de la représentation d'intérêts exercée pour le compte de pays tiers et modifiant la directive (UE) 2019/1937, COM/2023/637 final.

³ Recommandation (UE) 2023/2829 de la Commission du 12 décembre 2023 relative à des processus électoraux inclusifs et résilients dans l'Union, au renforcement du caractère européen des élections au Parlement européen et à une meilleure garantie de leur bon déroulement.

⁴ Recommandation de la Commission relative à la promotion de l'engagement et de la participation effective des citoyens et des organisations de la société civile aux processus d'élaboration des politiques publiques, C/2023/8627 final.

⁵ Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions JOIN/2025/791 final intitulée « bouclier européen de la démocratie : renforcer la position de démocraties fortes et résilientes », 12 novembre 2025.

Le bouclier européen de la démocratie est décrit par la Commission européenne comme « une série de mesures concrètes destinées à renforcer la position de démocraties fortes et résilientes et à protéger et promouvoir ces dernières dans l'ensemble de l'UE¹ ». Il propose ainsi une **cinquantaine de mesures réparties selon ces trois axes prioritaires**.

Or « la plupart de ces mesures consistent en des engagements de la Commission européenne visant à renforcer les structures volontaires de coordination et de partage d'informations, à élaborer des lignes directrices non contraignantes ou à renforcer la législation existante, sans fournir beaucoup de détails sur la manière dont elle compte les mettre en œuvre ni sur le calendrier prévu », comme le souligne une analyse de la *Hertie School* du Centre Jacques Delors², dès décembre 2025.

¹ Communiqué de presse de la Commission européenne, « Le bouclier européen de la démocratie et la stratégie de l'UE en faveur de la société civile ouvrent la voie à des démocraties plus fortes et plus résilientes », Bruxelles, 12 novembre 2025.

² Note d'orientation « Le « bouclier de la démocratie européenne » : masquer les failles », Luise Quaritsch, Hertie School, Centre Jacques Delors, 12 décembre 2025.

LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE : APERÇU DES MESURES REGROUPÉES PAR TYPE D'ACTION



À la lecture de l'infographie issue de la note d'orientation sur le bouclier européen de la démocratie de la Hertie School, Centre Jacques Delors, on note que **la création du Centre européen pour la résilience démocratique est en réalité la seule mesure concrète**. Hébergé au sein de la Commission européenne, dans sa direction générale chargée de la Communication (DG COMM), ce centre a pour ambition de rassembler l'expertise et les ressources de l'UE et des États membres afin « d'accroître la capacité collective à anticiper les menaces, à les détecter et à y réagir et de renforcer la résilience démocratique »¹.

Les rapporteurs considèrent donc à ce stade que **l'appréciation de la robustesse du bouclier passe essentiellement par l'évaluation des modalités de mise en œuvre de ce centre**, au travers de la feuille de route qui lui a été conférée dans le cadre de la communication conjointe du 12 novembre 2025 précitée.

C. UN BOUCLIER CRITIQUÉ DÈS SA PUBLICATION ET QUI RESTE MIS EN QUESTION AUJOURD'HUI

1. Dès sa publication, des critiques de plusieurs parties prenantes quant à la solidité du bouclier

Deux jours avant la publication du bouclier européen de la démocratie, **Reporters sans frontières (RSF) et l'Union européenne de radio-télévision (UER) ont appelé, dans une lettre ouverte adressée aux institutions européennes², à garantir un accès effectif à l'information fiable pour tous les citoyens, quels que soient les services que ceux-ci utilisent pour s'informer**. RSF et l'UER ont considéré que le bouclier n'était « qu'une première étape et devait déboucher sur des propositions législatives » visant notamment à exiger des algorithmes des réseaux sociaux qu'ils accentuent la visibilité des contenus issus de sources fiables d'information par défaut, ainsi qu'à réguler les services reposant sur l'intelligence artificielle de façon à ce qu'ils répondent à des exigences minimales en termes de pluralisme et d'intégrité de l'information.

Arguant que « les citoyens ne peuvent pas prendre de décisions éclairées ni participer à la vie démocratique sans avoir accès à des sources d'information fiables, indépendantes et adaptées au contexte local », RSF a ainsi réitéré sa demande aux plateformes d'« assurer un accès effectif » aux médias fiables.

¹ Communiqué de presse de la Commission européenne, « Le bouclier européen de la démocratie et la stratégie de l'UE en faveur de la société civile ouvrent la voie à des démocraties plus fortes et plus résilientes », Bruxelles, 12 novembre 2025.

² Lettre ouverte « Pas de faits ? Pas de liberté. La démocratie repose sur l'accès à des informations fiables », Thibaut Bruttin, directeur général de Reporters sans frontières (RSF) et Noel Curran, directeur général de l'Union européenne de radio-télévision (UER), 10 novembre 2025.

Partageant la préoccupation de RSF de « *préserver l'intégrité de l'information et la confiance à l'ère de l'IA* », les rapporteurs estiment ainsi **que le lien entre souveraineté numérique, réglementation des grandes plateformes, régulation de l'IA et intégrité informationnelle est fondamental et qu'il est insuffisamment pris en compte dans la communication conjointe sur le bouclier européen de la démocratie.**

D'autres associations, groupes d'influence (lobbies) ou groupes de presse ont également fait part de réserves quant à la portée effective attendue du bouclier européen de la démocratie.

Par exemple, le groupe d'influence européen de tendance progressiste *News Media Europe* a appelé à « un bouclier européen de la démocratie (plus) solide ». Dans un communiqué de presse, en date du 12 novembre 2025, il souligne que « les solutions proposées sont globalement satisfaisantes, mais doivent se montrer plus ambitieuses. L'UE doit saisir cette occasion pour tirer parti du pouvoir des marchés publicitaires et promouvoir les investissements dans des médias responsables, plutôt que de laisser des milliards d'euros de recettes publicitaires finir entre les mains de plateformes technologiques étrangères, qui les utilisent pour diffuser de la désinformation et d'autres types de contenus préjudiciables et illégaux. » *News Media Europe* demande ainsi à la Commission européenne de **soutenir le fléchage des publicités vers les « médias responsables », par voie réglementaire, en utilisant comme véhicule juridique la future proposition de règlement sur l'équité numérique (Digital Fairness Act - DFA)**, qui devrait être présentée à l'automne 2026 par la Commission européenne.

De leur côté, les chaînes de télévisions privées, représentées par le groupe d'influence ACT, appellent également à des actions « tangibles » pour assurer le succès du bouclier européen de la démocratie, en particulier, un « *soutien à un marché publicitaire qui incite véritablement les médias à investir dans un journalisme de qualité et dans des contenus culturels* ».

2. La position du gouvernement français sur le bouclier européen de la démocratie

Dans ses réponses à un questionnaire adressé par les rapporteurs, reçues le 23 juin 2026, **le secrétariat général des affaires européennes (SGAE) rappelle que la France a salué l'initiative du bouclier européen de la démocratie, qui permettrait de doter les États membres d'une approche et d'outils communs permettant d'identifier les menaces portant sur les phénomènes démocratiques.** En effet, le SGAE souligne que « la protection de l'espace informationnel contre les ingérences numériques étrangères constitue un enjeu majeur pour les autorités françaises, notamment lors des périodes pré-électorales et électorales ».

En amont de la publication du bouclier, les autorités françaises avaient dès lors identifié trois objectifs majeurs :

- renforcer la résilience des sociétés européennes en favorisant l'éducation aux médias et le soutien à une information plurielle, fiable et de qualité ;
- garantir l'intégrité des processus démocratiques ;
- renforcer les capacités de détection et de réponse des États membres face aux manipulations de l'information.

Dans le cadre des échanges avec la Commission européenne, le **gouvernement français recommandait ainsi de renforcer le soutien aux médias fiables et indépendants, d'assurer la pleine application du règlement sur les services numériques (DSA)¹, de développer la coordination européenne notamment dans le cadre du système d'alerte rapide (RAS) ou encore de travailler à l'émergence d'une véritable communauté d'acteurs pour lutter contre les manipulations de l'information** (harmonisation des pratiques et méthodologies, mise en réseau et interopérabilité des échanges) et participer au renforcement des capacités des États membres pour détecter et analyser les campagnes d'ingérences étrangères et de manipulation de l'information.

Le SGAE confirme ainsi que les autorités françaises contribuent activement aux travaux de la Commission européenne dans la mise en œuvre du bouclier, soulignant qu'il « s'inscrit en outre en synergie avec d'autres initiatives destinées à renforcer la préparation et la résilience de l'Union européenne, notamment face aux manipulations de l'information et aux ingérences numériques étrangères, dont le livre blanc sur la préparation à la défense, la stratégie de préparation, la stratégie de sécurité intérieure et la stratégie européenne de sécurité extérieure ».

Cependant, la position française transmise par le **SGAE envisage des points d'amélioration afin de renforcer le bouclier**. Au sein des institutions européennes, la France appelle ainsi, notamment, « *à responsabiliser davantage les plateformes dans la lutte contre ces phénomènes, notamment la persistance de modes opératoires informationnels sur leurs services* ».

Rappelant que le Sénat a approuvé le principe d'un bouclier européen de la démocratie dans sa résolution européenne sur le programme de travail de la Commission européenne pour l'année 2026 précitée², les rapporteurs soulignent qu'ils partagent cette réserve et **appellent à la consolidation du bouclier**. Ils formulent notamment des propositions relatives au **renforcement du cadre juridique applicable aux grandes plateformes**.

¹ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

² <https://www.senat.fr/leg/tas25-042.html> du 23 janvier 2026.

3. Un avis réservé de la commission spéciale du Parlement européen sur la portée effective du bouclier

Le **Parlement européen** a voté le 18 décembre 2024 en faveur de la création d'une **commission spéciale sur le bouclier européen de la démocratie**, dont le mandat a été prolongé jusqu'au 3 février 2027. Elle est présidée par Mme Nathalie Loiseau (Renew, France) et son rapporteur est M. Tomas Tobé (PPE, Suède).

Prenant la suite de deux commissions spéciales antérieures sur les ingérences étrangères, l'objectif de cette commission spéciale est d'évaluer la législation et les mesures de l'UE existantes et prévues à la lumière d'éventuelles ingérences malveillantes dans les processus démocratiques, notamment en ce qui concerne le bouclier européen de la démocratie, annoncé dans les orientations politiques de la Commission pour la période 2024-2029.

Or, dès la présentation du bouclier européen de la démocratie, le rapporteur bouclier a demandé à la Commission européenne d'« *aller plus loin dans son ambition, avec des réformes concrètes* ». Il regrette depuis, de façon constante, **le manque d'ambition du bouclier européen de la démocratie, considérant la proposition contenue dans la communication conjointe trop limitée, sans base juridique solide, sans budget spécifique et sans rôle clair** pour détecter, analyser et répondre aux ingérences, au-delà de son seul rôle de coordination.

Le rapport sur le bouclier européen de la démocratie, adopté dans sa version de compromis par la commission spéciale, le 23 juin 2026¹, **identifie des mesures visant à renforcer la capacité de l'UE à objectiver, prévenir et contrer la manipulation de l'information et l'ingérence étrangères (FIMI), ainsi que d'autres menaces hybrides**. Il constitue la première position politique globale du Parlement européen sur ces questions.

Il procède à une mise à jour rapide de la menace et des attaques auxquelles l'Europe fait face, rappelant que **la Russie, notamment, est une menace continue tant directement que via d'autres acteurs, étatiques ou non**. Le rapport fait cependant le constat qu'il serait **dangereux de ne pas ouvrir les yeux face aux autres menaces émanant d'autres États** comme la Biélorussie, la Chine, l'Iran et la Corée du Nord. Certes, de manière prudente, le rapport mentionne en outre ouvertement l'administration américaine actuelle et les groupes affiliés aux Etats-Unis.

Sur le fond, le rapport **regrette tout d'abord que le Centre européen pour la résilience démocratique (ECDR) soit proposé sans acte législatif** le dotant d'un statut institutionnel clair, d'une gouvernance définie, et de mécanismes de financement propres.

¹ Conclusions et recommandations de la commission spéciale sur le « bouclier européen de la démocratie » (2025/2069(INI)), Tomas Tobé, 23 juin 2026.

Il appelle à clarifier son mandat, insistant pour qu'il soit mis place par un acte juridique contraignant, avec des paramètres opérationnels, un budget spécifique et une gouvernance impliquant tous les États membres. La conséquence directe est le manque de moyens humains pour assurer ses opérations. Alors que Tomas Tobé proposait d'envisager des mécanismes de financement, dont une contribution des grandes plateformes en ligne¹, le rapport de la commission spéciale du Parlement européen demande une ligne budgétaire spécifique pour les opérations du Centre européen pour la résilience démocratique, au sein du budget de l'UE.

En second lieu, le rapport de la commission spéciale du Parlement européen **critique le fait que la participation des États membres au Centre soit volontaire, ce qui pourrait conduire à une protection inégale selon les pays**. Le rapport constate en outre que l'UE souffre d'une approche fragmentée dans la lutte contre les manipulation et ingérence de l'information étrangère (FIMI) et la désinformation, avec des variations significatives dans les capacités des États membres.

Sur ce volet, les rapporteurs de la commission des affaires européennes soulignent **qu'une participation de tous les États-membres apparaît indispensable pour assurer des capacités de réponses adaptées à des ingérences numériques qui conduisent à rendre les frontières superfétatoires. En complément, dans une approche conforme au respect des principes de subsidiarité et de proportionnalité**, les rapporteurs considèrent que la résilience démocratique européenne passe par un effort de coordination des initiatives nationales et par l'encouragement des États membres les moins avancés, à travers l'action du Centre européen pour la résilience démocratique.

Par ailleurs, le rapport de la commission spéciale du Parlement européen regrette que la communication instituant le bouclier ne lie pas explicitement le centre aux actions déjà annoncées au titre du règlement sur les services numériques (DSA) ou encore de l'Observatoire européen des médias numériques (EDMO). Il souligne également que d'autres outils de lutte contre la désinformation existent, telle l'initiative menée par le Service d'action extérieure de l'Union européenne (SEAE) appelé EUvsDiSiNFO², soulignant la fragmentation des actions existantes qui sont éparpillées dans différents cadres administratifs.

¹ *Rapport du 18 décembre 2025 de M. Tomas Tobé sur les conclusions et recommandations de la commission spéciale sur le bouclier européen de la démocratie.*

² <https://euvsdisinfo.eu/fr/>

Le rapport de la commission spéciale du Parlement européen souligne d'autres manquements dans la mise en œuvre du bouclier. Il critique notamment le fait que **les sanctions européennes contre la Russie et d'autres acteurs malveillants (par exemple, l'Iran ou encore la Chine) ne ciblent pas suffisamment les « facilitateurs » des campagnes de FIMI**, tels les plateformes de cryptomonnaies ou les réseaux publicitaires, qui sont communément utilisés pour financer des campagnes de désinformation ou de FIMI. Le rapport souligne en outre que l'efficacité des sanctions dépend de leur application stricte et coordonnée, mais que les États membres ne partagent pas suffisamment d'informations pour permettre aux agences Europol et Eurojust de jouer pleinement leur rôle dans la lutte contre les menaces hybrides.

À ce titre, le rapport de la commission spéciale du Parlement européen souligne, tout en la déplorant, **l'augmentation des attaques hybrides** (sabotage physique, cyberattaques, brouillage GPS, ...) **ciblant les infrastructures critiques** tels les câbles sous-marins, les ports, aéroports ou encore les réseaux énergétiques. Or **celles-ci ne sont pas abordées dans la communication sur le bouclier européen de la démocratie**.

De même, **le rapport de la commission spéciale du Parlement européen met en garde contre la dépendance de l'UE aux technologies étrangères** (semi-conducteurs, inverseurs solaires chinois, services d'informatique en nuage ou *cloud*) qui exposent les infrastructures critiques à des risques de cyberattaques ou de manipulation par des puissances étrangères ou des acteurs privés malveillants.

Auditionnée par les rapporteurs, le vendredi 26 juin 2026, la députée européenne Nathalie Loiseau (France, Renew), présidente de la commission spéciale du Parlement européen sur le bouclier européen de la démocratie, confirme qu'il apparaît urgent de réduire la dépendance aux technologies étrangères, qui sont « en elles-mêmes des vecteurs d'ingérence ».

Les rapporteurs de la commission des affaires européennes partagent pleinement cette analyse et **rappellent que la souveraineté numérique européenne est intimement liée aux enjeux de résilience démocratique**, au regard de la numérisation croissante des pratiques informationnelles des citoyens. C'est d'ailleurs un constat constant de la commission des affaires européennes du Sénat, depuis 2013 et le rapport « L'Europe, colonie du monde numérique ? »¹ de la rapporteure Catherine Morin-Desailly.

Recommandation : mieux intégrer la prise en compte des menaces hybrides dans le bouclier européen de la démocratie.

¹ Rapport d'information n° 443 (2011-2012) de Mme Catherine MORIN-DESAILLY au nom de la commission des affaires européennes.

Recommandation : renforcer par tous moyens la souveraineté numérique européenne, laquelle est un vecteur intrinsèque de résilience démocratique.

Enfin, le rapport de la commission spéciale du Parlement européen **regrette que les programmes de financement pour les médias indépendants et les fact-checkers soient insuffisants et peu prévisibles**. À titre d'exemple, il souligne que les fonds pour la société civile dans les pays candidats (Ukraine, Moldavie, Balkans occidentaux) ne sont pas garantis dans le prochain cadre financier pluriannuel (CFP) pour 2028-2034.

4. Un bouclier en papier ?

En somme, le bouclier européen de la démocratie se présente avant tout comme un **cadre d'orientation stratégique** plutôt que comme un ensemble de mesures **opérationnelles et contraignantes**. En effet, la plupart des actions proposées relèvent de **recommandations, d'incitations à la coopération volontaire** ou de **lignes directrices non obligatoires, sans mécanisme de sanction** ou de **contrôle effectif** pour en garantir l'application.

Il repose en outre essentiellement sur des protocoles et lignes directrices – à l'instar des lignes directrices sur l'utilisation de l'IA dans les processus électoraux que la Commission européenne doit proposer.

Les rapporteurs estiment que ce flou juridique et politique affaiblit la crédibilité du bouclier et favorise une application inégale selon les États membres, au risque de ne pas répondre à l'enjeu de disposer d'une capacité de réponse opérationnelle qui recouvre l'ensemble du territoire européen, s'agissant de risques qui transcendent les frontières nationales.

Le bouclier tout entier pourrait ainsi **gagner à être renforcé et ne pas se borner à une coordination de moyens existants**, ainsi que le déplorent certains États membres comme l'Estonie ou la Roumanie, sans nuire aux capacités et prérogatives des États membres les plus avancés en la matière, à l'instar de la France avec VIGINUM.

Les rapporteurs déplorent également la superposition d'acteurs intervenant dans la lutte contre les ingérences étrangères et la désinformation. Le bouclier ajoute de nouvelles structures (plateformes des parties prenantes, Centre européen pour la résilience démocratique) à des dispositifs existants (ex. : l'Observatoire européen des médias numériques - EDMO, le système d'alerte rapide du SEAE, l'Agence de l'Union européenne pour la cybersécurité (ENISA), le réseau européen de coopération en matière d'élections, *etc.*), sans clarifier leurs rôles respectifs ni éviter les chevauchements.

La suite du présent rapport entend réaliser un bilan d'étape sur la mise en œuvre du Centre européen pour la résilience démocratique, afin de questionner la pertinence de positionner cette nouvelle structure, en cours de construction, comme l'acteur de la coordination européenne en matière de détection des campagnes de FIMI, d'analyse en temps réel des données et de coopération entre les États membres pour apporter une réponse coordonnée aux tentatives d'ingérences détectées sur le territoire européen.

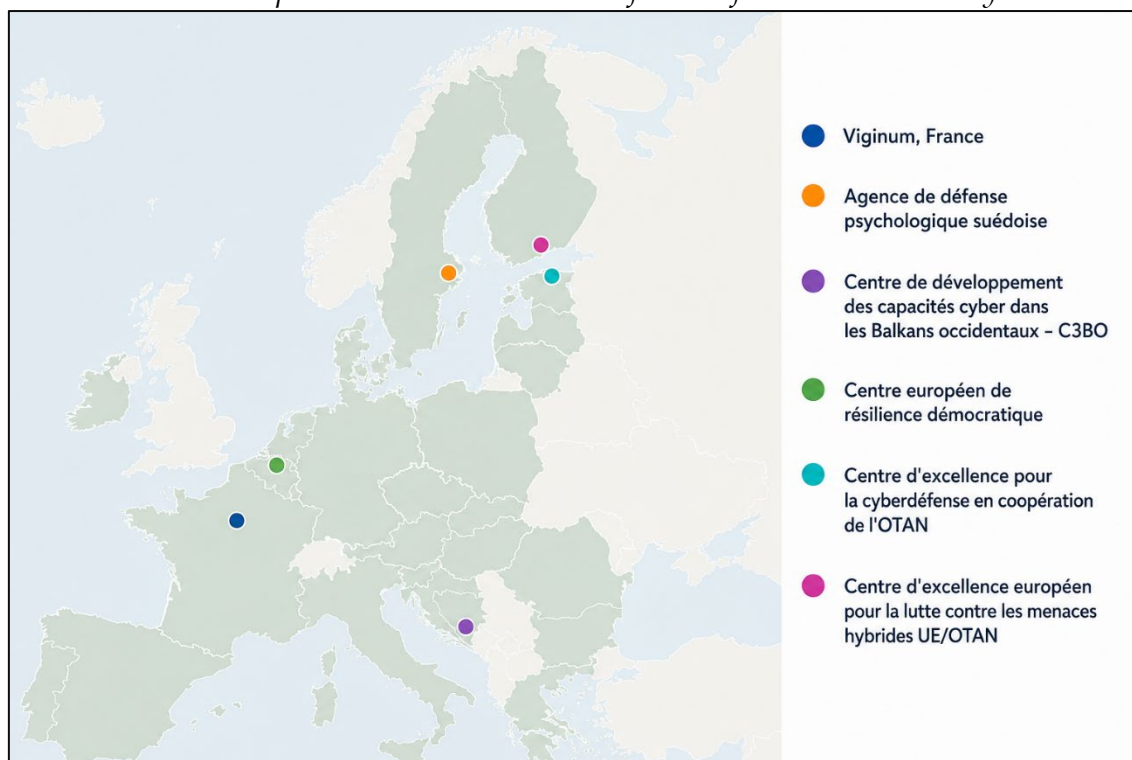
II. UN BILAN D'ÉTAPE DÉCEVANT DE LA MISE EN ŒUVRE DU CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE

Afin de pouvoir questionner la pertinence du Centre européen pour la résilience démocratique, les rapporteurs ont souhaité le replacer dans son contexte géostratégique, en cartographiant les initiatives européennes existant sur le territoire européen, soit qu'elles luttent déjà, au niveau national ou international, contre les ingérences étrangères numériques, les risques cyber, soit qu'elles visent à renforcer la résilience de la société civile ou des médias.

A. CARTOGRAPHIE DES INITIATIVES EUROPÉENNES DÉJÀ EXISTANTES

Plusieurs structures existent déjà sur le territoire européen, relevant soit d'initiatives nationales (VIGINUM en France, Agence de défense psychologique en Suède), soit d'initiative de coopération internationale (Centre d'excellence pour la cyberdéfense en coopération adossé à l'OTAN, basé à Tallinn ; Centre de développement des capacités cyber dans les Balkans occidentaux ou C3BO, basé à Podgorica ; Centre UE/OTAN de lutte contre les menaces hybrides – Hybrid CoE – basé à Helsinki), afin de déterminer comment le Centre européen pour la résilience démocratique, adossé à la Commission européenne, s'inscrit dans ce paysage. D'autres initiatives, plus ou moins avancées, existent dans d'autres États membres, notamment en Allemagne, en Pologne ou dans les pays baltes.

Centres européens de résilience et de défense informationnelle et cyber



Source : Infographie générée avec l'aide de l'IA

1. Le modèle français de VIGINUM, un exemple performant à répliquer dans l'Union européenne

a) Le mandat de VIGINUM

En France, la première stratégie nationale de lutte contre les manipulations de l'information, a été adoptée en février 2026. Élaborée sous l'égide du Secrétariat général de la défense et de la sécurité nationale (SGDSN), elle s'appuie sur des contributions d'experts, de chercheurs, de parlementaires et d'acteurs de terrain engagés dans la lutte contre les manipulations de l'information. Elle s'articule autour de quatre priorités, dont le renforcement de la résilience nationale et l'encadrement des plateformes en ligne et des intelligences artificielles génératives, soulignant l'impérieuse nécessité d'une action collective, tant au niveau national qu'eupéen.

Toutefois, la création du service de vigilance et de protection contre les ingérences numériques étrangères, communément appelé VIGINUM, précède cette stratégie nationale. Rattaché au SGDSN, VIGINUM a en effet été créé il y a cinq ans, le 13 juillet 2021. Il s'agit d'un service technique et opérationnel de l'État dont l'objectif est de lutter contre les manipulations de l'information, dans une approche défensive, puisqu'elle consiste à détecter et caractériser les opérations d'ingérences numériques étrangères qui ciblent la France, afin de protéger le débat public numérique.

Les missions de VIGINUM ont en outre été renforcées par le décret n° 2026-70 du 11 février 2026, lequel précise et renforce le mandat du service comme suit, au titre de son article 3 :

« 1° Détecter, caractériser et documenter, en analysant les données accessibles publiquement sur les plateformes en ligne, sur les moteurs de recherche en ligne ainsi que sur les interfaces en ligne, au sens des i, j et m de l'article 3 du 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, les opérations mentionnées au 9° de l'article R. 1132-3 du code de la défense, notamment lorsque celles-ci sont de nature à altérer l'information des citoyens pendant les périodes électorales mentionnées à l'article 33-1-1 de la loi du 30 septembre 1986 susvisée ;*

1° bis Contribuer à la recherche et au développement d'outils, d'algorithmes et de modèles susceptibles d'être mobilisés dans l'exercice de sa mission mentionnée au 1° du présent article ;

2° Assister le secrétaire général de la défense et de la sécurité nationale dans sa mission d'animation et de coordination des travaux interministériels en matière de protection contre les opérations mentionnées au 1° et d'anticipation des menaces qu'elles représentent ;

3° Fournir toute information utile :

a) À l'Autorité de régulation de la communication audiovisuelle et numérique dans l'accomplissement des missions qui lui sont confiées par la loi du 30 septembre 1986 susvisée, notamment son article 33-1-1, et la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment le dernier alinéa de son article 7-3 en vue de participer à la supervision de la mise en œuvre effective de l'obligation d'atténuer les risques systémiques mentionnés à l'article 34 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) ;

b) À la Commission nationale de contrôle instituée par l'article 13 du décret du 8 mars 2001 susvisé ;

c) À toute autorité, y compris juridictionnelle, saisie à l'occasion d'élections politiques ;

4° Contribuer aux travaux européens et internationaux et assurer la liaison opérationnelle et technique avec ses homologues étrangers, dans le respect des attributions du ministre des affaires étrangères ;

5° Contribuer à l'information du public, ainsi qu'aux actions d'éducation aux médias conformément aux dispositions de l'article L. 111-2 du code de l'éducation. »

Tirant ces missions de ce mandat clair, VIGINUM a depuis 5 ans mis en œuvre ses services pour relever et contrer les ingérences numériques étrangères (INE). Pour ce faire, le service est composé de 67 équivalents temps plein (ETP) dont les deux tiers relèvent du service opérationnel, chargé de veille et de caractérisation des MOI.

b) Des réalisations concrètes et opérationnelles

Alors que le service aura bientôt cinq ans d'existence, VIGINUM se démarque par des réalisations concrètes dans les trois domaines suivants :

- la caractérisation des menaces, l'identification et la lutte contre des MOI ;
- la formation et la sensibilisation de la société civile et des médias ;
- la coopération interministérielle et internationale.

Présentée aux rapporteurs lors de leur visite sur site à VIGINUM le 1^{er} juillet 2026, l'activité opérationnelle de VIGINUM constitue **80 % des activités du service** et consiste à suivre la cinquantaine de MOI majeurs identifiés par le service depuis 2022 et qui sont reliés à douze nationalités différentes. Le reste de l'activité de VIGINUM consiste en des opérations de veille destinées à repérer et caractériser de nouveaux MOI.

L'exemple d'un travail d'analyse mené par VIGINUM

L'analyse du mode opératoire informationnel appelé par VIGINUM « Fawn Mianju », attribuable à des acteurs chinois, illustre l'usage croissant de l'IA pour réécrire et diffuser à grande échelle des contenus propagandistes, ciblant notamment les francophones.

Mettant en œuvre une méthodologie mêlant analyse des métadonnées numériques, analyse du discours et méthodes d'investigation, VIGINUM a démontré comment des sites web comme ActuMérindien.fr, liés au média d'État chinois CGTN, utilisaient des outils d'automatisation (N8N, ChatGPT) pour publier des articles réécrits en un temps record, avec une standardisation stylométrique révélatrice d'une génération par IA. Bien que l'effet de ces campagnes reste limité en termes d'engagement de la société civile en réaction, leur coordination multilingue et leur ciblage géopolitique – notamment envers l'Afrique francophone – révèlent une stratégie systématique de manipulation de l'opinion publique, adaptée aux priorités diplomatiques du régime chinois.

Entendus le 1^{er} juillet 2026, les représentants de VIGINUM rappellent cependant que son mandat consiste à produire de l'investigation pour informer les services de l'État en capacité d'opérer une riposte informationnelle, notamment le ministère des affaires étrangères, qui peut riposter en mettant en œuvre une communication d'influence *ad hoc* voire le ministère des armées s'agissant des réponses non assumables. Pour ce faire et adapter la réponse, un comité technique opérationnel se réunit tous les quinze jours en présence de l'ensemble des acteurs étatiques et militaires partenaires. Les représentants de VIGINUM précisent qu'il existe en outre des structures spécifiques s'agissant de la prévention des ingérences électorales, notamment à l'aune de l'élection présidentielle de 2027 avec un réseau de coordination et de protection des élections (RCPE). Ce dernier a été mis en place tout récemment, le 7 janvier dernier, en prévision des ingérences et des déstabilisations susceptibles d'affecter la campagne des élections municipales. Il permet de rassembler régulièrement plusieurs institutions, dont l'Arcom, VIGINUM, la Commission nationale des comptes de campagne et des financements politiques (CNCCFP), afin de suivre l'évolution des menaces au cours de la campagne et d'y apporter une réponse commune.

Par ailleurs, **VIGINUM rappelle qu'une collaboration avec les plateformes numériques est indispensable** afin de pouvoir contrer les MOI identifiés, de même qu'avec l'Association française pour le nommage Internet en coopération (Afnic) qui est l'office d'enregistrement des noms de domaine en « .fr ».

Ainsi, VIGINUM partage des éléments techniques relatifs à l'activité inauthentique des modes opératoires informationnels étrangers avec de nombreuses plateformes numériques dont X, Google, YouTube, Facebook, Instagram, TikTok et Bluesky. Dans certains cas, VIGINUM est appelé à solliciter de la part de ces plateformes des actions de modération, pour supprimer les comptes, chaînes ou pages impliqués dans des manœuvres informationnelles étrangères malveillantes ou faire cesser les contenus caractérisant des campagnes d'ingérence numérique étrangère.

En juillet 2024, VIGINUM a signé **une convention avec l'Arcom** – coordinateur national pour les services numériques au titre du règlement européen sur les services numériques (DSA) – afin de faciliter les échanges entre les deux entités, mettre en commun les expertises et lutter plus efficacement contre les ingérences numériques étrangères.

c) L'ambition du renforcement de la résilience de la société civile : l'Académie de la lutte contre les manipulations de l'information (LMI)

Dans son mandat révisé en février 2026, VIGINUM s'est vu doter d'une **mission de sensibilisation de la société civile**. À cette fin a été créée fin 2025 une Académie de la lutte des manipulations de l'information avec trois objectifs :

- développer et massifier les efforts d'information vis-à-vis du public pour **renforcer la vigilance des citoyens** ;
- assurer la **formation en matière de lutte contre les manipulations de l'information** par le partage des savoir-faire auprès des partenaires internationaux et des médias (notamment sur techniques d'investigation numérique) ;
- **développer des partenariats académiques** avec le monde de la recherche, dans l'objectif de contribuer à l'émergence d'une filière de recherche sur les manipulations de l'information, en vue de bénéficier à termes aux missions institutionnelles de VIGINUM.

En cours de préfiguration, cette Académie compte déjà des résultats concrets, tels un jeu de plateau et une application en ligne « le bouclier contre les ingérences numériques étrangères », sur le modèle de la « fresque du climat », destiné à engager le dialogue, notamment auprès des publics d'élèves en âge secondaire. Concernant le public des élèves et des enseignants, des guides d'information sont également d'ores et déjà disponibles sur le site internet de VIGINUM.

L'Académie a en outre développé des *podcasts* et une chaîne Youtube pour informer sur les INE.

Des formations spécifiques aux journalistes sont également promues dans les écoles de journalismes et avec un programme de partenariat avec l'organisme Cyber for good, aux fins de formations des journalistes déjà en activités, notamment au sein de la presse quotidienne régionale, dans un objectif de renforcement de la résilience du secteur des médias.

Les rapporteurs saluent la variété des actions concrètes menées par VIGINUM pour sensibiliser la société civile et ainsi renforcer sa résilience.

Ils soulignent que **VIGINUM peut être un modèle pour les États membres qui n'ont pas encore finalisé leur organisation nationale pour la lutte contre les ingérences numériques étrangères.**

**Le Forum annuel 2026 de VIGINUM sur le thème
« Déstabilisation du paysage médiatique. Ensemble protégeons l'espace
informationnel contre les ingérences étrangères »**

Le forum annuel de VIGINUM, qui s'est tenu le jeudi 4 juin 2026, a mis en exergue une composante clé pour la lutte contre les ingérences étrangères en ligne : la protection et le renforcement de la résilience des médias.

Ce forum a été l'occasion de mettre en lumière les défis croissants pesant sur l'intégrité de l'espace médiatique français et européen, face à la multiplication et à la sophistication des opérations d'ingérence numérique étrangère. Depuis l'été 2025, VIGINUM indique que plus de quinze médias traditionnels français auraient vu leurs comptes usurpés, devenant malgré eux des vecteurs de désinformation, tandis que l'essor des médias en ligne, faciles à créer et potentiellement contrôlés par des puissances étrangères ou leurs avatars, aggrave la vulnérabilité du débat public.

Comme l'a souligné Marc-Antoine Brillant, chef de service de VIGINUM, l'enjeu réside désormais dans la capacité à distinguer « l'authentique » de « l'inauthentique », tout en comprenant les logiques algorithmiques qui sous-tendent la diffusion de contenus manipulés voire créés par l'IA et traduits potentiellement sans délai dans toutes les langues de l'Union européenne.

Des échanges lors d'une table ronde consacrée à la reconfiguration du paysage médiatique ont révélé une menace double : d'une part, l'exploitation de la crédibilité des médias traditionnels par des acteurs malveillants, comme en témoignent des tentatives de détournement de l'identité visuelle des journaux Le Monde ou Ouest-France, et, d'autre part, l'émergence de médias inauthentiques, souvent générés par IA, qui tentent de diffuser des informations fallacieuses sous couvert d'une apparente légitimité.

Mme Maud Lévrier, membre du directoire du groupe Ouest-France, a par exemple évoqué le cas du site « Var Actu », agréé en 2025 par la commission des publications de presse. Ce statut lui a permis de bénéficier du régime économique et juridique de la presse pendant plusieurs mois malgré son origine a priori artificielle et la génération de ses articles par l'IA.

Face à ces risques et aux diverses tentatives d'ingérence ou d'usurpation dont ils sont victimes, lesquelles s'accompagnent parfois de campagne d'intimidation ou de harcèlement ciblant les journalistes, les médias traditionnels adoptent des réponses graduées, allant de la mise en demeure à la demande de désindexation adressée aux plateformes et réseaux sociaux. Ils appellent toutefois à une coopération renforcée entre acteurs de la presse pour partager les bonnes pratiques et les outils de détection.

2. Une diversité d'acteurs aux approches hétérogènes implantés sur le territoire européen

a) Le modèle suédois : l'Agence de défense psychologique

Outre la France, **la Suède est l'autre pays européen communément mis en avant pour son avance relative en matière de capacité nationale d'identification et des réponses aux tentatives de désinformation ou d'ingérence numérique étrangères**. Créée un an après VIGINUM, son Agence de défense psychologique, est d'ailleurs, avec VIGINUM, la seule autre structure nationale citée comme exemple par la Commission européenne pour contribuer à l'édification du Centre européen pour la résilience démocratique dans sa communication conjointe du 12 novembre 2025 précitée.

Selon son mandat, l'Agence de défense psychologique « a pour mission d'identifier, d'analyser et d'apporter son soutien dans la lutte contre l'influence d'information malveillante et toute autre information trompeuse visant la Suède ou les intérêts suédois de la part de puissances étrangères hostiles. Il peut s'agir de désinformation visant à affaiblir la résilience de la Suède et la volonté de la population de se défendre, ou à influencer indûment les perceptions, le comportement et la prise de décision des citoyens ».

Selon l'Agence, « la défense psychologique désigne les capacités communes de la société à détecter et à contrer l'influence néfaste de l'information exercée à l'encontre de la Suède par des puissances étrangères hostiles ».

Composée de trois départements dont un service de communication, l'Agence de défense psychologique est un organisme **relevant du gouvernement**. Son siège se trouve à Karlstad et elle dispose d'un bureau supplémentaire à Solna.

Un département du **développement des capacités** a pour mission de développer et de renforcer les capacités collectives de défense psychologique de la société en apportant un soutien à la population, aux agences, aux municipalités, aux médias, aux organisations bénévoles de défense et à la société civile, ainsi qu'en favorisant une meilleure coordination entre ces acteurs. Parmi ses missions clés figurent également la responsabilité de la formation, des exercices et du renforcement des connaissances, par exemple en commanditant, en supervisant et en diffusant les travaux de recherche dans le domaine de la défense psychologique.

En outre, un département des opérations identifie, analyse et contre l'influence néfaste de l'information étrangère et d'autres informations trompeuses visant la Suède ou les intérêts suédois. Il est chargé d'établir des rapports de situation, d'analyses et des rapports sur les acteurs et les activités susceptibles de constituer des menaces en exploitant les vulnérabilités de la société suédoise, ainsi que de proposer des contre-mesures pertinentes. Le département développe des méthodes et des techniques permettant d'identifier et de répondre à l'influence d'information malveillante.

b) L'exemple du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO)

À la suite des cyberattaques majeures ayant touché le Monténégro et l'Albanie en 2022, et dans la perspective d'adhésion à l'UE, la France a lancé, avec la Slovénie et le Monténégro, le projet de création d'un Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO). Ce projet s'inscrit dans le Processus de Berlin et dans les priorités de sécurité européenne. La France assure le pilotage stratégique et technique de ce projet, ainsi que le financement principal.

Le centre C3BO a été inauguré officiellement à Podgorica, capitale du Monténégro, en décembre 2024. Il **repose sur trois piliers : la cybersécurité, la lutte contre la cybercriminalité, et la cyberdiplomatie**. Son objectif est de renforcer les capacités cyber pour atteindre les standards européens en matière de formation en cybersécurité, les licences logicielles mais aussi les équipements, sur le plan de leur cyberrésilience.

Sur le plan des ressources humaines, la France fournit sur place depuis 2023, trois experts : un directeur des programmes (issu de la Gendarmerie nationale) et deux formateurs (de la Police et de la Gendarmerie). Ces experts sont assistés au sein du centre C3BO par trois collaboratrices monténégrines recrutées localement par la Slovénie.

Ce centre se démarque par des premiers résultats concrets. Outre un partenariat académique avec l'Université de technologie de Troyes (UTT) fondé sur des cursus diplômants en cybersécurité et en forensique numérique et des partenaires privés et publics, 43 formations et dialogues stratégiques ont été organisés en 2025 au profit de 896 participants issus des 6 pays bénéficiaires : l'Albanie, la Bosnie-Herzégovine, le Kosovo, la Macédoine du Nord, le Monténégro, la Serbie¹.

Selon les chiffres transmis aux rapporteurs, **86 % de l'activité de formation correspond à une démarche de formation technique et pratique, axée sur la montée en compétences opérationnelles des publics formés.**

S'agissant d'une région stratégique, exposée aux menaces hybrides, à la désinformation et à la cybercriminalité organisée, les rapporteurs saluent le caractère opérationnel du centre C3BO, utile à la montée en compétence des pays accompagnés, dans la perspective d'une adhésion à l'Union européenne.

c) Le Centre d'excellence pour la cyberdéfense en coopération, adossé à l'OTAN

Le **Centre d'excellence pour la cyberdéfense en coopération** (CCDCoE) est l'un des centres d'excellence adossé à l'OTAN². Il est situé à Tallinn, en Estonie. Une délégation de la commission des affaires européennes avait échangé avec un membre français de ce centre, à l'occasion d'un déplacement les 24 et 25 mars 2025.

Ce centre organise notamment chaque année depuis 2010 **le plus grand exercice de cyberdéfense dans le monde appelé *Locked Shields*** (« boucliers verrouillés ») dans lequel des équipes s'affrontent. Réalisé en conditions réelles, une équipe monte une cyberattaque réaliste et à grande échelle que d'autres équipes doivent contrer. L'exercice intègre également des considérations juridiques et de communication de crise, favorisant, selon les termes du site web de Centre « *un état d'esprit de guerre qui oblige les équipes à réfléchir rapidement, à s'adapter à des menaces inattendues et à collaborer efficacement* ».

L'édition 2026 rassemble 4 000 participants issus de 41 pays.

Les rapporteurs soulignent le caractère hautement concret et opérationnel de tels exercices, ce qui en renforce l'utilité. Ces exercices mêlent en outre acteurs civils et militaires, dans un objectif de protection des services vitaux et des infrastructures critiques, ce qui participe au renforcement capacitaire des États, dans la droite ligne de l'objectif de résilience démocratique.

¹ Sont également ponctuellement accompagnés l'Ukraine et la Moldavie.

² Il est appelé NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), en anglais.

d) Le centre d'excellence européen pour la lutte contre les menaces hybrides, une initiative commune de l'UE et de l'OTAN

Le centre européen d'excellence pour la lutte contre les menaces hybrides (*Hybrid CoE*) est une initiative conjointe de l'Union européenne et de l'OTAN. Il se présente comme « *une organisation internationale d'experts, autonome et fonctionnant en réseau, qui se consacre à la lutte contre les menaces hybrides et à la promotion d'une approche impliquant l'ensemble des pouvoirs publics et de la société civile pour y faire face* ». Les travaux du centre sont planifiés et coordonnés par un secrétariat, situé à Helsinki, en Finlande.

Il s'agit d'une institution unique en son genre, destinée à permettre à l'UE et à l'OTAN de travailler ensemble pour identifier et contrer les menaces hybrides. Outre le partage de bonnes pratiques, des recommandations et la possibilité de tester de nouvelles approches, le centre européen d'excellence pour la lutte contre les menaces hybrides organise des exercices conjoints, ses activités couvrant un large éventail de domaines, allant du civil au militaire et de l'influence hostile à la guerre hybride.

Une délégation de la commission des affaires européennes avait échangé avec un représentant du centre, lors d'un déplacement en Finlande, le vendredi 29 mai 2026.

B. DANS CET ENVIRONNEMENT DÉJÀ DENSE, QUELLE PLACE ET QUEL RÔLE POUR LE CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE ?

1. Le risque d'une désorganisation des initiatives sans une coopération stratégique

a) Une vigilance nécessaire dans l'association au centre de pays tiers

La cartographie détaillée précédemment des différentes initiatives existantes en Europe relève **une certaine hétérogénéité dans le paysage de la lutte contre les FIMI**, tant dans les choix institutionnels que dans les approches adoptées pour les détecter et les contrer par les différents États membres au niveau national et international.

Si les rapporteurs considèrent que, par plusieurs aspects, la lutte contre les ingérences étrangères numériques, comme la cybersécurité, relèvent de la sécurité nationale et qu'à ce titre, les principes de subsidiarité et de proportionnalité doivent trouver à s'appliquer strictement¹, ils considèrent qu'une coordination est nécessaire au niveau européen pour assurer une coopération opérationnelle et stratégique.

Le Centre européen pour la résilience démocratique (CERD) pourrait utilement jouer ce rôle de coordinateur, sans nuire à la capacité des États membres.

Toutefois, pour ne pas risquer de devenir une autre plateforme ou un centre parmi d'autres, ce qui aggraverait la fragmentation des efforts européens et réduirait l'efficacité des outils existants, il ne peut exister que sur la base d'un mandat clair axé sur la seule coordination des initiatives nationales, la coopération en vue du partage des bonnes pratiques et du renforcement des capacités des pays les moins avancés en la matière.

À cet égard, dans ses réponses au questionnaire transmis par les rapporteurs, le Secrétariat général des affaires européennes (SGAE) indique que lors d'une réunion tenue le 17 juin 2026, en présence du secrétariat du CERD, une réflexion aurait été conduite sur l'association au Centre des pays candidats et candidats potentiels.

Les rapporteurs sont favorables à l'association des pays candidats ou potentiels, volontaires ou partenaires, dans la limite d'une analyse des risques géostratégiques. Ainsi, les rapporteurs rappellent que l'Union européenne demeure un espace de communauté de valeurs, qui est donc plus favorable à des échanges en matière de résilience démocratique que d'autres instances de coopération internationale.

Se pose par exemple la question de l'articulation des initiatives de l'Union européenne, notamment l'élargissement du Centre européen pour la résilience démocratique à des pays affinitaires situés sur le continent européen, avec le **Nouveau pacte démocratique annoncé par le Conseil de l'Europe**, alors que les États membres de l'Union européenne sont membres du Conseil de l'Europe.

¹ Voir notamment la pastille 12 de la n° 110 (2025-2026), devenue résolution du Sénat le 13 mai 2026 portant avis motivé sur la conformité au principe de subsidiarité et de proportionnalité de la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2) - COM(2026) 11 final et de la proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2] - COM(2026) 13 final : « Dès lors qu'elle est fondamentale du point de vue de la sécurité nationale, [la cybersécurité] relève également de l'article 4 du TUE qui stipule que l'Union européenne « respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale ».

Les rapporteurs rappellent qu'au sein du Conseil de l'Europe, certains pays membres peuvent être parties prenantes de modes opératoires informationnels tendant vers l'ingérence numérique étrangère. Aussi, ces instances, utiles au dialogue international, ne peuvent remplacer la coopération entre États membres de l'UE mise en place au sein du CERD.

Recommandation : associer les pays candidats ou candidats potentiels aux travaux du Centre, uniquement dans la limite d'une analyse des risques géostratégiques posés par ces pays du point de vue de leur implication potentielle dans des stratégies d'ingérences numériques étrangères (INE).

b) Quelle articulation avec le Nouveau pacte démocratique du Conseil de l'Europe ?

Le projet d'un « Nouveau pacte démocratique » a ainsi émergé à la suite de l'adoption de ces « *Principes de Reykjavik pour la démocratie* ». Selon M. Alain Berset, Secrétaire général du Conseil de l'Europe, il ne s'agit pas de « *réinventer la démocratie* », mais d'en consolider les fondements, plus particulièrement là où elle est encore fragile ou fragilisée. Il vise ainsi à renforcer la résilience des institutions démocratiques et à enrayer l'effritement de la démocratie entretenu par la désinformation et les dérives autoritaires.

Les Principes de Reykjavik : un nouvel élan du Conseil de l'Europe en faveur de la démocratie

Rassemblant aujourd'hui 46 États, de l'Islande à l'Azerbaïdjan, le Conseil de l'Europe a également voulu tirer les conséquences de l'invasion de l'Ukraine par la Fédération de Russie et du **contexte global de menaces qui pèsent sur les démocraties européennes**. Cette institution fondée en 1949, en période d'après-guerre, s'est structurée autour de la Convention européenne des droits de l'Homme, mais aussi du **protocole additionnel n° 1, dont l'article 3 garantit le droit à des élections régulières, libres et justes**.

Sur la base de ces instruments juridiques et des autres conventions initiées par le Conseil de l'Europe, les chefs des États et des gouvernements du Conseil de l'Europe ont réaffirmé dans une déclaration leur attachement aux principes démocratiques lors de leur 4^e Sommet, tenu à Reykjavik en 2023, considérant que « la sécurité démocratique est essentielle pour que les États membres puissent relever ensemble les défis actuels et futurs et garantir la paix et la prospérité en Europe ».

Ce concept de « sécurité démocratique » irrigue ainsi les « *Principes de Reykjavik pour la démocratie* » (l'annexe 3 de cette déclaration), qui constitue le fondement de ce projet de Nouveau pacte démocratique.

Ce projet de Nouveau pacte s'articule autour de trois phases :

- définir une ambition commune pour la démocratie, fondée sur la Convention et les Principes de Reykjavik ;
- mener une large consultation sur les défis démocratiques afin de revitaliser la démocratie par un dialogue ouvert ;
- traduire les résultats de ces consultations en politiques concrètes à tous les niveaux.

Les consultations ont démarré fin 2024 et se poursuivent aujourd'hui. **L'Assemblée parlementaire du Conseil de l'Europe (APCE), dont fait partie le Sénat français, participe activement à ces consultations ;** elle a à cet égard **créé une commission spéciale sur ce Nouveau pacte**, qui a notamment entendu en audition Mme Nathalie Loiseau, Présidente de la Commission spéciale du Parlement européen.

La stratégie du Conseil de l'Europe s'est progressivement affinée dans la mise en œuvre de ce Nouveau pacte, lequel reposerait sur trois piliers :

- 1. Apprendre et pratiquer la démocratie** en soutenant les initiatives d'éducation formelle et non formelle qui dotent les citoyens européens – en particulier les jeunes – des compétences, des attitudes et de la pensée critique nécessaires à une citoyenneté engagée ;
- 2. Protéger la démocratie** en élaborant des réponses solides aux menaces internes et externes, notamment la corruption, l'ingérence électorale et la désinformation – en particulier l'utilisation abusive de la technologie numérique et de l'intelligence artificielle (IA) ;
- 3. Innover pour la démocratie** en renforçant les processus démocratiques par la démocratie délibérative et participative, ainsi qu'en exploitant les nouvelles technologies pour améliorer l'accessibilité, la confiance et l'efficacité de la gouvernance.

Un nouvel instrument juridique serait élaboré dans le cadre de ce Nouveau pacte, afin d'apporter une réponse aux ingérences étrangères et aux manipulations de l'information. **L'inclusion de dispositions pénales** dans cet éventuel projet de traité **divise néanmoins les États membres**.

Même si les organisations sont distinctes et si leur périmètre diffère, et bien que les outils déployés soient relativement différents, la question **de l'articulation de ce pacte avec le bouclier européen de la démocratie se pose**, dans la mesure où les priorités et les piliers de ce Nouveau pacte rejoignent pour beaucoup les ambitions fixées pour le bouclier.

Lors de son audition au cours de la Session de l'été 2026 devant l'APCE, M. Alain Berset fut précisément interrogé **sur la valeur ajoutée que le Conseil de l'Europe pouvait apporter par rapport au « bouclier pour la démocratie »** et à son approche ciblée de lutte contre la manipulation de l'information et l'ingérence étrangères (FIMI).

Le Secrétaire général du Conseil de l'Europe a ainsi confirmé **les orientations vers un éventuel instrument juridique sur les FIMI** dans le respect de la démocratie et de l'État de droit et sous l'égide de la Convention européenne des droits de l'homme - à laquelle l'Union européenne n'est toujours pas partie, contrairement à tous ses États membres - et des décisions de la Cour européenne des droits de l'Homme. Il considère en outre que **le Nouveau pacte s'inscrit dans une approche complémentaire**, car le Conseil de l'Europe offre **un cadre paneuropéen plus large**, avec en outre **l'assise solide de la Convention**. Poursuivant le questionnement, Alain Berset déclarait qu'« *il ne s'agit pas de faire un double emploi. L'UE peut renforcer sa réponse opérationnelle, tandis que le pacte ancrera la résilience démocratique dans des normes juridiques communes.* »

Lors de son audition par les rapporteurs, **Mme Nathalie Loiseau reconnaissait aussi l'intérêt d'une initiative lancée par le Conseil de l'Europe**, notamment à l'égard du périmètre paneuropéen plus vaste qu'il recouvrirait. Une vingtaine d'États membres du Conseil de l'Europe ne font en effet pas encore partie de l'UE, comme la Moldavie, l'Albanie, ou le Monténégro, ou **ne font plus partie de l'UE comme le Royaume-Uni**. Ce dernier est pourtant considéré comme un allié incontournable dans la lutte contre les opérations de déstabilisations venant de l'étranger.

Recommandation : inviter la Commission européenne à développer les différentes activités prévues au titre du bouclier européen de la démocratie en lien étroit avec le Conseil de l'Europe, dans le cadre de son initiative en faveur d'un « Nouveau pacte pour la démocratie », lequel représente notamment l'intérêt de couvrir un périmètre plus large, incluant des pays tiers candidats à l'adhésion.

2. Une feuille de route encore peu lisible pour le Centre européen pour la résilience démocratique

Inauguré en marge du Conseil des Affaires générales de février 2026, le Centre européen pour la résilience démocratique doit devenir une plateforme de coopération pour les États membres, réunissant les réseaux et les experts existants, afin d'apporter une réponse plus efficace face à la désinformation et aux ingérences étrangères. Il doit se déployer de manière graduelle, avec la participation des États membres volontaires et, à compter de juillet 2026, des pays candidats et candidats potentiels volontaires.

Le Centre européen pour la résilience démocratique **s'appuie sur un secrétariat dépendant directement de la Commission et notamment de sa Direction générale de la communication (DG COMM)**.

Ce rattachement à la DG COMM est jugé peu opérationnel par les rapporteurs, qui craignent que le bouclier ne demeure qu'une simple initiative de communication. En effet, pour mémoire, la DG COMM a pour mission d'informer les médias et les citoyens européens sur les activités de la Commission européenne, ses actions et ses objectifs de politiques publiques, ainsi que d'informer la Commission européenne de l'état de l'opinion publique. Il ne s'agit donc pas d'une direction opérationnelle rompue à l'exercice de missions de coordination des capacités nationales des États membres.

Dans les discussions interinstitutionnelles ayant précédé la communication sur le bouclier, la France souhaitait pourtant qu'il puisse être rattaché au Conseil de l'UE ou auprès du Service européen d'action extérieure (SEAE). La France considérerait en effet qu'un tel **rattachement SEAE aurait été pertinent**, compte tenu des thématiques concernées et des compétences limitées de la Commission européenne en matière de résilience démocratique et lutte contre les ingérences numériques étrangères. Les rapporteurs partagent cet avis et notent de surcroît que le *Rapid Alert System* (RAS), à savoir le réseau destiné au partage, entre États membres et institutions européennes, d'informations sur les campagnes de manipulation de l'information ciblant l'Union européenne et ses États membres, est piloté par le SEAE.

Auditionnée par les rapporteurs, le vendredi 26 juin 2026, la députée européenne **Nathalie Loiseau (France, Renew), présidente de la commission spéciale du Parlement européen sur le bouclier européen de la démocratie, dresse plusieurs constats de nature à poser question** quant à la mise en place effective du Centre européen pour la résilience démocratique :

- le rattachement au SEAE ou à la Commission européenne n'apparaît pas en soit soulever de difficulté. En revanche, il peut être déploré que deux lieux distincts coexistent désormais. Mme Nathalie Loiseau indique ainsi qu'« *un seul centre, peu importe auprès de qui il serait installé, garantirait une plus grande efficacité et une meilleure allocation des ressources* ». Elle souligne en outre qu'un rattachement à la Commission européenne suppose l'implication de plusieurs directions générales dans la mise en œuvre du bouclier, ce qui nécessite en outre un effort de coopération accru entre elles ;

- en dépit de leurs demandes formulées à la Commission européenne, **les députés européens n'ont pas pu réaliser de visite de terrain du Centre européen pour la résilience démocratique ;**

- le **centre serait composé de 5 à 6 personnes** dont on ne connaîtrait à ce stade pas l'organigramme précis.

Concernant son organisation, dans les réponses au questionnaire écrit transmis par les rapporteurs, reçues le 1^{er} juillet 2026, le Centre européen pour la résilience démocratique indique que « *le Centre dispose d'un secrétariat spécifique, composé de fonctionnaires et d'agents issus de différents services pertinents de la Commission européenne et du SEAE, ainsi que d'experts nationaux* ».

détachés par les États membres. Son organisation et ses modalités de travail ont été approuvées par le Secrétariat en étroite collaboration avec les États membres ». En contrepoint, **concernant ses effectifs, la réponse est plus floue** : « À ce stade, 15 collaborateurs contribuent aux activités du Centre à temps partiel. Depuis mi-juin 2026, deux membres du personnel y sont affectés à temps plein ; ils seront rejoints, dans les mois à venir, par 10 autres (dont quatre experts nationaux détachés) ». À ce stade, aucun équivalent temps plein (ETP) n'est formellement annoncé.

Selon les recherches des rapporteurs, le Centre serait actuellement dirigé par Oana Hriscu, Cheffe d'unité à la DG COMM au sein de la Commission, qui **assure le pilotage du secrétariat du Centre par intérim**. Une **offre d'emploi** pour ce poste, correspondant à un poste d'administrateur au grade AD 14 (soit un grade parmi les plus élevés pour l'entrée dans les grades d'administrateur des services au sein des institutions européennes) a été publiée par la Commission européenne avec une date limite de candidature fixée au 10 avril 2026, sans que l'on ne connaisse le résultat de cette procédure de recrutement¹.

Alors que le Centre a été préfiguré dès novembre 2025 et inauguré officiellement le 24 février 2026, l'absence d'une équipe de pilotage stabilisée fin juin 2026 pose question quant à sa capacité à animer effectivement une « communauté de réseaux » et à être « désormais pleinement opérationnel », selon les termes employés par le Centre lui-même dans ses réponses au questionnaire transmis par les rapporteurs.

3. Le Centre a-t-il abouti à des résultats tangibles à ce stade ?

Dans ses réponses au questionnaire transmis par les rapporteurs, le Secrétariat général des affaires européennes (SGAE)² indique qu'il n'y a pas eu d'exercices ou de simulations au niveau européen sous la coordination du Centre européen pour la résilience démocratique à ce stade, **à l'exception d'un exercice sur table** dans le cadre d'un atelier organisé le 27 mars 2026 sur la résilience démocratique auquel la France a participé. Cet atelier a réuni les États membres de l'Union européenne pour échanger sur les approches et mécanismes existants en matière de lutte contre les manipulations de l'information (LMI).

Le Secrétariat général des affaires européennes (SGAE) indique en outre que la France a commencé à participer aux premiers travaux de réflexion du Centre et que des réunions réunissant les points de contacts des États membres pour échanger sur les travaux du CERD (pour la France, le SGAE assure cette fonction) sont organisées régulièrement (*a priori*, selon une périodicité mensuelle).

¹ Offre d'emploi de « Conseiller principal au Centre européen pour la résilience démocratique (DG COMM) », référence COM/2026/10479/

La France a notamment lancé, grâce au soutien de VIGINUM, le **premier groupe de travail sur les « concepts, méthodologies et standards communs en matière de lutte contre la manipulation de l'information (LMI) »** qui aura pour objectif de cartographier et de réfléchir sur des définitions et approches communes en matière de détection et d'analyse au niveau de l'UE. Un autre groupe de travail, mené par la Suède, porte sur le renforcement des capacités, afin de permettre aux États membres de l'UE de bénéficier d'une formation aux enjeux de lutte contre les manipulations de l'information.

Par l'intermédiaire du Parlement suédois – le Riksdag –, les rapporteurs ont également obtenu communication d'éléments écrits de la part de l'Agence de défense psychologique suédoise, reçus le 30 juin 2026. Celle-ci a confirmé son implication dans la mise en œuvre du bouclier. L'Agence de défense psychologique suédoise a ainsi détaché depuis début 2026 une personne pour la mise en œuvre d'un groupe de travail sur la construction capacitaire. Elle organisera également un programme de formation des formateurs en matière d'INE. Ce programme intitulé *Train the Trainers* est destiné à tous les États membres et sera mis en œuvre en septembre et novembre 2026. Il permettra également de mettre en place un réseau d'anciens participants, favorisant ainsi la poursuite de la formation et de l'éducation.

Dans les réponses au questionnaire écrit transmis par les rapporteurs, reçues le 1^{er} juillet 2026, le Centre européen pour la résilience démocratique ajoute également au titre des « initiatives concrètes développées à l'initiative ou en plein accord avec les États membres », le **développement d'un guide pratique listant les règles et systèmes européens pertinents dans le contexte des processus électoraux** en soutien au renforcement de l'intégrité des élections.

Concernant les objectifs prioritaires du Centre pour les 12 prochains mois, le Centre européen pour la résilience démocratique indique qu'ils seront les suivants et précise que le programme de travail pour 2027 sera élaboré conjointement avec les États membres :

- mettre au point des outils pour garantir l'intégrité des scrutins et pour renforcer la résilience des sociétés face aux menaces de FIMI. À cet fin, le Centre procédera notamment au recensement des règles existantes pertinentes ainsi que des outils non contraignants susceptibles de contribuer à la prévention et la lutte contre les activités d'ingérence étrangères dans les processus électoraux ;
- élaborer un « *Blueprint FIMI* », soit un guide destiné à lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation, afin de soutenir l'état de préparation et le renforcement des capacités à l'échelle européenne ;

- lancer une plateforme collaborative consacrée aux parties prenantes, réunissant notamment des organisations de la société civile, des groupes de réflexion, des chercheurs et établissements universitaires, des « fact-checkers » ainsi que des acteurs des médias. Cette plateforme visera à diffuser les résultats de la recherche et à faciliter les échanges entre les États membres et les parties prenantes concernées au sein du Centre ;
- favoriser le renforcement des capacités et l'apprentissage mutuel, grâce au partage d'expertise et de bonnes pratiques, ainsi qu'à un soutien ciblé apporté par les États les plus avancés à ceux qui sont moins préparés, dans le but d'élever le niveau global de résilience à l'échelle européenne ;
- définir des modalités de coopération avec des pays candidats ou candidats potentiels à l'adhésion à l'UE dans le cadre du Centre, en vue de mettre en place une coopération mutuellement bénéfique.

C. TRANSFORMER L'ESSAI DU CENTRE EUROPÉEN POUR LA RÉSILIENCE DÉMOCRATIQUE : LA NÉCESSITÉ D'UN MANDAT CLAIR ET D'UN PORTAGE POLITIQUE FORT

En somme, au regard notamment du flou sur les effectifs réellement affectés au Centre, les rapporteurs craignent que le Centre européen pour la résilience démocratique ne demeure qu'une initiative de communication, celui-ci étant pour mémoire rattaché à la direction générale de la Commission européenne chargée de la communication interne et externe (DG COMM).

Aussi, en ligne avec, d'une part, les conclusions du rapport adopté le 23 juin 2026 par la commission spéciale du Parlement européen et, d'autre part, la position portée par la France dans une note libre (« non papier ») d'avril 2026 adressé aux institutions européennes et signé en commun avec la Suède, la Belgique, la Roumanie et la Lettonie, **les rapporteurs insistent sur la nécessité de doter le Centre européen pour la résilience démocratique d'un mandat clair, lui permettant des bonnes pratiques entre États membres et avec les institutions de l'Union européenne, dans le respect des compétences des États membres et notamment de leurs capacités de détection souveraines.**

Recommandation : doter le Centre européen pour la résilience démocratique d'un mandat clair, lui permettant des bonnes pratiques entre États membres et avec les institutions de l'Union européenne, dans le respect des compétences des États membres et notamment de leurs capacités de détection souveraines.

Nonobstant la question de son rattachement (SEAE ou Commission européenne), **les rapporteurs regrettent la superposition du Centre avec d'autres instruments déjà existants.** Ils appellent la Commission à éviter tout doublon et rationaliser les ressources et moyens dans un objectif d'efficience.

En particulier, le rôle du Centre devrait être strictement de coordonner les initiatives des États membres, sans empiéter sur leurs capacités opérationnelles, mais aussi de coordonner les activités de résilience engagées notamment au titre des mécanismes d'alerte précoce (*Rapid Alert System*) et des protocoles de crise prévus par le règlement sur les services numériques (DSA), pour contrer les campagnes de FIMI pendant les périodes électorales ou de crise.

À cet égard, les rapporteurs rappellent que le protocole de crise du DSA souffre de l'absence de lignes directrices précises, que la Commission européenne s'est engagée à publier afin de favoriser des procédures claires de coordination entre les autorités compétentes, et ainsi mieux faire face aux incidents majeurs et aux ingérences dans l'environnement informationnel.

Recommandation : assurer l'efficacité de la réponse européenne en matière de FIMI en évitant tous doublons organisationnels et procéduraux.

Recommandation : faire du Centre européen pour la résilience démocratique la structure de coordination des activités de résilience entreprises au titre des mécanismes d'alerte précoce (*Rapid Alert System*) et des protocoles de crise prévus par le règlement sur les services numériques (DSA), sans nuire aux capacités opérationnelles souveraines des États membres en matière d'investigation et de riposte informationnelle.

Par ailleurs, le rapport de la commission spéciale du Parlement européen adopté le 23 juin 2026, relève **le Centre européen pour la résilience démocratique ne peut pas aboutir à des résultats tangibles, sans budget spécifique.**

Les rapporteurs de la commission des affaires européennes partagent le constat d'un **manque d'opérationnalité flagrant**. Ils appellent donc à doter le centre d'une équipe compétente, d'un format adapté aux missions qui lui sont attribuées, en pleine cohérence avec l'ambition affichée par la proposition de CFP 2028-2034 de renforcer les moyens de défense et de sécurité de l'UE en réponse aux menaces venant de l'extérieur.

Recommandation : doter le Centre européen pour la résilience démocratique d'une équipe compétente, d'un format adapté aux missions qui lui sont attribuées.

Enfin, les rapporteurs appellent à la mise en œuvre d'exercices de **simulation collectifs regroupant tous les États membres, sous la coordination du Centre**. Pour rappel, dans sa résolution européenne sur le programme de travail de la Commission pour l'année 2026, le Sénat

demandait que le Centre pour la résilience démocratique s'appuie sur l'expérience de VIGINUM, entité la plus en avance en la matière dans l'UE.

À l'issue de leur visite de terrain dans les locaux de VIGINUM le 1^{er} juillet 2026, laquelle a confirmé l'excellence des services français en la matière, les rapporteurs rappellent la nécessité pour l'UE de se fonder sur les expériences des pays les plus avancés en la matière et de promouvoir la montée en capacité des États membres les moins avancés, de manière souveraine, tout en capitalisant sur les bonnes pratiques éprouvées.

Entendu lors d'une audition de la commission des affaires européennes le 27 novembre 2025, Marc-Antoine Brillant, chef de VIGINUM, se disait ainsi satisfait que le Centre dispose d'une mission de renforcement des capacités « *afin d'accompagner les États membres qui le souhaitent dans la création d'unités proches de VIGINUM* ». Il indiquait cependant que le Centre devait nécessairement être doté d'une mission de rationalisation des pratiques afin de les rendre interopérables¹. Lors de la visite sur site du 1^{er} juillet 2026, il a confirmé que **le Centre européen pour la résilience démocratique « prenait plutôt le bon chemin », à savoir celui d'un acteur de coordination des initiatives nationales, sans nuire aux capacités opérationnelles des États membres, et sachant capitaliser sur les expériences des pays les plus avancés comme la France et la Suède.**

Enfin, les rapporteurs soulignent l'impérieuse nécessité pour le Centre d'aider l'ensemble des acteurs de la lutte contre les ingérences numériques étrangères – chercheurs, spécialistes du renseignement en source ouverte (open source), agences nationales, journalistes, etc. – à **contribuer de concert à un écosystème unifié en promouvant des lignes directrices communes pour l'interopérabilité des données d'analyse.** Il en va de la capacité du croisement de ces données pour repérer des tendances en ligne ou des modes opératoires informationnels dans l'UE, sans égard des frontières nationales. Ainsi que le résume Mme Nathalie Loiseau, lors de son audition par les rapporteurs le 26 juillet 2026, il s'agit pour le Centre européen pour la résilience démocratique d'être en capacité de « *mettre en place des standard européens de telle sorte à ce que ces acteurs partagent la même grammaire* ».

De manière concrète, **le Centre doit en outre organiser des exercices de simulation conjoints aux États membres, pour améliorer leur capacité collective à répondre aux crises** et ne pas s'en tenir à l'animation d'échanges lors de réunions mêmes régulières, qui impliquent pour la France l'administration du SGAE et non pas directement les experts opérationnels de VIGINUM. Les rapporteurs considèrent que, pour transformer l'essai du CERD, ces exercices devraient porter des thématiques proposées par les États membres, selon un programme de travail dirigé ou à tout le moins, co-dirigé

¹ *Compte rendu de l'audition de M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) au secrétariat général de la défense et de la sécurité nationale (SGDSN) – 27 novembre 2025.*

avec eux par exemple au sein du Conseil de l'UE et en association des agences nationales spécialisées existantes ou à venir.

Recommandation : organiser, sous la coordination du Centre européen pour la résilience démocratique, des exercices de simulation regroupant les acteurs compétents des États membres, selon un programme de travail co-dirigé avec eux au sein du Conseil.

III. PASSER D'UN BOUCLIER DE PAPIER À UN BOUCLIER D'ACIER : COMMENT RENFORCER LE BOUCLIER EUROPÉEN DE LA DÉMOCRATIE ?

Outre le renforcement du Centre européen pour la démocratie, les rapporteurs considèrent que d'autres actions à la main des institutions européennes sont susceptibles de contribuer à la résilience des démocraties européennes. Celles-ci passent notamment par le renforcement du cadre juridique et des obligations incombant aux grandes plateformes numériques, qui jouent un rôle clé dans les dynamiques d'ingérences numériques étrangères.

A. RENFORCER LE CADRE JURIDIQUE ET LES OBLIGATIONS INCOMBANT AUX GRANDES PLATEFORMES

Concernant la lutte contre les ingérences numériques étrangères, notamment pendant les périodes électorales, les **plateformes en ligne jouent désormais un rôle majeur dans les mécanismes d'information et de formation de l'opinion publique.**

Néanmoins, compte tenu de leurs modalités de fonctionnement totalement opaque et de leurs modèles économiques qui mettent en avant le profit et la captation de l'attention au détriment de la sécurité des utilisateurs, **les plateformes en lignes, notamment les plus grandes, constituent également un vecteur de choix pour les acteurs malveillants dans leurs tentatives de manipulation de l'information.**

Les risques systémiques liés aux opérations de manipulations de l'information visant à influencer sur le débat public et compromettre l'intégrité des processus électoraux sont **aggravés par les possibilités offertes par les politiques de monétisation des plateformes, leurs fonctionnalités ou les nouvelles technologies, telles que les IA génératives.** Plusieurs personnes entendues par les rapporteurs considéraient ainsi que **les plateformes en ligne n'étaient plus seulement de simples vecteurs, mais des bien des acteurs à part entière de la manipulation de l'information en s'appuyant notamment de plus en plus sur les IA génératives ou en reprenant leur contenu.**

Dans ce contexte, le SGAE indique dans ses réponses au questionnaire écrit reçues le 23 juin 2026, que « la France demande à renforcer l’usage des outils existants face à ces nouvelles menaces. Elle appelle la Commission à pleinement mobiliser **ses prérogatives d’enquête, d’injonctions, de prononcé de mesures provisoires et de sanctions**, en vertu du DSA¹, position que les rapporteurs partagent pleinement (cf. infra).

Cet arsenal doit être exploité dans des délais compatibles avec la réalité des phénomènes de manipulation de l’information ». Le gouvernement français appelle également à la mise à jour, dès 2026, des **lignes directrices relatives à l’atténuation des risques systémiques menaçant les processus électoraux**, adoptées sur la base de l’article 35 du règlement sur les services numériques (DSA). Cet article prévoit en effet que « les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne mettent en place des mesures d’atténuation raisonnables, proportionnées et efficaces, adaptées aux risques systémiques spécifiques [...] en tenant compte en particulier de l’incidence de ces mesures sur les droits fondamentaux ».

Les rapporteurs partagent cette préoccupation et considèrent que la responsabilité des grandes plateformes doit être renforcée pour assurer la préservation des valeurs démocratiques et notamment, ne pas contribuer à nuire à la fiabilité des processus électoraux. Ils **demandent à nouveau la Commission européenne de « ne pas trembler ni transiger dans l’application de l’arsenal juridique novateur et ambitieux qu’elle a commencé à construire pour encadrer l’IA et le secteur numérique »**².

Recommandation : mettre à jour les lignes directrices relatives à l’atténuation des risques systémiques menaçant les processus électoraux, adoptées sur la base de l’article 35 du règlement sur les services numériques (DSA), en renforçant les exigences d’encadrement des systèmes et algorithmes de recommandation, la lutte contre les comptes et contenus inauthentiques, la transparence publicitaire en période électorale, le financement des contenus de manipulation de l’information, et des indicateurs quantitatifs sur la performance des outils mis en œuvre.

¹ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

² Résolution n° 144 (2025-2026) sur la proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2024/1689 et (UE) 2018/1139 en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l’intelligence artificielle (train de mesures omnibus numérique sur l’IA) - COM(2025) 836 final et sur la proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024 (règlement omnibus numérique) - COM(2025) 837 final, devenue résolution du Sénat le 19 juin 2026

Recommandation : publier sans délai des lignes directrices sur les registres publicitaires, prévues par l'article 39 du règlement sur les services numériques (DSA), afin d'assurer la transparence des plateformes en la matière, y compris hors période électorale.

En outre, le règlement sur les services numériques (DSA) prévoit la possibilité pour la Commission européenne d'adopter des **lignes directrices pour l'application de son article 39 relatif à la transparence des publicités en ligne**, afin d'en assurer une mise en œuvre effective et proportionnée. Le non-respect avéré ou potentiel par les très grandes plateformes en ligne et les très grands moteurs de recherche (aussi appelés « VLOPSEs ») des dispositions relatives à l'article 39 du DSA a des conséquences opérationnelles très concrètes pour le suivi de leurs obligations et l'identification de contenus manifestement illicites, notamment en période électorale.

Du point de vue des rapporteurs, il serait utile de préciser les exigences en matière de transparence des annonceurs ainsi que les fonctionnalités qui devraient être mises à disposition dans le cadre des registres publicitaires et des interfaces de programmation d'application (APIs¹) des plateformes.

Recommandation : dans les lignes directrices relatives à l'application de l'article 39 du règlement sur les services numériques (DSA), les exigences en matière de transparence des annonceurs ainsi que les fonctionnalités qui devraient être mises à disposition dans le cadre des registres publicitaires et des interfaces de programmation d'application (APIs²) des très grandes plateformes et des grands moteurs de recherche.

¹ Selon la CNIL, une API (application programming interface ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. Les API offrent de nombreuses possibilités, comme la portabilité des données, la mise en place de campagnes de courriels publicitaires, des programmes d'affiliation, l'intégration de fonctionnalités d'un site sur un autre ou l'open data. Elles peuvent être gratuites ou payantes.

² Selon la CNIL, une API (application programming interface ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. Les API offrent de nombreuses possibilités, comme la portabilité des données, la mise en place de campagnes de courriels publicitaires, des programmes d'affiliation, l'intégration de fonctionnalités d'un site sur un autre ou l'open data. Elles peuvent être gratuites ou payantes.

Cette mesure, également soutenue par le Gouvernement français dans ses positions au sein du Conseil, viendrait en outre renforcer l'application du règlement européen sur la publicité politique (TTPA), qui prévoit des exigences de transparence et de marquage pour les annonces publicitaires à caractère politique et l'obligation pour les VLOPSEs de les mettre à disposition dans les registres publicitaires, ainsi qu'une interdiction de toute publicité à caractère politique fournie à un parraineur extérieur à l'Union européenne à partir de trois voire six mois précédant une échéance électorale. Elle faciliterait incidemment le contrôle du respect, au niveau national, de l'article L. 52-1 du code électoral qui prévoit l'interdiction de toute publicité politique dans les six mois précédant un scrutin.

De même, entendue par les rapporteurs le 26 juin 2026, Mme Nathalie Loiseau, présidente de la commission spéciale du Parlement européen sur le bouclier européen de la démocratie, suggérerait que puisse **être demandé aux grandes plateformes de ne pas modifier leurs algorithmes en période de campagne électorale**, pour éviter tout soupçon de biais en faveur de certains partis politiques.

Mme Christine Dugoin Clément, chercheuse à la Chaire Risques de l'IAE Paris Sorbonne et à l'Observatoire de l'Intelligence artificielle de Paris 1- Panthéon Sorbonne, corroborait ces inquiétudes lors de son audition par les rapporteurs le 3 juillet 2026. Elle rappelait ainsi que les algorithmes de certains réseaux sociaux étaient susceptibles d'orienter les utilisateurs davantage vers certains contenus promouvant un parti ou un mouvement politique en particulier. Elle citait notamment l'étude menée par les ONG AI Forensics et Interface en 2024, qui indiquait que **l'algorithme du réseau TikTok aurait accru la visibilité du parti d'extrême-droite allemand *Alternative für Deutschland* (AfD)**, y compris lorsque les utilisateurs, en particulier les plus jeunes, recherchaient des informations sur d'autres formations politiques, à l'occasion des dernières élections européennes.

Quand bien même les grandes plateformes l'accepteraient, il semble difficile de vérifier matériellement l'absence de modification de leurs algorithmes, eu égard à leur faible transparence. Cette mesure est toutefois soutenue dans son principe par les rapporteurs de la commission des affaires européennes.

Recommandation : demander aux grandes plateformes numériques de ne pas modifier leurs algorithmes en période électorale afin d'éviter tout soupçon de biais en faveur de certains partis politiques.
--

Enfin, les rapporteurs soulignent que **les obligations existantes au titre du règlement sur les services numériques (DSA) incombent aux seules très grandes plateformes ou moteurs de recherche (VLOPSEs)**, dont le seuil est fixé à 45 millions d'utilisateurs actifs moyens par mois dans l'Union européenne, ce qui correspond à environ 10 % de la population de l'Union européenne. Au titre de ces obligations figurent notamment l'évaluation et la mitigation des risques systémiques découlant de leurs services. En application des articles 34 et 35 du DSA, ceux-ci incluent notamment la désinformation ou la manipulation électorale, la cyberviolence à l'égard des femmes ou les préjudices causés aux mineurs en ligne.

Toutefois, certains fournisseurs de services numériques continuent à échapper à l'application de ces règles et à la supervision directe de la Commission européenne. Les rapporteurs rappellent ainsi que le service de messagerie russe Telegram déclare depuis 2024 un nombre d'utilisateurs moyens inférieur à celui le faisant accéder à la catégorie des très grandes plateformes¹. Or des doutes sérieux existent quant aux mesures d'utilisateurs annoncés par Telegram, sans que la Commission européenne ou le superviseur national au titre du DSA (la Belgique s'agissant de ce service) n'ait pu à ce stade prouver qu'il dépassait ce seuil, fixé à 45 millions d'utilisateurs dans l'UE.

Or des modes opératoires d'ingérence numérique connus s'articulent autour de campagnes d'influence d'abord menées sur des plateformes comme Telegram avant d'apparaître sur d'autres réseaux sociaux tels TikTok ou autres.

La qualification des plateformes numériques en très grande plateforme est donc critique et constitue un corollaire essentiel à la lutte contre les ingérences numériques étrangères dans l'UE, car elle permet d'activer les dispositions existantes au titre du DSA. Les rapporteurs considèrent donc qu'il est essentiel d'affiner la méthodologie retenue pour qualifier un service numérique de « très grande plateforme », par exemple en substituant le seuil d'utilisateurs mensuels moyens par un faisceau d'indices attestant du caractère systémique des plateformes concernées (par exemple selon une formule comprenant différents seuils : seuil d'utilisateurs total moyen dans l'UE, seuil d'utilisateurs rapporté à la population de chaque État membre, seuil d'utilisateur mondial hors UE, etc.).

Recommandation : affiner la méthodologie pour qualifier un service numérique de « très grande plateforme » au titre du DSA, afin d'éviter que des services comme Telegram soient exempts des obligations de mitigation des risques systémiques en matière de lutte contre la désinformation et les ingérences électorales.

¹ Telegram avait déclaré 41 millions d'utilisateurs mensuels moyens en février 2024.

Recommandation : sans attendre une révision du DSA, au niveau de la Commission européenne, mettre en œuvre les moyens nécessaires pour réaliser les enquêtes nécessaires à attester le nombre d'utilisateurs réels de Telegram afin qu'il soit requalifié comme très grande plateforme et incombe au contrôle direct de la Commission européenne.

B. FAUT-IL RENFORCER LA DIMENSION COERCITIVE DU BOUCLIER ?

En première analyse, la dimension coercitive du bouclier semble également perfectible. Alors qu'il est censé s'appuyer sur la boîte à outils « FIMI¹ », comprenant des mesures restrictives contre les personnes et entités de pays tiers, « dont l'interdiction de diffuser le contenu des médias de propagande soutenus par le Kremlin », il est dans les faits essentiellement fondé sur le règlement sur les services numériques (DSA).

Le cadre d'application de la législation sur les services numériques

Applicable depuis février 2024 (mais dès quatre mois avant cette date s'agissant des très grandes plateformes en ligne et très grands moteurs de recherche en ligne), le règlement sur les services numériques (DSA) permet à la Commission européenne de déployer des moyens d'enquêtes en cas de soupçons d'infraction aux exigences prévues par ce texte, y compris en matière de mitigation des risques systémiques relatifs à la désinformation et à l'ingérence.

La Commission européenne peut subséquemment décider l'engagement d'une procédure à l'encontre des très grandes plateformes, permettant, après avoir entendu le fournisseur concerné, de prononcer, le cas échéant, une décision constatant un manquement, une décision infligeant des amendes ou une décision infligeant des astreintes.

Ces décisions peuvent donner lieu à des amendes qui sont déterminées par la nature, la gravité, la récurrence et la durée de l'infraction. Le montant de l'amende doit être proportionné et ne doit en aucun cas dépasser 6 % du chiffre d'affaires annuel global d'un fournisseur. La Commission européenne peut en outre ordonner aux plateformes de mettre en œuvre des mesures pour remédier à la violation dans un délai déterminé.

En dernier recours, si l'infraction persiste et cause un préjudice grave aux utilisateurs et entraîne des infractions pénales mettant en danger la vie ou la sécurité des personnes, la Commission peut demander la suspension temporaire du service, à l'issue d'une procédure spécifique.

¹ La boîte à outils relative aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger (FIMI) est un mécanisme à disposition de l'UE pour se protéger les processus démocratiques dans l'UE contre les effets préjudiciables des activités de manipulation de l'information et d'ingérence menées depuis l'étranger et de la désinformation.

La récente polémique sur le cas de la chroniqueuse russe Xenia Fedorova, ancienne responsable de RT, qui a fait régulièrement des apparitions dans certaines chaînes françaises, suscite des interrogations, dans la mesure où seuls la France et le Parlement européen ont réagi afin que des sanctions soient prises.

Entendue par les rapporteurs le 26 juin 2026, Mme Nathalie Loiseau, présidente de la commission spéciale du Parlement européen sur le bouclier européen de la démocratie, **rappelait que les outils coercitifs existent déjà au titre notamment du règlement sur les services numériques (DSA) et du règlement sur l'IA¹**, en cours de révision. En effet, des premières sanctions ont été mises en œuvre au titre du DSA, dont la première illustre l'effectivité du mécanisme : la décision de la Commission européenne en décembre 2025 de sanctionner la plateforme X à hauteur de 120 millions d'euros en raison de plusieurs manquements à ses obligations issues du règlement sur les services numériques et notamment la conception trompeuse des coches bleues (article 25 du RSN), le manque de transparence de son répertoire publicitaire (article 39 du RSN) ainsi que l'accès limité, voire impossible, à ses données publiques pour les chercheurs (article 40.12 du RSN). Comme le soulignait Mme Nathalie Loiseau, *« les cris d'Elon Musk montrent que cette sanction tapait là où cela fait mal »*.

Entendu par les rapporteurs le 30 juin 2026, M. Benoît Loutrel, membre du collège de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), considère également que le DSA est outil très puissant, qui a l'avantage de présenter un double niveau technique aux mains des régulateurs et politique, comme instrument de négociation et d'influence vis-à-vis des grandes plateformes. L'Arcom souligne que plusieurs dossiers d'enquêtes ouverts par la Commission européenne peuvent être considérés comme des succès du point de vue de la mise en conformité des plateformes, qui demeure l'objectif poursuivi, nonobstant les sanctions. À titre d'illustration, à l'issue de l'enquête ouverte le 19 février 2024 et des conclusions préliminaires de mai 2025 sur le réseau social TikTok, la Commission européenne a obtenu des engagements contraignants de la part de cette entreprise concernant la transparence en matière de publicité au titre du règlement sur les services numériques. TikTok a depuis mis en œuvre d'une manière jugée satisfaisante les obligations au titre du DSA, notamment de tenir un registre accessible et consultable des annonces publicitaires diffusées sur ses services. Or ces registres sont essentiels pour permettre aux régulateurs, aux chercheurs et à la société civile de détecter les publicités frauduleuses, les annonces pour des produits illégaux ou inadaptés à l'âge de

¹ 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) no 300/2008, (UE) no 167/2013, (UE) no 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 (règlement sur l'intelligence artificielle).

l'utilisateur en ligne, les annonces publicitaires fausses et les opérations de diffusion coordonnée d'informations, notamment dans un contexte électoral.

M. Benoît Loutrel considère en outre qu'il ne faut « *pas surestimer la petite irresponsabilité juridique* » qui a été reconnue aux plateformes numériques au titre du DSA, soulignant que « *le droit pénal doit continuer à jouer son rôle sans que le DSA n'y fasse obstacle* ». Sur ce plan, **la France se démarque en la matière avec deux parquets spécialisés dans le numérique et le cyber**, comme l'illustre la procédure contre Pavel Durov, fondateur et dirigeant de la messagerie instantanée et plateforme Telegram, à la suite de l'enquête préliminaire d'initiative diligentée par la section J3 (lutte contre la cybercriminalité – JUNALCO) du parquet de Paris, en août 2024, face à « *la quasi-totale absence de réponse de Telegram aux réquisitions judiciaires* », et s'agissant de plusieurs infractions pénales¹. Benoît Loutrel souligne en outre que les fournisseurs d'IA ne peuvent pas être considérés comme des hébergeurs ou des éditeurs car ils génèrent des contenus. Dès lors, si les services d'IA sont assimilables à des plateformes numériques, ils ne sauraient bénéficier d'aucune responsabilité réduite au titre du DSA.

Les rapporteurs considèrent ainsi que **si des outils coercitifs existent, il est impératif que ceux-ci soient utilisés utilement par la Commission européenne, dès lors que cela est nécessaire, pour veiller au respect de l'acquis numérique**. Il en relève d'une réelle volonté politique, dans le contexte d'une opposition devenue séculaire entre valeurs européennes (au premier chef desquelles, les valeurs démocratiques, objets du présent rapport) et compétitivité européenne, dans une dialectique opposant l'UE aux grandes plateformes numériques principalement américaines et chinoises.

Recommandation : appliquer sans trembler le cadre juridique ambitieux que l'UE a développé en matière numérique, la Commission européenne devant exercer pleinement ses prérogatives d'enquête, d'injonctions, de prononcé de mesures provisoires et de sanctions prévues par le règlement sur les services numériques (DSA), dès qu'elles sont nécessaires pour préserver l'espace informationnel numérique.

¹ Communiqué de presse de Laure BECCUAU, Procureure de la République, Tribunal judiciaire de Paris, 28 août 2024.

Entendu par les rapporteurs le 1^{er} juillet 2026 à l'occasion d'une visite sur site dans les locaux de VIGINUM, M. **Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM)** a indiqué qu'il considère que le DSA est « **un outil puissant, mais pas suffisamment utilisé** ». Rappelant que les très grandes plateformes hébergent tout ou partie du débat public, terreau de la démocratie, il a indiqué que la réglementation des plateformes constitue un enjeu de souveraineté pour les États membres, s'agissant des risques d'ingérence étrangère dans leurs processus démocratiques, notamment électoraux. Dès lors, dans ce contexte, la responsabilité des plateformes devrait être reconnue en tant « qu'hébergeurs du débat public ». Selon Marc-Antoine Brillant, on peut leur appliquer « *le principe du responsable mais pas coupable* ».

Les rapporteurs considèrent en effet que la responsabilité limitée des plateformes qui invoquent leur statut d'hébergeur et d'éditeur de contenus pour se soustraire à certaines du DSA n'est pas satisfaisante. Ils **appellent les institutions européennes, lors de la révision à venir du DSA, laquelle devrait s'ouvrir fin 2027, à envisager d'établir un véritable régime juridique de la responsabilité très grandes plateformes numériques, quel que soit leur statut d'hébergeur ou d'éditeur.**

Recommandation : envisager d'établir un régime juridique de la responsabilité des très grandes plateformes numériques quel que soit leur statut d'hébergeur ou d'éditeur, lors de la prochaine révision du DSA, prévue en 2027.

C. CONTRIBUER À RÉTABLIR UNE HIÉRARCHIE DE L'INFORMATION

La fiabilité de l'information est au cœur des questionnements sur la résilience démocratique. En effet, pour pouvoir prendre des décisions éclairées, les citoyens doivent pouvoir se reposer sur des informations vérifiées. En contrepoint, le pluralisme des médias et la liberté d'expression sont des valeurs démocratiques fondamentales. Dès lors, réglementer l'information est une opération délicate et il ne s'agit pas de se transformer en « ministère de la vérité » ou de « la post-vérité », selon les travaux de la délégation à la prospective du Sénat, sur le futur de notre rapport à l'autorité et à la vérité à l'horizon 2050¹.

¹ Rapport d'information n° 655 (2025-2026), déposé le 26 mai 2026 Le futur de notre rapport à l'autorité et à la vérité à l'horizon 2050, par Mmes Nadège HAVET, Christine LAVARDE et M. Jean-Jacques MICHAU.

Entendu par les rapporteurs le 30 juin 2026, M. Benoît Loutrel, membre du collège de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) a insisté sur l'urgence de rétablir une hiérarchie de l'information, dans un écosystème numérique dominé par « *des algorithmes qui ne savent pas faire la différence entre une vraie et une fausse information, entre une information produite par un journaliste qui respecte la Charte de Munich¹ et une information générée par IA* ». Selon l'Arcom, il est donc nécessaire de rehiérarchiser l'information afin de permettre de **distinguer les « médias éditorialisés » des « médias synthétiques »**, selon la formule utilisée par l'Arcom depuis 2024, qui désigne des ensembles de productions médiatiques générées par une ou deux personnes grâce à l'IA, « *à coup de prompts* ».

Selon le Baromètre du numérique de l'Arcom (édition 2026), 20 % des Français, et 54 % des moins de 25 ans, s'informent désormais principalement par les outils d'IA.

Lors de son audition le 3 juillet, la chercheuse Christine Dugoin-Clément soulignait par ailleurs le phénomène d'altération de l'IA à travers les outils d'« IA compagnon », soit des outils dotés d'interfaces en langage naturel qui offrent des réponses personnalisées à son utilisateur. Ces outils entraînent **une forte tendance anthropomorphique de l'IA**, qui font d'elle une **source d'information privilégiée, voire unique pour ses utilisateurs, et dont la fiabilité, l'objectivité et la crédibilité ne sont plus remises en cause**. Christine Dugoin-Clément préférait dès lors employer le terme **d'informatique augmentée** plutôt que celui d'intelligence artificielle, afin de mieux caractériser ce phénomène sur le plan sémantique.

Elle rappelait également **le danger que représentaient les recherches effectuées sur les moteurs s'appuyant sur l'IA**, susceptibles de renvoyer vers des informations – parfois elles-mêmes générées par l'IA – au contenu trompeur, du simple fait qu'elles sont accessibles depuis des sources considérées comme fiables par l'algorithme.

Eu égard aux limites inhérentes aux IA (informations tronquées, hallucinations, biais informationnels) et aux risques induits pour la formation éclairée des opinions dans le débat public, les rapporteurs considèrent qu'il est essentiel d'agir pour valoriser les médias éditorialisés, sans compromettre la liberté d'expression et le pluralisme. Pour ce faire, des solutions existent qu'elles consistent à soutenir le modèle économique des médias traditionnels ou à permettre de caractériser la différence entre un

¹ La Charte de déontologie de Munich ou Déclaration des devoirs et des droits des journalistes, signée le 24 novembre 1971 à Munich et adoptée par la Fédération européenne des journalistes, est une référence européenne concernant la déontologie du journalisme.

« média éditorialisé » et un « média synthétique », pour reprendre la partition proposée par l'Arcom.

En premier lieu, les rapporteurs encouragent à soutenir le renforcement des médias d'information, notamment locaux, à travers les divers instruments disponibles au sein du prochain cadre financier pluriannuel (Agora EU, Horizon Europe, Fonds européen de compétitivité, Global Europe etc.), afin de lutter contre les déserts d'information et la désinformation, de promouvoir la logique du *fact-checking* ou encore l'éducation aux médias.

Recommandation : soutenir le renforcement des médias d'information, notamment locaux, à travers les divers instruments disponibles au sein du prochain cadre financier pluriannuel (Agora EU, Horizon Europe, Fonds européen de compétitivité, Global Europe etc.), afin de lutter contre les déserts d'information et la désinformation.

Par ailleurs, les rapporteurs estiment que la Commission européenne doit aller plus loin dans le soutien à l'initiative de Reporters Sans Frontières (RSF) de certification du journalisme éditorialisé par un cabinet d'audit externe selon une norme ISO, appelée « *Journalism Trust Initiative (JTI)* ».

La certification Journalism Trust Initiative (JTI)

Promue par Reporters Sans Frontières (RSF), la certification Journalism Trust Initiative (JTI) consiste en une norme ISO, reconnue par un organisme de normalisation. Fondée sur 130 critères axés strictement sur le processus de qualité de l'entreprise médiatique et son mode de gouvernance et non pas sur le fond ou le contenu éditorial. La norme s'intéresse par exemple à la présence de journalistes humains, à l'existence d'une charte éditoriale ou encore à l'existence d'un siège social physique.

Selon le site web public de la norme, plus de 2450 médias à travers le monde ont déjà été labellisés, dont Le Monde, Le Figaro, l'AFP, etc.

Cette initiative est strictement destinée à distinguer les médias éditorialisés des médias synthétiques (générés ou alimentés par l'IA).

Les rapporteurs soulignent qu'une telle certification a un coût financier pour les médias traditionnels et qu'elle doit donc être assortie d'une contrepartie pour en valoriser l'investissement. Celle-ci pourrait prendre la forme d'une recommandation voire d'une obligation adressée aux grandes plateformes de **garantir la visibilité de contenus journalistiques qualifiés**, reconnues par leur appartenance à des médias certifiés JTI.

Recommandation : imposer aux très grandes plateformes de prendre en compte dans leurs algorithmes un objectif de visibilité prioritaire des contenus issus de médias certifiés de la norme *Journalism Trust Initiative* (JTI) ou d'une norme équivalente.

De même, les rapporteurs partagent la préoccupation d'un cadre juridique européen du numérique encourageant les annonceurs publicitaires à privilégier les sources d'informations fiables, en soutien aux médias de qualité. Ils seront attentifs à cet aspect dans l'analyse que pourra conduire la commission des affaires européennes du Sénat sur la future proposition de règlement sur l'équité numérique (ou *Digital Fairness Act* – DFA). Là encore, la norme JTI pourrait être utilisée comme critère de distinction entre média éditorialisé et médié synthétique voire inauthentique.

Recommandation : intégrer dans le cadre de régulation européen du numérique des mesures d'incitation à la publicité dans des médias fiables, afin de soutenir le modèle économique d'une presse de qualité.

En outre, comme le propose déjà la France dans ses positions soutenues au Conseil de l'UE, les rapporteurs défendent, dans le cadre de la **révision de la directive 2010/13 sur les services de médias audiovisuels (SMA)**, prévue à la fin de l'année 2026, de garantir la visibilité des médias dans l'environnement numérique et d'opérer un rééquilibrage des règles entre les services de médias audiovisuels et les plateformes de partage de vidéos. Ces mesures ont un objectif économique et démocratique, dans la mesure où le développement des plateformes génère des risques quant à l'accès des citoyens à des contenus d'information fiables et pluralistes et affaiblit le modèle économique des médias indépendants.

Par ailleurs, les rapporteurs soulignent **la nécessité de clarifier le régime juridique du droit d'auteur en matière d'IA**, comme cela avait été demandé dans l'avis politique de la commission des affaires européennes du 14 mai 2025 sur le code de bonnes pratiques en matière d'IA¹, précisant que des solutions juridiques ont été identifiées pour veiller à la rémunération des contenus culturels utilisés par les systèmes d'IA, en particulier la proposition de loi relative à l'instauration d'une présomption d'utilisation des contenus culturels par les fournisseurs d'intelligence artificielle², adoptée en première lecture par le Sénat le 8 avril 2026, que les deux rapporteurs ont soutenue.

¹https://www.senat.fr/fileadmin/Commissions/Affaires_europeennes/Fichiers/Avis_politiques/AP_co_de_bonnes_pratiques_ADOPTE_def.pdf

² Proposition de loi n° 220 (2025-2026) de Mme Laure DARCOS et plusieurs de ses collègues, déposé au Sénat le 12 décembre 2025.

Les rapporteurs estiment ainsi qu’une réflexion similaire doit être menée concernant l’utilisation par l’IA des contenus médiatiques. Ils notent que le directeur général de l’Alliance de la presse d’information générale (Apig), Pierre Pétillault, auditionné par la commission d’enquête du Sénat sur les zones grises de l’information, le 22 juin 2026, a souligné que *« ce ne serait pas absurde qu’il y ait la même réflexion en matière de presse »* que pour l’audiovisuel dans la directive sur les services de médias audiovisuels (SMA)¹.

Recommandation : engager une réflexion sur l’utilisation par l’IA des contenus médiatiques pour aboutir à une solution permettant la juste rémunération des médias traditionnels et la pérennité de leur modèle économique.

Enfin, il convient de rappeler que l’information européenne de qualité passe également par des actions concrètes comme le soutien direct à des médias européens. Ainsi, la France et l’Allemagne défendent le développement de plateformes audiovisuelles paneuropéennes, via notamment **l’eupréanisation de la chaîne Arte**².

Si la Commission européenne se montre réticente à soutenir ce projet au regard de la nécessité d’un appel à projets conforme aux règles de concurrence, les rapporteurs soutiennent ce projet dans son objectif, tout en reconnaissant qu’il nécessite des travaux préparatoires pour en assurer la faisabilité et la viabilité. Selon les rapporteurs, **l’émergence de médias paneuropéens capables de véhiculer des valeurs communes et des informations de qualité serait utile à la vitalité d’un écosystème médiatique éditorialisé**, fondé sur des journalistes formés.

Recommandation : soutenir le développement de plateformes audiovisuelles paneuropéennes multilingues, susceptibles d’offrir une information fiable et de qualité et fondées sur un accès libre, gratuit et facile pour le plus grand nombre dans l’UE, à partir du modèle de la chaîne Arte en cours d’eupréanisation.

¹ Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l’évolution des réalités du marché.

² Brève de Contexte, 27 mai 2026.

D. RENFORCER L'EFFICACITÉ DES MÉCANISMES D'ALERTE PRÉCOCE (RAPID ALERT SYSTEM) ET DES PROTOCOLES DE CRISE PRÉVUS PAR LE RÈGLEMENT SUR LES SERVICES NUMÉRIQUES (DSA)

Le *Rapid Alert System* (RAS) ; ou mécanisme d'alerte précoce en français, est un réseau européen piloté par le SEAE destiné au partage, entre États membres et institutions européennes, d'informations sur les campagnes de manipulation de l'information ciblant l'Union européenne et ses États membres. Il dispose d'une valeur ajoutée en associant les points de contact au sein des États membres et en coordonnant les réponses, notamment en matière de communication stratégique. Toutefois, il présente un faible intérêt purement opérationnel en matière de détection et d'analyse.

En ce qui concerne le protocole de crise prévu par le règlement sur les services numériques (DSA), l'article 36 du règlement met en place un mécanisme permettant à la Commission européenne et aux autorités nationales de recommander l'adoption de mesures spécifiques en cas de crise grave. Néanmoins, le seuil qualitatif de déclenchement de ces mécanismes est très élevé, afin de faire face à des menaces graves pour la sécurité publique ou la santé publique à l'échelle de plusieurs États membres.

Recommandation : réévaluer l'adéquation du seuil de déclenchement des mécanismes d'alerte précoce, pour assurer leur mise en œuvre effective en cas de menace pour la sécurité publique ou la santé publique à l'échelle de plusieurs États membres.

Les rapporteurs insistent sur le rôle que doit jouer le Centre européen pour la résilience démocratique en matière de coordination des activités menées au titre du RAS, qui est un outil pertinent de la résilience européenne face aux ingérences étrangères.

Ils **appellent à la mise en place d'une base de données « FIMI » au niveau du Centre**, afin de pouvoir identifier rapidement le niveau de la menace et déclencher le RAS, le cas échéant.

Recommandation : mettre en place au sein du Centre européen pour la résilience démocratique une base de données « FIMI », afin de pouvoir identifier rapidement le niveau de la menace et déclencher le mécanisme d'alerte précoce (RAS), le cas échéant.

E. AMÉLIORER LA LITTÉRATIE DES CITOYENS EN MATIÈRE NUMÉRIQUE

De manière générale, pour améliorer la résilience démocratique, les rapporteurs considèrent que **doit être renforcée la littératie du numérique pour les citoyens européens** – c’est à dire leur capacité à lire, comprendre et traiter l’information en ligne, sur les réseaux sociaux et l’information produite par l’IA –, afin de repérer plus facilement les contenus trompeurs ou inauthentiques.

Dans un espace informationnel désormais menacé à tous les niveaux, à l’échelle globale comme à l’échelle locale, chaque citoyen devrait **avoir les moyens de se défendre** face à ce que la chercheuse Christine Dugoin-Clément désigne comme une véritable guerre cognitive, voire une « guerre ontologique ». Elle indiquait ainsi que les opérations de déstabilisations sont **de moins en moins le seul fait de grandes puissances étatiques hostiles. Elles s’inscrivent dans un continuum** particulièrement diversifié, et organisé en plusieurs strates :

- des puissances étatiques plus ou moins désinhibées, à visage plus ou moins découvert ;
- des sociétés privées ou semi-privées très structurées, comme Wagner ou la *Social Design Agency* (SDA), avec lesquelles les puissances étatiques passent d’ailleurs des contrats ;
- d’autres acteurs privés de petite voire de très petite taille, dont l’activité consiste à cibler des contenus attractifs et générer des publications dérivées dont ils monétiseront les flux, sans se soucier de l’orientation ou de la partialité de ces contenus ;
- les influenceurs, et surtout les micro-influenceurs, qui n’ont que quelques centaines ou milliers d’abonnés qui leur accordent un très haut niveau de confiance ; ces petits groupes d’abonnés finissent par s’accumuler et se sédimenter jusqu’à former un phénomène de taches d’huile, générant alors un effet de masse.

Dans le contexte de cette guerre ontologique qui touche tous les cercles de citoyens, quelle que soit leur taille, **un effort particulier doit être réalisé en faveur d’une consolidation de la littératie du numérique.**

Avec son **Académie de la lutte contre les manipulations de l’information**, VIGINUM a engagé cette démarche au niveau national. Toutefois, les rapporteurs estiment qu’une initiative européenne doit être promue au titre du III^e pilier du bouclier européen de la démocratie, relatif au renforcement de la résilience de la société civile et citoyens. Celle-ci passe en réalité essentiellement par des financements aux acteurs de la société civile et de la recherche qui œuvre dans le domaine et qui sont des remparts de proximité pour la résilience citoyenne.

Le bouclier européen doit donc nécessairement être doté d'un budget propre, pour financer d'une part des initiatives de résilience conduites par la société civile et d'autre part, pour s'associer à l'effort indispensable de renforcement de la souveraineté industrielle et technologique de l'UE en matière numérique.

En conclusion, les rapporteurs insistent sur la responsabilité directe de l'UE pour réguler et encadrer le numérique, dans le sens de sa transparence et de son alignement avec les valeurs européennes. À ce titre, les rapporteurs **regrettent le report de trois mois des obligations de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA (article 50 du règlement sur l'IA), qui visent le marquage des contenus générés artificiellement, alors qu'aucun report n'était initialement envisagé pour ce point¹** dans le cadre des négociations portant sur la proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2024/1689 et (UE) 2018/1139 en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l'intelligence artificielle. Celui-ci, décidé à l'occasion du trilogue conclusif du 7 mai 2026 sur la révision du règlement sur l'IA, conduit à reporter au 2 novembre 2026 l'obligation de marquage des contenus générés par IA, au lieu du 2 août 2026. Cette mesure simple et de bon sens est un premier rempart contre la désinformation, puisqu'elle devrait contribuer à réduire l'effet des *deepfakes* ou hypertrucages générés par IA. Son report est un aveu d'échec que les rapporteurs déplorent et ils espèrent que la Commission continuera à être elle-même résiliente face aux tentatives d'ingérences menées par les géants américains du numérique.

¹ Voir le rapport d'information n° 626 (2025-2026) « Omnibus numérique européen : un risque pour la protection des droits numériques des citoyens, de Mmes Catherine Morin-Desailly et Karine Daniel, déposé le 13 mai 2026.

LISTE DES RECOMMANDATIONS

- **Recommandation n° 1** : mieux intégrer la prise en compte des menaces hybrides dans le bouclier européen de la démocratie ;
- **Recommandation n° 2** : renforcer par tous moyens la souveraineté numérique européenne, laquelle est un vecteur intrinsèque de résilience démocratique ;
- **Recommandation n° 3** : associer les pays candidats ou candidats potentiels aux travaux du Centre, uniquement dans la limite d'une analyse des risques géostratégiques posés par ces pays du point de vue de leur implication potentielle dans des stratégies d'INE ;
- **Recommandation n° 4** : développer les différentes activités prévues au titre du bouclier européen de la démocratie en lien étroit avec le Conseil de l'Europe, dans le cadre de son initiative en faveur d'un « Nouveau pacte pour la démocratie », lequel représente notamment l'intérêt de couvrir un périmètre plus large, incluant des pays tiers candidats à l'adhésion ;
- **Recommandation n° 5** : doter le Centre européen pour la résilience démocratique d'un mandat clair, lui permettant de coordonner le partage des bonnes pratiques entre États membres et avec les institutions de l'Union européenne, dans le respect des compétences des États membres et notamment de leurs capacités de détection souveraines ;
- **Recommandation n° 6** : assurer l'efficacité de la réponse européenne en matière de FIMI en évitant tous doublons organisationnels et procéduraux ;
- **Recommandation n° 7** : faire du Centre européen pour la résilience démocratique la structure de coordination des activités de résilience entreprises au titre des mécanismes d'alerte précoce (Rapid Alert System) et des protocoles de crise prévus par le règlement sur les services numériques (DSA), sans nuire aux capacités opérationnelles souveraines des États membres en matière d'investigation et de riposte informationnelle ;
- **Recommandation n° 8** : doter le Centre européen pour la résilience démocratique d'une équipe compétente, d'un format adapté aux missions qui lui sont attribuées ;
- **Recommandation n° 9** : organiser, sous la coordination du Centre européen pour la résilience démocratique, des exercices de simulation regroupant les acteurs compétents des États membres, selon un programme de travail co-dirigé avec eux au sein du Conseil ;

- **Recommandation n° 10** : inviter la Commission européenne à mettre à jour les lignes directrices relatives à l'atténuation des risques systémiques menaçant les processus électoraux, adoptées sur la base de l'article 35 du règlement sur les services numériques (DSA), en renforçant les exigences d'encadrement des systèmes et algorithmes de recommandation, la lutte contre les comptes et contenus inauthentiques, la transparence publicitaire en période électorale, le financement des contenus de manipulation de l'information, et des indicateurs quantitatifs sur la performance des outils mis en œuvre ;

- **Recommandation n° 11** : publier sans délai des lignes directrices sur les registres publicitaires, prévues par l'article 39 du règlement sur les services numériques (DSA), afin d'assurer la transparence des plateformes en la matière, y compris hors période électorale ;

- **Recommandation n° 12** : préciser, dans les lignes directrices relatives à l'application de l'article 39 du règlement sur les services numériques (DSA), les exigences en matière de transparence des annonceurs ainsi que les fonctionnalités qui devraient être mises à disposition dans le cadre des registres publicitaires et des interfaces de programmation d'application (APIs) des très grandes plateformes et des grands moteurs de recherche ;

- **Recommandation n° 13** : demander aux grandes plateformes numériques de ne pas modifier leurs algorithmes en période électorale afin d'éviter tout soupçon de biais en faveur de certains partis politiques ;

- **Recommandation n° 14** : affiner la méthodologie pour qualifier un service numérique de « très grande plateforme » au titre du DSA, afin d'éviter que des services comme Telegram soient exempts des obligations de mitigation des risques systémiques en matière de lutte contre la désinformation et les ingérences électorales ;

- **Recommandation n° 15** : sans attendre une révision du DSA, mettre en œuvre, au niveau de la Commission européenne, les moyens nécessaires pour réaliser les enquêtes permettant d'attester le nombre d'utilisateurs réels de Telegram afin qu'il soit requalifié comme très grande plateforme et incombe au contrôle direct de la Commission européenne ;

- **Recommandation n° 16** : appliquer sans trembler le cadre juridique ambitieux que l'UE a développé en matière numérique, la Commission européenne devant exercer pleinement ses prérogatives d'enquête, d'injonctions, de prononcé de mesures provisoires et de sanctions prévues par le règlement sur les services numériques (DSA), dès qu'elles sont nécessaires pour préserver l'espace informationnel numérique ;

- **Recommandation n° 17** : envisager la prochaine révision du règlement sur les services numériques (DSA), prévue en 2027, pour établir un régime juridique de la responsabilité très grandes plateformes numériques quel que soit leur statut d'hébergeur ou d'éditeur ;

- **Recommandation n° 18** : soutenir le renforcement des médias d'information, notamment locaux, à travers les divers instruments disponibles au sein du prochain cadre financier pluriannuel, afin de lutter contre les déserts d'information et la désinformation ;

- **Recommandation n° 19** : imposer aux très grandes plateformes de prendre en compte dans leurs algorithmes un objectif de visibilité prioritaire des contenus issus de médias certifiés de la norme *Journalism Trust Initiative* (JTI) ou d'une norme équivalente ;

- **Recommandation n° 20** : intégrer dans le cadre de régulation européen du numérique des mesures d'incitation à la publicité dans des médias fiables, afin de soutenir le modèle économique d'une presse de qualité ;

- **Recommandation n° 21** : engager une réflexion sur l'utilisation par l'IA des contenus médiatiques pour aboutir à une solution permettant la juste rémunération des médias traditionnels et la pérennité de leur modèle économique ;

- **Recommandation n° 22** : soutenir le développement de plateformes audiovisuelles paneuropéennes multilingues, susceptibles d'offrir une information fiable et de qualité et fondées sur un accès libre, gratuit et facile pour le plus grand nombre dans l'UE, à partir du modèle de la chaîne Arte en cours d'eupéanisation ;

- **Recommandation n° 23** : réévaluer l'adéquation du seuil de déclenchement des mécanismes d'alerte précoce, pour assurer leur mise en œuvre effective en cas de menace pour la sécurité publique ou la santé publique à l'échelle de plusieurs États membres ;

- **Recommandation n° 24** : mettre en place au sein du Centre européen pour la résilience démocratique une base de données « FIMI » au niveau du Centre, afin de pouvoir identifier rapidement le niveau de la menace et déclencher le RAS, le cas échéant.

EXAMEN EN COMMISSION

La commission des affaires européennes, réunie le mercredi 8 juillet 2026, a engagé le débat suivant :

M. Ronan Le Gleut, vice-président. – Nous en venons maintenant au bouclier européen de la démocratie, présenté le 12 novembre 2025, sous forme d’une communication conjointe, par la Commission européenne et la haute représentante de l’Union européenne pour les affaires étrangères et la politique de sécurité.

Huit mois plus tard, les annonces de la Commission européenne trouvent-elles réellement des traductions concrètes ? Comment s’articulent-elles avec les initiatives déjà prises par les États membres, en particulier la France ?

Je cède la parole à nos collègues Didier Marie et Catherine Morin-Desailly pour qu’ils puissent nous éclairer sur ce sujet et nous présenter leur proposition d’avis politique, qui reprend les principales recommandations formulées dans le projet de rapport.

M. Didier Marie, rapporteur. – C’est un sujet qui me tient à cœur dont nous allons vous parler aujourd’hui : celui de la résilience démocratique.

Alors que l’Union européenne s’est construite autour d’un socle de valeurs communes et notamment des piliers de la démocratie que sont le pluralisme et la liberté d’expression, ces valeurs sont aujourd’hui contrariées, voire combattues.

Dans un monde de plus en plus numérisé, il devient difficile de distinguer vraie et fausse information. Les manipulations de l’information opérées par des puissances étrangères ou des acteurs privés malveillants se multiplient et ciblent les institutions démocratiques.

Les ingérences numériques étrangères ciblent surtout de manière accrue les processus électoraux, aux fins de déstabilisation des institutions démocratiques. Outre les exemples européens récents fortement médiatisés, telles les ingérences russes à l’occasion de l’élection présidentielle en Roumanie en 2024, ou plus récemment lors des élections législatives moldaves en septembre 2025, la menace apparaît d’ores et déjà matérialisée en France, comme le démontre un récent rapport du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

Ainsi, quatre ingérences numériques étrangères ciblant spécifiquement les élections municipales françaises des 15 et 22 mars derniers ont été détectées et caractérisées par Viginum. Deux de ces ingérences numériques étrangères sont attribuables à des modes opératoires informationnels pro-russes, pour lesquels Viginum précise qu’ils sont connus et ont déjà mené des activités numériques malveillantes contre la France par

le passé. La troisième a été conduite au moyen d'un nouveau mode opératoire informationnel impliquant un acteur non étatique localisé au Vietnam, à des fins lucratives. Elle reposait sur la monétisation publicitaire d'actifs numériques, administrés dans le cadre de cette ingérence numérique étrangère. Plusieurs des experts que nous avons auditionnés nous ont d'ailleurs manifesté leur inquiétude quant à l'instrumentalisation de certaines fonctionnalités des plateformes et des réseaux sociaux, aux fins de manipulation de l'information voire d'ingérence. C'est notamment vrai des outils de micropaiement et de monétisation publicitaire des plateformes numériques. La dernière ingérence identifiée par Viginum relativement aux élections municipales ciblait plusieurs candidats du parti La France Insoumise (LFI) et impliquait un acteur non étatique localisé en Israël.

Si l'effet réel des campagnes d'ingérence numérique étrangères détectées par Viginum doit être relativisé s'agissant des élections municipales de 2026, elles démontrent toutefois la tendance à l'accroissement des menaces numériques qui pèsent sur notre société et leurs conséquences potentielles pour les institutions démocratiques, auxquelles s'ajoutent des défis structurels en France, comme dans d'autres pays européens : la montée des extrémismes, la polarisation du débat public et l'érosion de la confiance envers les institutions démocratiques.

C'est dans ce contexte que la Commission européenne a présenté conjointement avec la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, une communication intitulée « bouclier européen de la démocratie », le 12 novembre 2025. Cette initiative entend apporter une réponse européenne coordonnée aux défis croissants que présentent la désinformation et les autres tentatives de manipulations de l'information, notamment en ligne.

À ce jour, l'espace public informationnel est en effet articulé autour de l'activité de quelques très grandes plateformes numériques, dont les modèles économiques et les algorithmes, particulièrement opaques, conduisent à brouiller la frontière entre vraie et fausse information.

Dans cet écosystème informationnel complexe, des puissances étrangères ou des entités privées malveillantes instrumentalisent les outils numériques pour conduire des activités d'ingérence.

Or les ingérences numériques étrangères vont croissant. Elles s'inscrivent de plus en plus dans de stratégies hybrides : numériques d'abord, mais mêlant parfois d'autres leviers d'attaque, en ciblant les infrastructures critiques tels les câbles sous-marins, les ports, les aéroports ou encore les réseaux énergétiques.

Ces stratégies hybrides exploitent largement les vulnérabilités numériques : utilisation de l'intelligence artificielle (IA), hypertrucages, ou *deepfakes* en anglais, autres contenus synthétiques, ou encore recours à des comptes fictifs ou inauthentiques sur les réseaux sociaux. J'ajoute que l'effet d'amplification algorithmique joue à plein s'agissant des contenus polarisants, qui se trouvent mis en avant et plus visibles que des informations fiables.

À cela s'ajoute le recul des médias traditionnels éditorialisés, dont les modèles économiques sont aujourd'hui une nouvelle fois mis à mal avec le développement de l'IA.

Il est devenu très facile de créer un « vrai » faux média en ligne grâce à l'IA. Une ou deux personnes suffisent alors à alimenter un site web de pseudo-informations générées artificiellement, sans contrôle de la ligne éditoriale ou pire, aux fins de désinformation. En 2025, par exemple, un site dénommé « Var Actu » a été agréé par la Commission paritaire des publications et agences de presse (CPPAP). Ce statut lui a permis de bénéficier du régime économique et juridique de la presse pendant plusieurs mois malgré son origine artificielle et la génération de ses articles par l'IA.

On est donc confronté à un double problème : d'une part, la perte de la hiérarchie traditionnelle de l'information, d'autre part, un espace informationnel numérique qui rend possible voire facilite les ingérences étrangères.

Dès lors, le bouclier européen de la démocratie apparaît comme une réponse bienvenue pour lutter contre le développement des manipulations et ingérences de l'information étrangère, que l'on résume sous l'acronyme Fimi, pour *Foreign Information Manipulation and Interference*.

Toutefois, malheureusement, la solidité de ce bouclier résiste mal à notre analyse.

La Commission européenne a beau jeu de le décrire comme « une série de mesures concrètes destinées à renforcer la position de démocraties fortes et résilientes et à protéger et promouvoir ces dernières dans l'ensemble de l'Union européenne ». En réalité, la plupart de ces mesures sont peu concrètes. La Commission européenne s'engage surtout à renforcer les structures volontaires de coordination et de partage d'informations, à élaborer des lignes directrices non contraignantes ou à renforcer la législation existante, sans qu'un calendrier précis soit proposé. Or l'urgence est là.

Au titre des mesures concrètes se trouve en réalité exclusivement la création d'un Centre européen pour la résilience démocratique. Plusieurs initiatives de ce type existent déjà sur le plan national : la France avec Viginum, la Suède ou encore l'Allemagne disposent déjà de structures chargées de caractériser les tentatives d'ingérences numériques étrangères voire de riposter ; mais aussi sur le plan international – notamment avec l'Otan. En parallèle, le Conseil de l'Europe développe également son propre arsenal contre les Fimi, avec son projet de Nouveau pacte démocratique. En

tant que membre de la délégation sénatoriale à l'Assemblée parlementaire du Conseil de l'Europe, je m'intéresse à la mise en œuvre de ce Nouveau pacte démocratique, mais je m'interroge beaucoup sur son articulation avec le bouclier européen de la démocratie. Je plaide à ce titre pour que cet outil de l'Europe des 46 soit bien complémentaire de celui de l'Europe des 27.

Ce Centre européen pour la résilience démocratique doit pouvoir trouver sa place, tout en respectant très strictement les principes de subsidiarité et de proportionnalité. Il pourrait utilement jouer un rôle de coordinateur des initiatives des États membres voire de catalyseur pour les États les moins avancés, tout en veillant à ne pas nuire à leurs capacités souveraines.

Toutefois, pour ne pas risquer de devenir une autre plateforme ou un centre parmi d'autres, ce qui aggraverait la fragmentation des efforts européens et réduirait l'efficacité des outils existants, il ne peut exister que sur la base d'un mandat clair axé sur la seule coordination des initiatives nationales, la coopération en vue du partage des bonnes pratiques et du renforcement des capacités des pays les moins avancés en la matière.

Or il n'existe aujourd'hui qu'une feuille de route floue et le Centre ne dispose à ce stade pas de moyens réels.

En effet, inauguré en marge du Conseil des affaires générales de février 2026, il est directement adossé à la direction générale de la communication (DG COMM) de la Commission européenne.

Dans notre résolution sur le programme de travail de la Commission européenne pour 2026, avec Jean-François Rapin, nous considérons pour mémoire qu'il aurait plutôt dû être rattaché au service européen pour l'action extérieure – le SEAE.

Aujourd'hui, ce n'est plus tant la question de son rattachement qui se pose que celle de ses moyens. Après presque six mois d'existence, le Centre ne s'appuie que sur très peu de personnes, qui ne lui sont pas totalement affectées et selon un organigramme flou. Le pilotage du secrétariat est assuré par intérim et on ne sait pas encore si l'offre d'emploi publiée par la Commission européenne, avec une date limite de candidature fixée au 10 avril 2026, a abouti.

Sur le plan opérationnel, peu de réalisations concrètes sont à noter. De premiers groupes de travail ont été lancés. Ils sont pilotés par la France et la Suède. C'est une bonne chose et cela tend à nous rassurer sur le rôle du Centre européen de résilience démocratique.

Afin d'éviter que ce centre ne demeure qu'une initiative de communication, il est impératif de le doter d'un mandat clair, juridiquement contraignant, lui permettant un partage de bonnes pratiques entre États membres et avec les institutions de l'Union européenne, dans le respect des compétences des États membres et notamment de leurs capacités de détection

souveraines. Cet avis est d'ailleurs partagé par l'excellent rapport de M. Tomas Tobé pour la commission spéciale du Parlement européen sur le bouclier européen de la démocratie, présidée par Mme Nathalie Loiseau, que nous avons auditionnée.

Nous considérons par ailleurs qu'il faut faire de ce centre la structure de coordination des activités de résilience entreprises au titre des mécanismes d'alerte précoce et des protocoles de crise prévus par le règlement sur les services numériques, le *Digital Services Act* (DSA), sans nuire aux capacités opérationnelles souveraines des États membres en matière d'investigation et de riposte informationnelle.

De manière concrète, le centre doit en outre pouvoir organiser des exercices de simulation conjoints aux États membres, pour améliorer leur capacité collective à répondre aux crises transfrontalières.

Pour conclure au sujet du Centre européen pour la résilience démocratique, alors qu'il est la principale mesure du bouclier européen de la démocratie, six mois après sa création, force est de constater que sa mise en œuvre reste balbutiante et sa feuille de route pour l'avenir, très imprécise.

Alors que nous avons par principe salué cette création, elle n'est à ce jour pas à la hauteur des enjeux. Il lui faut des moyens et des orientations claires pour partager les bonnes pratiques et tirer vers le haut les États membres qui sont encore à la traîne.

Mme Catherine Morin-Desailly, rapporteure. – Didier Marie l'a bien résumé : le bouclier européen de la démocratie reste très fragile ; il s'agit de transformer sans délai ce bouclier de papier en un bouclier d'acier.

Au vu des enjeux très réels sur le plan des valeurs européennes, pour la liberté, le pluralisme et la transparence du débat démocratique, il nous apparaît plus que jamais nécessaire d'appliquer pleinement, d'une part, et de renforcer, d'autre part, le cadre réglementaire imposé aux grandes plateformes numériques et grands moteurs de recherche : règlement sur les marchés numériques (*Digital Markets Act* – DMA), DSA et règlement sur l'intelligence artificielle (*AI Act*).

En effet, aujourd'hui, dans notre monde, ce sont cinq plateformes ou presque qui décident de tout. Elles décident par leurs algorithmes les contenus que nous pouvons voir ; elles trient pour nous les informations voire les orientent, sans distinguer le vrai du faux.

Or dans un monde de plus en plus numérisé, la lutte contre les ingérences étrangères relève en grande partie de la régulation des plateformes numériques, des moteurs de recherche, mais aussi, de façon croissante, des services d'intelligence artificielle.

Selon le Baromètre du numérique de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), en 2026, 20 % des Français, et 54 % des moins de 25 ans, s'informent désormais principalement par les outils d'IA. Dès lors, comme nous l'avions déjà dit il y a plus d'un an avec Florence Blatrix Contat, nous devons appeler la Commission européenne à appliquer sans trembler l'arsenal juridique novateur et ambitieux qu'elle a commencé à construire pour encadrer l'intelligence artificielle et le secteur numérique.

Outre le renforcement du Centre européen pour la démocratie, le renforcement du bouclier passe par le renforcement du cadre juridique et des obligations incombant aux grandes plateformes numériques, qui jouent un rôle clé dans les dynamiques d'ingérences numériques étrangères. Pendant un temps, se cachant derrière les statuts d'hébergeurs ou d'éditeurs, elles ont voulu nous faire croire qu'elles n'étaient que des vecteurs de ces ingérences. Or il est clair aujourd'hui qu'elles peuvent être considérées comme des acteurs de désinformation, voire d'ingérence, tout comme les services d'intelligence artificielle.

Je regrette que le règlement sur les services numériques de 2022 ait octroyé l'irresponsabilité aux plateformes. Sa révision devrait s'ouvrir en 2027, et le risque qu'il soit assoupli plutôt que durci, comme il devrait l'être, n'est pas nul.

Pourtant, je crois sincèrement que nous devons plaider pour la création d'un régime juridique de la responsabilité des plateformes numériques. Nous le disons depuis des années !

Plusieurs éléments du DSA peuvent par ailleurs être renforcés. Ce matin, nos collègues de la commission de la culture rendaient un rapport sur les zones grises de l'information. Ils ont formulé les mêmes préoccupations et recommandations que nous. Par exemple, une interdiction doit être faite aux grandes plateformes de modifier leurs algorithmes en période de campagne électorale, pour éviter tout soupçon de biais en faveur de certains partis politiques. Cela suppose la transparence totale des algorithmes.

En outre, sans attendre la révision du DSA, la Commission européenne doit mettre à jour sans délai les lignes directrices relatives à l'atténuation des risques systémiques menaçant les processus électoraux, adoptées sur la base de l'article 35 du DSA. Il s'agit notamment de renforcer les exigences d'encadrement des systèmes et algorithmes de recommandation, la lutte contre les comptes et contenus inauthentiques, la transparence publicitaire en période électorale, le financement des contenus de manipulation de l'information, et des indicateurs quantitatifs sur la performance des outils mis en œuvre. De même, la Commission doit publier sans délai des lignes directrices sur les registres publicitaires, prévues par l'article 39 du DSA, afin d'assurer la transparence des plateformes en la matière, y compris hors période électorale.

Trop d'éléments de type lignes directrices sont en retard ou pas à jour. Or ces éléments sont indispensables aux régulateurs nationaux pour exercer leurs contrôles. Si la Commission européenne souhaite continuer de s'attribuer des prérogatives d'actes délégués ou d'édications de normes de droit souple, il faut qu'elle soit à la hauteur des enjeux.

Un autre exemple en ce sens est celui du service de messagerie Telegram, qui déclare depuis 2024 un nombre d'utilisateurs moyens inférieur à celui le faisant accéder à la catégorie des très grandes plateformes, lui permettant donc d'échapper au contrôle direct de la Commission européenne et aux obligations en matière d'atténuation des risques systémiques. Or il y a fort à parier que Telegram dépasse depuis longtemps ce seuil critique de 45 millions d'utilisateurs actifs moyens par mois dans l'Union européenne.

Il nous apparaît donc indispensable que la Commission européenne mette en œuvre les moyens utiles pour réaliser les enquêtes nécessaires en vue d'attester le nombre d'utilisateurs réels de Telegram afin qu'il soit requalifié comme très grande plateforme et soit enfin soumis au contrôle direct de la Commission européenne.

Enfin, je souhaite conclure par un constat simple : la souveraineté numérique européenne est un vecteur intrinsèque de résilience démocratique. Au-delà du bouclier européen pour la démocratie, il est donc primordial d'investir pour notre indépendance numérique et notre souveraineté industrielle. Sans elles, nous sommes voués à être une colonie du monde numérique – nous sommes les vassaux de ces Big Tech –, avec tous les risques que cela comporte pour la préservation de nos modes de vie, de nos valeurs et de nos institutions démocratiques. Il y a plus qu'urgence !

M. Didier Marie, rapporteur. – Je voudrais vous parler de deux derniers éléments qui nous apparaissent essentiels à la résilience démocratique : des médias libres, indépendants, pluralistes, d'une part, et des citoyens éclairés, d'autre part.

La frontière entre les médias éditorialisés, autour de plusieurs journalistes et d'une charte éditoriale, et les médias synthétiques, biberonnés à l'IA, s'estompe. Or la qualité et la fiabilité de l'information sont des prérequis à un débat public fonctionnel.

En premier lieu, nous encourageons donc l'Union européenne à soutenir le renforcement des médias d'information, notamment locaux, à travers les divers instruments disponibles au sein du prochain cadre financier pluriannuel, afin de lutter contre les déserts d'information et la désinformation, de promouvoir la logique du *fact-checking*, c'est-à-dire la vérification des faits, ou encore l'éducation aux médias.

Par ailleurs, nous considérons que des solutions neutres existent pour distinguer un vrai média d'un faux média. C'est le cas de la certification *Journalism Trust Initiative* (JTI), promue par Reporters sans frontières (RSF), qui consiste en une norme ISO, reconnue par un organisme de normalisation.

Cette norme n'est pas fondée sur la qualité du journalisme ou la ligne éditoriale – on est loin d'un ministère de la vérité – mais elle est fondée sur le processus de qualité de l'entreprise médiatique et son mode de gouvernance.

Cette initiative qui a fait ses preuves doit être davantage valorisée. Elle a un coût financier pour les médias traditionnels, qui doivent suivre le processus de certification. Il est donc logique qu'elle puisse être assortie d'une contrepartie pour en valoriser l'investissement. Celle-ci pourrait prendre la forme d'une recommandation voire d'une obligation adressée aux grandes plateformes de garantir la visibilité de contenus journalistiques qualifiés, reconnues par leur appartenance à des médias certifiés JTI.

De même, nous partageons la préoccupation d'un cadre juridique européen du numérique encourageant les annonceurs publicitaires à privilégier les sources d'informations fiables, en soutien aux médias de qualité.

Il me paraît donc important que notre commission se montre attentive à cet aspect dans l'analyse du futur règlement sur l'équité numérique. Là encore, la norme JTI pourrait être utilisée comme critère de distinction entre média éditorialisé et médié synthétique voire inauthentique.

Enfin, nous considérons qu'être Européens, c'est aussi partager une culture informationnelle commune et qu'il faut donc soutenir le développement de plateformes audiovisuelles paneuropéennes multilingues, susceptibles d'offrir une information fiable et de qualité et fondées sur un accès libre, gratuit et facile pour le plus grand nombre dans l'Union européenne, à partir du modèle de la chaîne Arte en cours d'eupéanisation.

La résilience démocratique passe par les citoyens eux-mêmes. Dans le rapport, nous proposons d'agir au niveau européen pour améliorer la littératie de tous les citoyens européens en matière de numérique, d'IA et de détection des dérives qu'ils sont capables de produire. Viginum est en train de mettre en place une académie de la lutte contre les manipulations de l'information destinée au grand public. Une démarche complémentaire doit exister au niveau européen, au titre du troisième pilier du bouclier européen de la démocratie, relatif au renforcement de la résilience de la société civile et des citoyens. Une telle initiative passe en réalité essentiellement par des financements aux acteurs de la société civile et de la recherche qui œuvrent dans le domaine et qui sont des remparts de proximité pour la résilience citoyenne.

M. Ronan Le Gleut, vice-président. – Je vous remercie pour ce remarquable rapport.

Mme Pascale Gruny. – Combien d'agents sont-ils affectés à ces contrôles, à l'échelon européen comme national ? Ce phénomène représente un fléau pour nos jeunes notamment. Quand on entend que l'IA aidera les électeurs à voter, c'est inquiétant !

M. Louis-Jean de Nicolaÿ. – Comment garantir la sécurité des médias régionaux ?

Mme Audrey Linkenheld. – Merci pour cette présentation. Je me félicite de votre proposition de développer des plateformes audiovisuelles paneuropéennes multilingues. Nous avons assisté, avec quelques collègues, à une présentation de l'équipe d'Arte sur ses ambitions. J'y souscris personnellement, mais je sais que d'autres les regardent d'un œil plus critique. La ligne éditoriale d'Arte serait trop ouverte, trop accueillante, trop diverse... Bravo pour cette recommandation !

Mme Catherine Morin-Desailly, rapporteur. – S'agissant des plateformes paneuropéennes, Arte est un modèle, qui a été sollicité par différents pays, tels que la Moldavie qui subit des ingérences russes, mais manque de moyens. Il faut encourager l'eupéanisation d'Arte.

Notre audiovisuel public est à la traîne : c'est le dernier à ne pas avoir connu de réforme structurelle. Désormais, tout est en replay. C'est pourquoi il faut aller vers une plateforme paneuropéenne de nos audiovisuels publics, d'abord pour une question de moyens. Tout coûte cher ! Moi qui ai siégé au conseil d'administration de France Télévisions, je n'ai pas arrêté de plaider pour une telle plateforme, qui offrirait une masse critique face aux géants tels que Netflix ou Amazon Prime. La Commission doit aider nos audiovisuels publics européens, qui sont des marques qui doivent survivre.

La presse régionale subit les mêmes aléas que la presse nationale. Elle dépend d'un écosystème de plateformes qui éditorialisent ou diffusent son contenu. Tout simplement, si l'on ne travaille pas sur les modèles économiques corrélés à ces plateformes, c'est-à-dire les droits d'auteur et les droits voisins, notre presse mourra. Nous sommes à la croisée des chemins. Si la presse ne bénéficie pas de la valeur ajoutée de ce qui circule sur les plateformes, elle s'appauvrira et disparaîtra. La presse réalisée par des professionnels doit être labellisée, pour que l'on puisse l'identifier, dans ce magma d'informations.

Toutes nos autorités de régulation doivent assumer un monceau de missions ; elles sont à la peine. Elles nous alertent. Il leur faut des développeurs, des spécialistes du traitement de données. Cette question des moyens est transnationale.

Si le DSA ne s'applique pas comme il le devrait, c'est aussi parce que trop peu de moyens de la Commission européenne y sont dévolus.

Il ne faut pas se limiter à demander des moyens pour la régulation ; il faut aussi impulser une stratégie industrielle extrêmement puissante. Il faut travailler à des outils européens pour construire un système qui soit plus à notre main.

M. Didier Marie, rapporteur. – Nous avons interrogé Mme Nathalie Loiseau, présidente de la commission spéciale du Parlement européen, sur ce nouvel outil en place. Selon elle, entre cinq et six personnes seraient affectées à temps partiel au dispositif. La Commission dit qu'il y en aurait dix. En tout cas, nous n'avons pas d'organigramme. Mme Loiseau et les membres de la commission spéciale ont voulu visiter le centre et ne l'ont pas pu. C'est dire combien l'opacité règne. Il y a donc un problème de moyens, mais aussi de pilotage. Nous craignons que le rattachement à la DG COMM ne montre que ce n'est qu'une opération de communication. Pourtant, il y a urgence.

Le système français est plutôt bien organisé, avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) et Viginum, qui est une petite structure, d'une soixantaine d'équivalents temps plein (ETP), mais d'une très grande efficacité, avec des doctorants et des diplômés de bac+ 5. Si l'ensemble des pays européens parvenaient à se doter souverainement d'outils de cette nature, cela nous aiderait à avancer, mais il faut un outil de coordination européen, d'échange de bonnes pratiques et d'aide aux pays qui ne sont pas en capacité d'agir seuls.

Il y a un vrai problème de mutation du modèle économique de la presse régionale. Le marché de la publicité s'est effondré. Tous ces médias doivent passer au numérique. Certains ne le peuvent pas. Des journaux disparaissent. Il faut des moyens nationaux et européens.

S'agissant de la lutte contre les ingérences, on ne peut que regretter la baisse des moyens de France Médias Monde. La politique d'influence s'érode, faute de moyens. Il y a beaucoup à faire à l'échelle européenne et à l'échelle nationale. C'est bien de passer le rabot budgétaire, mais il faut faire attention à ses conséquences.

La commission adopte, à l'unanimité, le rapport d'information et en autorise la publication.

La commission adopte, à l'unanimité, l'avis politique disponible en ligne sur le site du Sénat qui sera adressé à la Commission européenne.

LISTE DES PERSONNES ENTENDUES

Jeudi 27 novembre 2025

- *M. Marc-Antoine BRILLANT*, chef du service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM), entendu en audition plénière devant les membres de la commission des affaires européennes

Vendredi 26 juin 2026

- *Mme Nathalie LOISEAU*, députée européenne (Renew France), présidente de la commission spéciale sur le bouclier européen de la démocratie

Mardi 30 juin 2026

Autorité de régulation de la communication audiovisuelle et numérique (Arcom) :

- *M. Benoit LOUTREL*, membre du collège de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom)
- *M. Ivaylo SAVOV*, chargé de missions affaires européennes, Autorité de régulation de la communication audiovisuelle et numérique (Arcom)

Vendredi 3 juillet 2026

- *Mme Christine DUGOIN-CLÉMENT*, chercheuse, Chaire Risques de l'IAE Paris-Sorbonne, Observatoire de l'Intelligence Artificielle de Paris 1 Panthéon-Sorbonne, centre de recherche des écoles de Saint Cyr Coëtquidan (CREC) et centre de recherche de l'École des officiers de la Gendarmerie nationale (CREOGN)

LISTE DES CONTRIBUTIONS ÉCRITES

- Secrétariat général des affaires européennes (SGAE), reçue le 23 juin 2026
- Centre européen pour la résilience démocratique, DG COMM, Commission européenne, reçue le 1^{er} juillet 2026
- Agence de défense psychologique suédoise, reçue le 30 juin 2026

DÉPLACEMENT

Mercredi 1^{er} juillet 2026

- Déplacement dans les locaux du service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM), Paris