



Bruxelles, le 26.4.2018
COM(2018) 236 final

**COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU
CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ
DES RÉGIONS**

Lutter contre la désinformation en ligne: une approche européenne

1. INTRODUCTION

L'exposition des citoyens à la désinformation à grande échelle, y compris à des informations trompeuses ou absolument fausses, constitue un défi majeur pour l'Europe.

Nos sociétés démocratiques ouvertes dépendent du débat public. Celui-ci permet à des citoyens bien informés d'exprimer leur volonté par l'intermédiaire de processus politiques libres et équitables. Les médias ont toujours joué un rôle clé pour obliger les pouvoirs publics à rendre des comptes et pour fournir aux citoyens les informations nécessaires afin de leur permettre de se forger une opinion sur les questions de société et de participer ainsi activement et efficacement à la société démocratique. En Europe, les médias traditionnels sont subordonnés à l'existence d'un large éventail de règles en matière d'impartialité, de pluralisme, de diversité culturelle, de contenu préjudiciable, de publicité et de contenu sponsorisé. La démocratie dans l'Union européenne repose sur l'existence de médias libres et indépendants¹.

L'internet a non seulement considérablement accru le volume et la diversité des informations disponibles, mais il a également modifié en profondeur la manière dont les citoyens accèdent à l'information et s'investissent par rapport à cette dernière. Les jeunes utilisateurs, en particulier, utilisent désormais les médias en ligne comme principale source d'information. L'accès aisé à des informations diversifiées de qualité peut rendre les processus démocratiques plus participatifs et inclusifs.

Or, les nouvelles technologies peuvent être utilisées, notamment par l'intermédiaire des médias sociaux, comme vecteur de désinformation à une échelle jamais atteinte, avec une rapidité et une précision de ciblage sans précédent. Elles donnent alors naissance à des sphères d'information personnalisées et deviennent de puissantes chambres d'échos pour les campagnes de désinformation.

La désinformation mine la confiance dans les institutions et dans les médias traditionnels et numériques, et elle nuit à nos démocraties en entravant la capacité des citoyens à prendre des décisions informées. Par ailleurs, la désinformation soutient souvent des idées et des activités radicales et extrémistes. Elle porte atteinte à la liberté d'expression, qui est un droit fondamental inscrit dans la Charte des droits fondamentaux de l'Union européenne (ci-après la «charte»)². La liberté d'expression comprend le respect de la liberté et du pluralisme des médias, ainsi que le droit des citoyens d'émettre des opinions et de recevoir ou de communiquer des informations et des idées «sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière».

La principale obligation des acteurs publics en matière de liberté d'expression et de liberté des médias est de s'abstenir de toute forme d'ingérence et de censure, ainsi que de garantir un environnement propice à un débat public inclusif et pluraliste. Les contenus licites, même prétendument préjudiciables, sont généralement protégés par la liberté d'expression et doivent faire l'objet d'un traitement différent de celui réservé aux contenus illicites, dont la suppression peut être justifiée. Ainsi que la Cour européenne

¹ http://ec.europa.eu/information_society/newsroom/image/document/2016-50/2016-fundamental-colloquium-conclusions_40602.pdf

² Article 11 de la charte. L'article 6, paragraphe 1, du traité sur l'Union européenne confère une valeur contraignante à la charte et dispose qu'elle «a la même valeur juridique que les traités».

des droits de l'homme l'a conclu, cet aspect est particulièrement important en ce qui concerne les élections³.

Une série d'acteurs nationaux et étrangers ont largement recours à des campagnes massives de désinformation en ligne pour semer la méfiance et créer des tensions sociétales, ce qui peut avoir de graves conséquences pour notre sécurité. En outre, les campagnes de désinformation menées par des pays tiers peuvent faire partie de menaces hybrides à la sécurité intérieure, y compris dans le cadre des processus électoraux, en particulier lorsqu'elles s'accompagnent de cyberattaques. Par exemple, la doctrine militaire russe reconnaît explicitement que la guerre de l'information est l'un de ses domaines de compétence.⁴

La propagation de la désinformation touche également les processus d'élaboration des politiques, en ce sens qu'elle permet de faire vaciller l'opinion publique. Les acteurs nationaux et étrangers peuvent recourir à la désinformation pour manipuler les politiques, les débats sociétaux et les attitudes dans des domaines tels que le changement climatique, la migration, la sécurité publique, la santé⁵ et les finances. La désinformation peut également nuire à la confiance de l'opinion publique dans la science et les preuves empiriques.

En 2014, le Forum économique mondial a considéré que la propagation rapide de la désinformation en ligne était l'une des dix principales tendances des sociétés modernes⁶.

En 2016, les médias sociaux, les agrégateurs d'informations et les moteurs de recherche, pris conjointement, ont été les principaux moyens de lecture de l'actualité en ligne pour 57 % des utilisateurs de l'Union européenne⁷. En ce qui concerne les jeunes, un tiers des 18-24 ans ont déclaré que les médias sociaux constituaient leur principale source d'information⁸.

80 % des Européens se sont retrouvés face à des informations qu'ils considéraient fausses ou trompeuses, et ce plusieurs fois par mois, voire plus souvent. Pour 85 % des participants, il s'agit d'un problème dans leur pays⁹.

Les plateformes en ligne qui distribuent des contenus, en particulier les médias sociaux, les services de partage de vidéos et les moteurs de recherche, jouent un rôle essentiel dans la propagation et l'amplification de la désinformation en ligne. En ne réagissant pas d'une manière proportionnée, ces plateformes n'ont pas été jusqu'ici à la hauteur des défis que posent la désinformation et l'utilisation de leurs infrastructures à des fins de manipulation. Quelques timides initiatives visant à contrer la propagation de la désinformation en ligne ont certes été recensées, mais seulement dans un petit nombre de

³ [Voir, par exemple, l'affaire Bowman c. Royaume-Uni \(141/1996/760/961\) http://hudoc.echr.coe.int/eng?i=001-58134.](http://hudoc.echr.coe.int/eng?i=001-58134)

⁴ <https://www.rusemb.org.uk/press/2029>

⁵ La Commission propose une recommandation du Conseil sur la réticence à la vaccination, comportant des mesures spécifiques pour surveiller et combattre la désinformation en la matière. Voir COM (2018)245/2

⁶ [http://reports.weforum.org/outlook-14/top-ten-trends-category-page/10-the-rapid-spread-of-misinformation-online/.](http://reports.weforum.org/outlook-14/top-ten-trends-category-page/10-the-rapid-spread-of-misinformation-online/)

⁷ [https://ec.europa.eu/digital-single-market/en/news/eurobarometer-internet-users-preferences-accessing-content-online.](https://ec.europa.eu/digital-single-market/en/news/eurobarometer-internet-users-preferences-accessing-content-online)

⁸ *Digital News Report 2017*, Reuters Institute, [https://reutersinstitute.politics.ox.ac.uk/risj-review/2017-digital-news-report-now-available.](https://reutersinstitute.politics.ox.ac.uk/risj-review/2017-digital-news-report-now-available)

⁹ [http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183.](http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183)

pays et en laissant de côté un grand nombre d'utilisateurs. En outre, de sérieux doutes planent sur l'efficacité des mesures prises par les plateformes pour protéger dûment les utilisateurs contre l'utilisation non autorisée de leurs données à caractère personnel par des tiers, comme l'ont illustré les récentes révélations concernant Facebook/Cambridge Analytica, actuellement examinées par les autorités chargées de la protection des données, concernant l'extraction de données à caractère personnel de millions d'utilisateurs des médias sociaux de l'Union européenne et leur exploitation à des fins électorales.

La désinformation croissante et la gravité de la menace qu'elle représente ont suscité une prise de conscience et une préoccupation croissantes au sein de la société civile, aussi bien dans les États membres de l'Union européenne qu'à l'échelle internationale. En mars 2015, le Conseil européen a invité la haute représentante à élaborer un plan d'action pour contrer les campagnes de désinformation menées par la Russie¹⁰. Cette demande a abouti à la création de la task force East Stratcom, qui fonctionne comme prévu depuis septembre 2015. En juin 2017, le Parlement européen a demandé à la Commission «d'analyser en profondeur la situation et le cadre juridique actuels en ce qui concerne les fausses informations et de vérifier la possibilité d'une intervention législative afin de limiter la publication et la diffusion de faux contenus»¹¹. En mars 2018, le Conseil européen a déclaré que «les réseaux sociaux et les plateformes numériques doivent garantir des pratiques transparentes ainsi qu'une protection totale de la vie privée et des données à caractère personnel des citoyens»¹². La *déclaration conjointe sur la liberté d'expression et les «fausses nouvelles», la désinformation et la propagande*, adoptée en 2017 par des rapporteurs spéciaux désignés par des organisations internationales¹³, aborde de manière ciblée l'application des normes internationales relatives aux droits de l'homme à ce phénomène.

Plusieurs États membres examinent actuellement les mesures qu'il serait possible d'adopter pour protéger l'intégrité des processus électoraux contre la désinformation en ligne et pour garantir la transparence de la publicité à caractère politique en ligne¹⁴.

Il est clair, cependant, que si la protection du processus électoral relève en premier lieu de la compétence des États membres, la dimension transfrontière de la désinformation en ligne rend nécessaire une approche européenne afin de garantir des actions efficaces et coordonnées et de protéger l'Union, ses citoyens, ses politiques et ses institutions.

La présente communication a été élaborée en tenant compte des vastes consultations menées auprès des citoyens et des parties prenantes. La Commission a mis en place, fin 2017, un groupe d'experts à haut niveau chargé de la conseiller en la matière. Ce groupe a rendu son rapport le 12 mars 2018¹⁵. La Commission a également lancé une vaste

¹⁰ <http://www.consilium.europa.eu/fr/press/press-releases/2015/03/20/conclusions-european-council/>.

¹¹ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0272+0+DOC+PDF+V0//FR>.

¹² <http://www.consilium.europa.eu/fr/press/press-releases/2018/03/23/european-council-conclusions-22-march-2018/>.

¹³ *Déclaration conjointe sur la liberté d'expression et les «fausses nouvelles», la désinformation et la propagande*, <http://www.osce.org/fom/302796?download=true>.

¹⁴ Certains États membres ont adopté ou envisagent d'adopter des mesures en matière de publicité à caractère politique. Il s'agit, entre autres, de la récente proposition de loi française sur les fausses informations et les lignes directrices non contraignantes proposées par le régulateur italien.

¹⁵ <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

consultation publique sous la forme de questionnaires en ligne, qui ont reçu 2 986 réponses¹⁶, ainsi que des dialogues structurés avec les parties prenantes concernées¹⁷, et un sondage d'opinion Eurobaromètre mené auprès des 28 États membres¹⁸.

La présente communication présente les points de vue de la Commission sur les défis liés à la désinformation sur l'internet. Elle expose les grands principes et objectifs généraux qui devraient guider les actions visant à sensibiliser l'opinion à la désinformation et à combattre efficacement ce phénomène, ainsi que les mesures spécifiques que la Commission entend prendre à cet égard.

2. PORTÉE ET CAUSES DE LA DÉSINFORMATION EN LIGNE

2.1. Portée

On entend par désinformation, les informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public. Par préjudice public on entend les menaces aux processus politiques et d'élaboration des politiques démocratiques et aux biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité. La désinformation ne comprend pas les erreurs de citation, la satire, la parodie, ni les informations et commentaires partisans clairement identifiés. La présente communication est sans préjudice des règles juridiques en vigueur dans l'Union ou à l'échelle nationale ayant trait aux questions examinées, y compris la désinformation contenant des contenus illicites¹⁹. La présente communication est sans préjudice des stratégies et des actions en cours concernant les contenus illicites, y compris les contenus terroristes en ligne et le matériel à caractère pédopornographique.

83 % des Européens considèrent que les fausses nouvelles constituent un problème pour la démocratie en général. Ils sont 45 % à penser que cette affirmation est absolument vraie, et 38 % à considérer qu'elle l'est dans une certaine mesure²⁰.

Selon les résultats d'une consultation menée par la Commission, les participants ont estimé que les deux principaux domaines dans lesquels la désinformation délibérée était susceptible d'avoir des effets préjudiciables sur la société étaient les élections et les politiques d'immigration, suivis de près par les politiques en matière de santé, d'environnement et de sécurité²¹.

¹⁶ <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation>.

¹⁷ https://ec.europa.eu/epsc/events/high-level-hearing-preserving-democracy-digital-age_en et <https://ec.europa.eu/digital-single-market/en/fake-news>.

¹⁸ <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183>.

¹⁹ Recommandation de la Commission du 1^{er} mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne (C(2018) 1177 final), <https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online>

²⁰ <https://ec.europa.eu/digital-single-market/en/news/first-findings-eurobarometer-fake-news-and-online-disinformation>.

²¹ <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation>.

2.2. Contexte et causes principales de la désinformation

La prolifération de la désinformation découle de causes économiques, technologiques, politiques et idéologiques étroitement liées.

Premièrement, la propagation de la désinformation est symptomatique d'un phénomène plus vaste qui touche les sociétés confrontées à des changements rapides. L'insécurité économique, la montée en puissance des extrémismes et les changements culturels sont générateurs d'anxiété et offrent aux campagnes de désinformation un terrain fertile pour accroître les tensions sociétales, la polarisation et la méfiance. Des organisations et des entités capables d'exercer une influence (entreprises, États ou organisations non gouvernementales ayant un intérêt dans les débats politiques et stratégiques, y compris des sources extérieures à l'Union européenne) peuvent avoir recours à la désinformation pour manipuler les débats politiques et sociétaux. L'incidence de la désinformation varie d'une société à l'autre en fonction des niveaux d'éducation, de la culture démocratique, de la confiance dans les institutions, du caractère inclusif des systèmes électoraux, du rôle de l'argent dans les processus politiques, et des inégalités sociales et économiques.

Sur le long terme, la lutte contre la désinformation ne sera efficace que si elle s'accompagne d'une volonté politique claire de renforcer la résilience collective pour soutenir nos convictions démocratiques et nos valeurs européennes.

Deuxièmement, la propagation de la désinformation se produit dans un secteur des médias en proie à de profondes mutations. L'essor des plateformes actives dans le secteur des médias a porté un coup dur aux journalistes et aux médias d'information professionnels, qui tentent encore, d'une manière générale, d'adapter leurs modèles commerciaux et de trouver de nouveaux moyens pour monétiser les contenus. En outre, certaines plateformes se sont approprié des fonctions généralement associées aux médias, faisant irruption dans le monde de l'information en tant qu'agrégateurs et distributeurs de contenus, sans disposer systématiquement des cadres et des capacités éditoriales des médias. Leurs motivations économiques les incitent à attirer une large base d'utilisateurs en exploitant les effets de réseau et à maximiser le temps que les usagers passent sur leurs sites en privilégiant la quantité à la qualité de l'information, sans tenir compte de l'incidence que cela peut avoir.

Entre 2010 et 2014, les recettes totales des organes de presse ont diminué de 13,45 milliards d'euros, tandis que les recettes numériques augmentaient de 3,98 milliards d'euros, soit une diminution des recettes nette de 9,47 milliards d'euros (-13 %) ²². En outre, selon les organes de presse, le déclin actuel de ce secteur a déjà entraîné la fermeture ou la réduction de leurs équipes de rédaction ²³.

Troisièmement, les technologies des réseaux sociaux sont manipulées pour propager la désinformation au cours d'étapes successives: i) création des éléments de désinformation, ii) amplification au moyen des médias sociaux et d'autres médias en ligne, et iii) diffusion par les utilisateurs.

²² http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17211.

²³ <https://ec.europa.eu/digital-single-market/en/news/public-consultation-role-publishers-copyright-value-chain-and-panorama-exception>.

i) Création des éléments de désinformation

La désinformation est un outil d'influence puissant et peu onéreux, souvent même économiquement rentable. À ce jour, la plupart des cas connus ont concerné des articles écrits, parfois accompagnés de photographies authentiques ou de contenus audiovisuels sortis de leur contexte. Toutefois, de nouvelles technologies, peu onéreuses et faciles à utiliser, sont désormais disponibles. Elles permettent de créer des images et du contenu audiovisuel truqués («*deep fakes*») et offrent des outils plus puissants pour manipuler l'opinion publique.

ii) Amplification au moyen des médias sociaux et d'autres médias en ligne

Plusieurs facteurs constituent le terreau de la propagation de la désinformation en ligne. Les mécanismes de la prolifération de la désinformation sont:

- basés sur des algorithmes: les critères utilisés par les algorithmes pour hiérarchiser l'affichage des informations sont influencés par le modèle économique des plateformes, lequel accorde la priorité aux contenus personnalisés et sensationnels, généralement plus susceptibles d'attirer l'attention des utilisateurs et d'être partagés. En facilitant le partage de contenus personnalisés entre usagers ayant des affinités, les algorithmes renforcent indirectement la polarisation et les effets de la désinformation;
- axés sur la publicité: le modèle actuel de publicité numérique est souvent basé sur le nombre de clics effectués et récompense les contenus sensationnels et viraux. Ce modèle repose sur des réseaux publicitaires gérés par des agences qui garantissent le placement en temps réel d'annonces basées sur des processus décisionnels algorithmiques. Il facilite le placement d'annonces sur des sites web à contenus sensationnalistes qui jouent sur les émotions des utilisateurs, y compris la désinformation;
- fondés sur la technologie: les technologies en ligne telles que les services automatisés (parfois appelés robots ou «*bots*») amplifient artificiellement la propagation de la désinformation. Ces mécanismes peuvent être facilités par des profils fabriqués de toutes pièces (faux comptes) n'appartenant pas à des utilisateurs réels, et parfois orchestrés à une échelle massive (on parle alors d'«usines à trolls»).

iii) Diffusion par les utilisateurs

Les utilisateurs eux-mêmes jouent aussi un rôle dans la diffusion de la désinformation et leur tendance à partager des contenus sans effectuer de vérifications préalables ne fait qu'accroître la vitesse de circulation sur les médias sociaux. Le volume et la vitesse des flux de contenus en ligne ne cessent d'augmenter, accroissant le risque de partage des éléments de désinformation sans discernement.

Bien que les sites web d'actualités les plus populaires aient une audience moyenne mensuelle plus élevée, les fausses nouvelles connaissent une propagation virale plus importante. Par exemple, en France, un site de fausses nouvelles a généré à lui seul en moyenne plus de 11 millions d'interactions par mois, soit cinq fois plus que les sites d'informations mieux établis²⁴.

Les participants à la consultation publique ont estimé que la désinformation se propageait plus facilement par les médias en ligne, étant donné que les fausses nouvelles jouent sur les émotions des lecteurs (88 %), peuvent orienter le débat public (84 %) et sont conçues pour générer des recettes (65 %)²⁵.

3. UNE APPROCHE EUROPÉENNE POUR LUTTER CONTRE LA DÉSINFORMATION EN LIGNE

Compte tenu de la complexité du problème et du rythme rapide des mutations de l'environnement numérique, la Commission considère que toute réponse politique devrait être globale, et prévoir l'évaluation continue du phénomène de la désinformation et l'adaptation des objectifs politiques à l'évolution de celle-ci.

Il ne faut certes pas s'attendre à trouver une solution unique à tous les problèmes posés par la désinformation, mais l'inaction n'est pas envisageable.

De l'avis de la Commission, les mesures pour lutter contre la désinformation devraient être guidées par les principes et objectifs généraux suivants:

- Premièrement, améliorer la transparence en ce qui concerne l'origine des informations, et la manière dont elles sont produites, sponsorisées, diffusées et ciblées afin de permettre aux citoyens d'évaluer les contenus auxquels ils accèdent en ligne et de révéler d'éventuelles tentatives de manipulation de l'opinion.
- Deuxièmement, favoriser la diversité des informations, pour permettre aux citoyens de prendre des décisions éclairées guidées par l'esprit critique, en soutenant le journalisme de qualité, l'éducation aux médias et le rééquilibrage de la relation entre les créateurs et les diffuseurs d'informations.
- Troisièmement, promouvoir la crédibilité des informations en fournissant une indication sur leur fiabilité, notamment à l'aide de signaleurs de confiance, et en améliorant la traçabilité des informations et l'authentification des fournisseurs d'information influents.
- Quatrièmement, élaborer des solutions inclusives. La sensibilisation des utilisateurs au problème, une extension de l'éducation aux médias, une large mobilisation des parties prenantes et la coopération des pouvoirs publics, des plateformes en ligne, des annonceurs, des signaleurs de confiance, des

²⁴ *Measuring the reach of "fake news" and online disinformation in Europe*, Reuters Institute <https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe>.

²⁵ <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation>.

journalistes et des médias sont nécessaires pour parvenir à des solutions efficaces à long terme.

Sur la base de toutes les contributions recueillies, la Commission a l'intention de prendre les mesures énoncées ci-après. Ces mesures complètent le règlement général relatif à la protection des données, qui sera applicable dans toute l'Union européenne à partir du 25 mai 2018 et aura pour effet de renforcer la protection des données à caractère personnel des utilisateurs de plateformes en ligne²⁶. Le règlement général relatif à la protection des données précise la notion de consentement et inclut la notion fondamentale de transparence du traitement. En outre, il clarifie et harmonise les conditions dans lesquelles les données à caractère personnel peuvent être transférées («traitées ultérieurement»).

3.1. Un écosystème en ligne plus transparent, plus fiable et plus responsable

Les mécanismes sous-jacents à la création, à l'amplification et à la diffusion des éléments de désinformation exploitent le manque de transparence et de traçabilité de l'actuel écosystème de plateformes, ainsi que l'incidence des algorithmes et des modèles de publicité en ligne. Il est dès lors nécessaire de promouvoir des changements adéquats dans le comportement des plateformes, le renforcement de la responsabilité de l'écosystème d'information, l'amélioration des capacités de vérification des informations et la progression des connaissances collectives sur la désinformation, ainsi que l'utilisation des nouvelles technologies, afin d'améliorer la manière dont les informations sont produites et diffusées en ligne.

3.1.1. Les plateformes en ligne doivent agir rapidement et efficacement pour protéger les utilisateurs contre la désinformation

On attend de plus en plus des plateformes en ligne non seulement qu'elles respectent les obligations juridiques relevant du droit de l'Union européenne et du droit national, mais aussi qu'elles agissent de manière responsable, compte tenu de leur rôle central, pour garantir un environnement en ligne sûr, protéger les utilisateurs contre la désinformation et permettre à ces derniers d'accéder à des opinions politiques diversifiées.

D'une manière générale, les plateformes ont manqué de transparence en matière de publicité à caractère politique et de contenu sponsorisé. Par ailleurs, elles n'ont pas fourni d'informations suffisantes sur l'utilisation de techniques de diffusion stratégiques, telles que le recours à des influenceurs rémunérés et/ou à des robots, pour commercialiser des messages. Cet aspect a été l'un des principaux moteurs pour les initiatives menées dans certains États membres et pays tiers ayant décidé d'adopter des mesures de transparence concernant la publicité à caractère politique en ligne.

La Commission invite les plateformes à intensifier résolument leurs efforts pour lutter contre la désinformation en ligne. Elle considère qu'une autorégulation peut contribuer à ces efforts, pour autant qu'elle soit mise en œuvre et contrôlée de manière effective.

À cette fin, la Commission soutiendra l'élaboration d'un code de bonnes pratiques ambitieux, s'appuyant sur les principes clés proposés par le groupe d'experts de haut

²⁶ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

niveau²⁷, conformément auquel les plateformes en ligne et le secteur de la publicité s'engageraient à atteindre les objectifs suivants:

- améliorer considérablement le contrôle des placements de publicité, notamment afin de réduire les recettes des vecteurs de désinformation, et restreindre les options de ciblage pour la publicité à caractère politique;
- garantir la transparence au sujet des contenus sponsorisés, en particulier de la publicité à caractère politique et de la publicité engagée. Cette mesure devrait être complétée par des référentiels contenant des informations complètes sur les contenus sponsorisés, telles que l'identité réelle du sponsor, les montants dépensés et les critères de ciblage utilisés. Il conviendrait de mettre en place des mécanismes similaires pour permettre aux utilisateurs de comprendre les raisons pour lesquelles ils ont été ciblés par une publicité donnée;
- intensifier les efforts visant à fermer les faux comptes et démontrer l'efficacité de tels efforts;
- faciliter l'évaluation des contenus par les utilisateurs au moyen d'indicateurs de la fiabilité des sources de contenu basés sur des critères objectifs et approuvés par les associations de médias d'information, conformément aux principes et aux processus journalistiques, à la transparence en matière de propriété des médias et à la vérification de l'identité;
- diluer la visibilité de la désinformation en améliorant la repérabilité de contenus fiables;
- établir des systèmes et des règles clairs de marquage en ce qui concerne les robots et veiller à ce que les activités de ces derniers ne puissent pas être confondues avec des interactions humaines;
- fournir aux utilisateurs des outils de personnalisation et d'interaction en ligne pour leur permettre de découvrir plus facilement des contenus et d'accéder plus aisément à des sources d'information différentes offrant des points de vue contrastés; fournir aux utilisateurs des outils aisément accessibles pour signaler des cas de désinformation;
- veiller à ce que les services en ligne soient conçus de telle sorte à offrir des garanties contre la désinformation, par exemple, la fourniture d'informations détaillées sur le comportement des algorithmes qui hiérarchisent l'affichage des contenus, ainsi que le développement de méthodes d'essai;
- fournir à des organismes fiables de vérification des faits et à des universités (notamment via les interfaces de programmation d'applications) un accès aux données des plateformes, tout en veillant au respect de la vie privée des utilisateurs, du secret commercial et de la propriété intellectuelle, de façon à leur permettre de mieux comprendre le fonctionnement des algorithmes utilisés et de mieux analyser et surveiller la dynamique de la désinformation et son incidence sur la société.

²⁷ <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>, p. 32 du rapport du groupe d'experts de haut niveau.

Les actions poursuivant ces objectifs devraient respecter rigoureusement la liberté d'expression et prévoir des garanties pour éviter leur utilisation abusive, par exemple, pour censurer des discours critiques, satiriques, dissidents ou choquants²⁸. Elles devraient aussi être rigoureusement conformes à l'engagement pris par la Commission d'œuvrer à l'ouverture, à la sécurité et à la fiabilité de l'internet.

*La Commission convoquera un forum plurilatéral sur la désinformation, afin d'instaurer un cadre de coopération efficace entre les parties prenantes, dont les plateformes en ligne, le secteur de la publicité et les grands annonceurs, les médias et les représentants de la société civile, et afin d'obtenir des engagements en faveur de la coordination et de l'intensification des efforts de lutte contre la désinformation. Ce forum est distinct du forum de l'Union européenne sur l'internet consacré aux contenus terroristes en ligne. Il devrait, pour commencer, aboutir à la publication d'un **code européen de bonnes pratiques contre la désinformation** d'ici la fin juillet 2018, en vue de produire des effets mesurables d'ici octobre 2018. La Commission évaluera la mise en œuvre dudit code au moyen d'une large consultation avec les parties prenantes, sur la base d'indicateurs clés de performance conformes aux objectifs précités. Si les résultats devaient ne pas être satisfaisants, la Commission pourrait proposer de nouvelles mesures, notamment des mesures d'ordre réglementaire.*

*En parallèle, la Commission lancera **une étude afin d'examiner l'applicabilité des règles de l'Union européenne et les éventuelles lacunes en matière d'identification des contenus sponsorisés en ligne**. Dans ce contexte, elle évaluera également l'efficacité d'outils potentiels d'identification de contenus sponsorisés en ligne.*

3.1.2. Renforcer la vérification des faits, les connaissances collectives et la capacité de contrôle en matière de désinformation

Les vérificateurs de faits font désormais partie intégrante de la chaîne de valeur des médias; ils vérifient et évaluent la crédibilité des contenus sur la base de faits et de preuves. Leur tâche consiste aussi à analyser les sources et les processus de création et de diffusion de l'information. Pour être crédibles, ces vérificateurs de faits doivent être indépendants et obéir à des règles d'éthique et de transparence strictes.

L'existence d'un réseau dense de vérificateurs de faits fiables et indépendants est une condition essentielle pour la bonne santé de l'écosystème numérique. Les vérificateurs de faits doivent s'appuyer sur des normes élevées comme le code de principes du réseau international de vérification des faits²⁹.

En outre, de nombreux aspects de la désinformation restent à analyser et l'accès aux données des plateformes en ligne est encore limité. Pour définir une réponse efficace, il est indispensable de disposer d'un ensemble solide de faits et d'éléments de preuve sur la propagation de la désinformation et son impact. La collecte de données supplémentaires

²⁸ Comme l'a fait observer la Cour européenne des droits de l'homme, la liberté d'expression vaut non seulement pour les informations et idées accueillies avec faveur ou considérées comme inoffensives, mais aussi pour celles qui «heurtent, choquent ou inquiètent». *Handyside c. United Kingdom*, requête n° 5493/72 (7 décembre 1976), point 49.

²⁹ Le code de principes du réseau international de vérification des faits [International Fact-Checking Network (IFCN)] s'adresse aux organisations qui publient régulièrement des rapports non partisans sur l'exactitude des déclarations faites par des personnalités publiques et des grandes institutions, ainsi que d'autres affirmations largement diffusées qui présentent un intérêt pour la société, <https://www.poynter.org/international-fact-checking-network-fact-checkers-code-principles>.

et leur analyse par les vérificateurs de faits et les chercheurs universitaires devraient inclure les activités suivantes:

- surveillance continue de l’ampleur, des techniques et des outils, ainsi que de la nature exacte et de l’incidence potentielle de la désinformation;
- repérage et cartographie des mécanismes de désinformation qui contribuent à l’amplification numérique;
- contribution à l’élaboration d’indicateurs justes, objectifs et fiables pour ce qui est de la transparence des sources; et
- partage des connaissances avec les médias d’information, les plateformes et les autorités publiques afin de sensibiliser davantage le public à la question de la désinformation.

Un accès facilité aux données des plateformes en ligne ainsi qu’un espace sécurisé pour l’analyse et l’échange d’informations constituent des exigences essentielles dans ce contexte.

*Dans un premier temps, la Commission soutiendra la **création d’un réseau européen indépendant de vérificateurs de faits**, qui aura pour mission d’établir des méthodes de travail communes, d’échanger les bonnes pratiques, d’obtenir la couverture la plus large possible dans l’Union européenne et de prendre part à des activités conjointes de vérification de faits et à des activités connexes. Le réseau sera invité à participer au forum plurilatéral sur la désinformation. La Commission mettra à sa disposition des outils en ligne (par exemple un espace partagé sécurisé) qui faciliteront la collaboration.*

*Dans un deuxième temps, la Commission lancera une **plateforme européenne en ligne sécurisée sur la désinformation** afin de soutenir le réseau européen indépendant de vérificateurs de faits et les chercheurs universitaires concernés. Cette plateforme devrait proposer des outils de collecte transfrontière et d’analyse de données, ainsi qu’un accès à des données ouvertes à l’échelle européenne, et notamment à des informations statistiques indépendantes et fiables. Ainsi, le réseau pourra servir de signaleur de confiance. Il favorisera aussi une meilleure compréhension de la désinformation en ligne et aidera à définir des stratégies fondées sur des preuves pour limiter la propagation de ce phénomène. À cet égard, la Commission envisagera le recours au mécanisme pour l’interconnexion en Europe et s’appuiera sur l’expérience acquise dans la mise en œuvre du programme «Internet plus sûr».*

3.1.3. Promouvoir la responsabilité en ligne

Pour pouvoir faire respecter l’obligation de rendre des comptes, pour renforcer la confiance dans les fournisseurs d’informations identifiables et encourager un comportement en ligne plus responsable, il est essentiel d’identifier la source de désinformation en assurant sa traçabilité tout au long de la chaîne de diffusion. Par exemple, un utilisateur pourrait choisir de n’entrer en contact avec d’autres personnes sur des plateformes en ligne que si elles se sont identifiées.

À cet égard, le règlement sur l'identification électronique³⁰ établit un environnement réglementaire prévisible pour l'utilisation, la reconnaissance et la mise en œuvre transfrontalières en ligne de services d'identification électronique, de services d'authentification et de services de confiance, sur lesquels il serait possible de s'appuyer pour favoriser le développement et l'utilisation volontaire de systèmes aux fins de l'identification sécurisée des fournisseurs d'information sur la base de normes extrêmement strictes en matière de sécurité et de respect de la vie privée, y compris l'utilisation possible de pseudonymes vérifiés.

Afin de faciliter les enquêtes sur les comportements malveillants en ligne, comme indiqué dans la communication commune sur la cybersécurité présentée en septembre 2017, la Commission continuera de promouvoir l'adoption du protocole internet version 6 (IPv6), qui permet d'attribuer à une adresse IP un seul utilisateur. Elle poursuivra également ses efforts pour améliorer le fonctionnement, la disponibilité et l'exactitude des informations contenues dans les systèmes WHOIS relatifs aux noms de domaines et aux adresses IP³¹, conformément aux efforts déployés par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) et dans le strict respect des règles relatives à la protection des données.

La Commission encouragera le réseau de coopération eIDAS à promouvoir, en coopération avec les plateformes, l'utilisation volontaire de systèmes en ligne permettant l'identification des fournisseurs d'information sur la base de moyens d'identification et d'authentification électroniques fiables, y compris les pseudonymes vérifiés, comme le prévoit le règlement sur l'identification électronique.

Conjointement, ces mesures devraient aussi contribuer à limiter les cyberattaques, qui sont souvent associées à des campagnes de désinformation dans le contexte de menaces hybrides.

3.1.4. Tirer parti des nouvelles technologies

Les technologies émergentes continueront à modifier la façon dont les informations sont produites et diffusées, mais elles peuvent également jouer un rôle central dans la lutte contre la désinformation sur le long terme. Citons quelques exemples:

- l'intelligence artificielle, si elle fait l'objet d'un contrôle humain adéquat, aura une importance cruciale dans la vérification, l'identification, et le balisage de la désinformation;
- les technologies utilisées par les médias pour proposer des expériences personnalisables et interactives en ligne peuvent aider les citoyens à mettre au jour des contenus et à déceler des éléments de désinformation;
- les technologies innovantes, telles que la chaîne de blocs (*blockchain*), peuvent contribuer à préserver l'intégrité des contenus, à valider la fiabilité des informations et/ou de leurs sources, à garantir la transparence et la traçabilité, et à favoriser la confiance dans les informations présentées sur l'internet. l'identification électronique

³⁰ Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

³¹ <https://whois.icann.org/fr>.

de confiance, l'authentification et les pseudonymes vérifiés pourraient être utilisés dans ce contexte; et

- les algorithmes cognitifs qui assurent le traitement des informations contextuelles, lesquelles concernent entre autres l'exactitude et la qualité des sources de données, amélioreront la pertinence et la fiabilité des résultats de recherche.

La Commission joue un rôle actif dans le domaine des technologies émergentes, en particulier dans le cadre de son initiative pour la prochaine génération d'internet³².

La Commission utilisera pleinement le programme de travail Horizon 2020 pour mobiliser ces technologies. Elle examinera par ailleurs la possibilité d'apporter un soutien supplémentaire au déploiement d'outils de lutte contre la désinformation, en s'attachant à raccourcir les délais de mise sur le marché des résultats des activités d'innovation à forte incidence et à encourager les partenariats entre les chercheurs et les entreprises.

3.2. Sécurité et résilience des processus électoraux

La sécurité des processus électoraux, qui constitue le fondement de notre démocratie, requiert une attention toute particulière. La désinformation fait partie aujourd'hui d'un arsenal d'outils utilisés pour manipuler les processus électoraux, comme le piratage ou la corruption de sites web, ou encore l'accès à des informations à caractère personnel sur des responsables politiques et la divulgation de ces données. Les opérations facilitées par les technologies de l'information et de la communication peuvent être utilisées pour miner l'intégrité des informations destinées au public et empêcher l'identification des sources de désinformation. Cet aspect joue un rôle critique lors des campagnes électorales, pour lesquelles il peut s'avérer impossible, compte tenu des contraintes de temps, de détecter les éléments de désinformation et d'y répondre en temps utile.

Au cours de ces dernières années, des pratiques de manipulation et de désinformation en ligne en période électorale ont été détectées dans au moins 18 pays et «*les tactiques de désinformation ont contribué à faire reculer la liberté sur l'internet pour la septième année consécutive*»³³.

Dans la perspective des élections européennes de 2019, la Commission encourage³⁴ les autorités nationales compétentes à recenser les meilleures pratiques en matière d'identification, d'atténuation et de gestion des risques que représentent la désinformation et les cyberattaques pour le processus électoral. Au sein du groupe de coopération institué en vertu de la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI), les États membres ont commencé à cartographier les initiatives européennes dans le domaine de la cybersécurité des réseaux et des systèmes d'information utilisés dans les processus électoraux, dans l'objectif d'élaborer des orientations non contraignantes.

³² <https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative>.

³³ *Freedom on the net 2017 report*, Freedom house, <https://freedomhouse.org/report/freedom-net/freedom-net-2017>.

³⁴ Recommandation de la Commission du 14 février 2018 visant à renforcer le caractère européen des élections au Parlement européen de 2019 et à rendre leur conduite plus efficace, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2018%3A045%3ATOC>.

Le colloque sur les droits fondamentaux qui aura lieu les 26 et 27 novembre 2018 aura la «démocratie» pour thème central. Il y sera discuté, d'une part, des ingrédients essentiels des sociétés démocratiques inclusive et saines, y compris des possibilités et des enjeux liés à la transformation numérique pour un débat démocratique éclairé et pluraliste, et, d'autre part, des incidences négatives de la propagande.

La Commission démarrera un dialogue permanent pour soutenir les États membres dans la gestion des risques que font peser les cyberattaques et la désinformation sur les processus électoraux démocratiques, eu égard notamment aux processus électoraux dans les États membres et aux élections européennes de 2019. Les aspects suivants seront abordés:

- les mesures de suivi appropriées dans le prolongement d'un premier échange avec les États membres lors de la conférence sur les meilleures pratiques en matière d'élections, qui se tiendra les 25 et 26 avril 2018;

- le soutien nécessaire, en collaboration avec l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, aux travaux actuellement menés par le groupe de coopération SRI sur la cybersécurité des élections. D'ici à la fin de l'année 2018, le groupe devrait publier un recueil de recommandations et de mesures concrètes qui pourront être mises en œuvre par les États membres pour sécuriser les cycles électoraux;

- une conférence à haut niveau sur les menaces liées au cyberspace pour les élections, qui sera organisée fin 2018 avec les États membres, sous les auspices de la task force sur l'union de la sécurité.

3.3. Promotion de l'enseignement et de l'éducation aux médias

Le développement des compétences numériques essentielles tout au long de la vie, et en particulier pour les jeunes, est essentiel pour renforcer la résilience de nos sociétés à la désinformation.

Le plan d'action en matière d'éducation numérique, adopté par la Commission en janvier 2018³⁵, met en évidence les risques que la désinformation représente pour les enseignants et les élèves ainsi que l'urgence qu'il y a à développer des compétences et des aptitudes numériques chez tous les apprenants, aussi bien dans le cadre de l'enseignement formel que non formel. Le cadre de compétences numériques pour les citoyens élaboré par la Commission décrit le large éventail de compétences dont ont besoin tous les apprenants: l'éducation à l'information et au numérique, la création de contenus numériques ainsi que la sécurité et le bien-être en ligne³⁶.

Selon la majorité des participants à la consultation publique, l'éducation et la responsabilisation des utilisateurs pour un meilleur accès et une meilleure utilisation des informations en ligne ainsi que l'émission d'un avertissement lorsque du contenu est

³⁵ <https://ec.europa.eu/education/sites/education/files/digital-education-action-plan.pdf>.

³⁶ <https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework>.

généralisé ou diffusé par un robot sont des mesures que les plateformes en ligne pourraient mettre en œuvre très efficacement pour empêcher la propagation de la désinformation³⁷.

En raison de la dimension transfrontière de la désinformation, l'Union européenne a un rôle à jouer en soutenant la diffusion, dans les États membres, des bonnes pratiques qui permettront d'accroître la résilience des citoyens, et la Commission peut continuer de renforcer ses actions en faveur des jeunes et des adultes:

- la Commission dirige le groupe d'experts en éducation aux médias et soutient des projets pilotes tels que «l'éducation aux médias pour tous»³⁸;
- l'importance de l'éducation aux médias³⁹ est reconnue dans la directive sur les services de médias audiovisuels, dont la révision a pour but de renforcer le suivi des mesures prises par les autorités des États membres en matière d'éducation aux médias⁴⁰;
- la Commission soutient un certain nombre d'initiatives, y compris au moyen du programme Erasmus +, concernant la sécurité sur l'internet, le bien-être numérique et les compétences numériques visant à stimuler une connaissance critique de l'environnement numérique chez les citoyens, en particulier chez les jeunes, ce qui contribue à renforcer l'éducation aux médias numériques;
- les États membres, les partenaires sociaux et les établissements d'enseignement partagent les expériences et les bonnes pratiques en matière d'éducation numérique dans le cadre du groupe de travail de l'Union européenne sur les compétences numériques⁴¹;
- la Commission encourage les États membres à mobiliser des ressources et à inclure dans leurs politiques en matière d'éducation la citoyenneté numérique, l'éducation aux médias, le développement de compétences de réflexion critique dans un environnement en ligne ainsi que des activités de sensibilisation à la désinformation et aux techniques d'amplification en ligne. Il est essentiel à cet égard de soutenir les enseignants, notamment par la formation et par l'échange de bonnes pratiques.

La Commission entend également:

- *encourager les vérificateurs de faits indépendants et les organisations de la société civile à fournir du matériel pédagogique aux écoles et aux éducateurs;*

³⁷ <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation>.

³⁸ <https://ec.europa.eu/digital-single-market/en/news/2016-call-proposals-pilot-project-media-literacy-all>

³⁹ Conformément au considérant 47 de la directive sur les services de médias audiovisuels, «[i]l convient [...] de favoriser le développement de l'éducation aux médias à tous les niveaux de la société et de suivre attentivement les progrès réalisés en la matière».

⁴⁰ Dans son orientation générale, le Conseil a inclus l'obligation pour les États membres de promouvoir et d'adopter des mesures en faveur du développement des compétences liées à l'éducation aux médias. Cette exigence est actuellement examinée par les colégislateurs dans le cadre de la révision de la directive sur les services de médias audiovisuels.

⁴¹ https://ec.europa.eu/education/policy/strategic-framework/expert-groups/digital-skills-competences_fr

- *inclure dans la campagne #SaferInternet4EU⁴² des initiatives ciblées sur la désinformation en ligne;*
- *organiser une semaine européenne de l'éducation aux médias dans le but de sensibiliser l'opinion publique et de soutenir la coopération transfrontière entre les organisations concernées;*
- *faire rapport sur l'éducation aux médias dans le cadre de l'application de la directive sur les services de médias audiovisuels;*
- *collaborer avec l'Organisation de coopération et de développement économiques, dans le cadre du processus du programme international pour le suivi des acquis des élèves, afin d'examiner la possibilité d'ajouter l'éducation aux médias aux critères utilisés par l'organisation dans ses rapports comparatifs;*
- *encourager les travaux de la coalition en faveur des compétences et des emplois numériques⁴³, afin de soutenir les compétences numériques, notamment pour favoriser la participation à la société;*
- *poursuivre la mise en œuvre du plan d'action en matière d'éducation numérique⁴⁴ et continuer à soutenir les initiatives telles que le programme de stages en matière d'accès au numérique «Digital Opportunity traineeships»⁴⁵ qui visent à renforcer les compétences numériques et la prise de conscience des citoyens européens — en particulier, de la jeune génération — et de promouvoir des valeurs communes ainsi que l'inclusion.*

3.4. Soutien d'un journalisme de qualité, en tant que rouage essentiel d'une société démocratique

Des médias d'information, y compris publics, et un journalisme de qualité jouent un rôle important en fournissant aux citoyens des informations diversifiées et de haute qualité. En offrant un environnement médiatique pluraliste et diversifié, ils sont capables de dévoiler, de contrebalancer, et de diluer les éléments de désinformation.

Dans un environnement numérique changeant, il est nécessaire d'investir dans un journalisme de haute qualité, de renforcer la confiance dans le rôle clé, pour la société et la démocratie, d'un journalisme de qualité, à la fois hors ligne et en ligne, et d'encourager les médias d'information de qualité à explorer des formes de journalisme innovantes.

Selon l'enquête Eurobaromètre, les citoyens perçoivent les médias traditionnels comme étant les sources d'information les plus fiables: la radio (70 %), la télévision (66 %) et les journaux et magazines d'actualités imprimés (63 %). Les sources d'information considérées comme les moins dignes de confiance sont les sites d'hébergement de vidéos (27 %) et les réseaux sociaux en ligne (26 %). Les plus jeunes participants à l'enquête

⁴² <https://www.betterinternetforkids.eu/web/portal/saferinternet4eu>.

⁴³ <https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition>.

⁴⁴ <https://ec.europa.eu/digital-single-market/en/news/specific-actions-digital-education-action-plan>.

⁴⁵ <https://ec.europa.eu/digital-single-market/en/digital-opportunity-traineeships-boosting-digital-skills-job>.

sont plus enclins à faire confiance aux actualités et aux informations auxquelles ils peuvent accéder en ligne⁴⁶.

Par ailleurs, il est nécessaire de rééquilibrer la relation entre les médias et les plateformes en ligne. Ce processus sera facilité par une approbation dans les meilleurs délais de la réforme du droit d'auteur de l'Union européenne, qui aura pour effet de renforcer la position des éditeurs et d'assurer une répartition plus équitable des revenus entre les titulaires de droits et les plateformes, ce qui devrait en particulier aider les médias d'information et les journalistes à monétiser leurs contenus.

Les journalistes et les professionnels des médias devraient également mieux exploiter toutes les possibilités offertes par les nouvelles technologies et acquérir les compétences numériques qui doivent leur permettre d'utiliser les analyses de données et de médias sociaux et, partant, les aider à trouver et à vérifier les informations.

Enfin, un soutien public aux médias et aux médias de service public est très important pour la fourniture d'informations de haute qualité et la protection du journalisme dans l'intérêt public. Les mesures de soutien adoptées par les États membres en vue d'atteindre des objectifs d'intérêt commun de l'Union européenne tels que la liberté et le pluralisme des médias ont été déclarées compatibles avec les règles de l'Union européenne en matière d'aides d'État (voir les décisions de la Commission concernant les aides aux médias⁴⁷).

Les États membres sont encouragés à envisager l'adoption de régimes d'aides horizontales pour remédier aux défaillances du marché qui minent la viabilité du journalisme de qualité, ainsi que de mesures de soutien pour des activités spécifiques, telles que la formation des journalistes et l'innovation en matière de produits et de services.

Les règles existantes⁴⁸ précisent les conditions dans lesquelles les États membres peuvent accorder des aides publiques. Afin de renforcer la transparence et la prévisibilité de l'application des règles en matière d'aides d'État dans ce domaine, la Commission mettra à la disposition du public un répertoire en ligne sur les règles applicables en

⁴⁶ <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183>.

⁴⁷ La Commission a notamment approuvé l'aide aux agences de presse (par exemple SA.30481, aide d'État en faveur de l'agence France-Presse (AFP), France, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_30481), les régimes d'aides à la presse généraliste (par exemple SA.36366, Régime d'aides en faveur de la production et de l'innovation dans le domaine de la presse écrite, Danemark, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_36366) et les régimes d'aides destinés aux publications à faibles ressources publicitaires (par exemple SA.47973, aide à la presse française, décret de 2015, France, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_47973).

⁴⁸ En ce qui concerne les services publics de radiodiffusion, des orientations détaillées spécifiques sont disponibles (communication de la Commission concernant l'application aux services publics de radiodiffusion des règles relatives aux aides d'État, JO C 257 du 27.10.2009, p. 1). Selon le type de soutien envisagé, les orientations sur les aides à la R&D&I (communication de la Commission intitulée «Encadrement des aides d'État à la recherche, au développement et à l'innovation», JO C 198 du 27.6.2014, p. 1) et le règlement général d'exemption par catégorie [règlement (UE) n° 651/2014 de la Commission du 17 juin 2014 déclarant certaines catégories d'aides compatibles avec le marché intérieur en application des articles 107 et 108 du traité (JO L 187 du 26.6.2014, p. 1, modifié par le règlement (UE) 2017/1084 de la Commission du 14 juin 2017, JO L 156 du 20.6.2017, p. 1] peuvent aussi être pertinents.

matière d'aides d'État et les précédentes affaires correspondantes. En outre, des informations régulièrement mises à jour sur les aides accordées par les États membres pourront être consultées dans le registre de transparence⁴⁹.

La Commission lancera un appel à propositions, en 2018, en vue de la production et de la diffusion de contenus d'information de qualité sur les affaires européennes au moyen de médias d'information fondés sur les données.

Sur la base des résultats des projets en cours, la Commission examinera les moyens d'accroître le financement en soutien aux initiatives visant à promouvoir la liberté et le pluralisme des médias ainsi que des médias d'information et un journalisme de qualité, y compris les qualifications, la formation des journalistes, les nouvelles technologies pour les salles de presse et les plateformes collaboratives fondées sur les données.

La boîte à outils pour les professionnels des médias, élaborée par l'Agence des droits fondamentaux, relative à la couverture de l'information sous l'angle des droits fondamentaux proposera aux journalistes un ensemble de recommandations, de conseils et d'outils pour le traitement de dilemmes éthiques, y compris la désinformation, sous l'angle des droits fondamentaux.

3.5. Éliminer les menaces de désinformation internes et externes grâce à une communication stratégique

La communication et la sensibilisation par les autorités publiques font partie intégrante de la réponse à la désinformation. La communication stratégique exige, outre la détection et l'analyse de données, des actions d'information appropriées pour lutter contre les discours mensongers. Les mesures prévues à la section 3.1 permettront d'affiner et d'accélérer la détection et l'analyse de la désinformation en ligne et faciliteront la communication stratégique sur l'Europe et les politiques de l'Union européenne.

Cet aspect est particulièrement important étant donné que l'Union européenne est souvent la cible de campagnes de désinformation dont le but délibéré est d'affaiblir ses institutions, ses politiques, ses actions et ses valeurs. Les sources de ces activités peuvent être internes ou externes et les acteurs peuvent être privés ou publics et exercer leurs activités aussi bien sur le territoire de l'Union européenne que dans les pays tiers. Comme indiqué précédemment, la task force East StratCom a été créée en 2015 au sein du Service européen pour l'action extérieure afin de répondre aux campagnes de désinformation alors menées par la Russie compte tenu de l'importance du problème. De même, la cellule de fusion de l'Union européenne contre les menaces hybrides a été mise en place en 2016 au sein du Centre de situation et du renseignement de l'Union européenne pour surveiller et éliminer les menaces hybrides constituées par des acteurs étrangers, y compris la désinformation, qui visent à influencer les décisions politiques au sein de l'Union européenne et dans son voisinage. Ces institutions forment, avec le nouveau centre européen d'excellence pour la lutte contre les menaces hybrides, le socle d'une réponse européenne renforcée⁵⁰, et sont des maillons importants de la coopération

⁴⁹ Page de recherche publique «State Aid Transparency»:

<https://webgate.ec.europa.eu/competition/transparency/public/search/home?lang=en>.

⁵⁰ Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne, communication conjointe au Parlement européen et au Conseil du 6 avril 2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52016JC0018&from=fr>

entre l'Union européenne et l'Organisation du traité de l'Atlantique Nord visant à améliorer la résilience, la coordination et la préparation de l'Europe face aux interférences hybrides.

La Commission, en coopération avec le Service européen pour l'action extérieure, développera ses capacités de communication stratégique; à cet effet, elle renforcera dans un premier temps la coordination interne de ses activités de communication visant à lutter contre la désinformation.

La Commission, en collaboration avec le Service européen pour l'action extérieure, étendra cette collaboration, ses connaissances et ses activités aux autres institutions de l'Union européenne et, au travers d'un mécanisme approprié, aux États membres. Le réseau utilisera les données recueillies par la plateforme en ligne sécurisée sur la désinformation mentionnée à la section 3.1.2 pour concevoir des actions d'information visant à contrecarrer les discours mensongers sur l'Europe et à lutter contre la désinformation, tant à l'intérieur qu'à l'extérieur de l'Union européenne.

La Commission et le Service européen pour l'action extérieure examineront les options possibles pour élaborer des réponses de communication stratégique et d'autres mécanismes, en collaboration avec les États membres, afin de renforcer la résilience et de contrer les campagnes de désinformation systématique et les interférences hybrides de la part de gouvernements étrangers dirigées contre les citoyens et les entités de l'Union européenne.

La Commission, en coopération avec le Service européen pour l'action extérieure, présentera en juin un rapport sur les progrès accomplis dans le renforcement des capacités de lutte contre les menaces hybrides, y compris la cybersécurité, la communication stratégique et le contre-espionnage.

4. CONCLUSION

Un écosystème d'information performant, libre et pluraliste, ancré dans des normes professionnelles élevées, est indispensable à un débat démocratique sain. La Commission est attentive aux menaces que fait peser la désinformation sur nos sociétés ouvertes et démocratiques. La présente communication expose une démarche globale qui permettra de répondre à ces menaces sérieuses en favorisant des écosystèmes numériques fondés sur la transparence, qui privilégient l'information de qualité, responsabilisent les citoyens face à la désinformation et protègent nos démocraties et nos processus d'élaboration des politiques. La Commission invite tous les acteurs concernés à redoubler d'efforts pour apporter une réponse appropriée au problème. Elle considère que les mesures décrites ci-dessus, pour peu qu'elles soient mises en œuvre efficacement, contribueront de manière significative à contrecarrer la désinformation en ligne. Elle poursuivra néanmoins ses travaux dans ce domaine.

D'ici à décembre 2018, la Commission présentera un rapport sur les progrès accomplis. Elle examinera également dans ce rapport si de nouvelles mesures sont nécessaires pour garantir le suivi et l'évaluation continus des actions décrites.