

Sciences Po Strasbourg

École

de l'Université de Strasbourg

LA LUTTE CONTRE LA DÉSINFORMATION

ACTEURS ET TECHNIQUES

Ils ont rédigé ce rapport : Abd El Malek Océane, Bonnet Sarah, Corset Mathieu, Desponds Nérine, Falconnet Léo-Paul, Ghazi Tara, Nossent Louise, Perchine Zacharie, Perragin Adrien, Roudil Estelle.

La désinformation utilisée à des fins d'ingérence étrangère n'est pas récente mais s'est massivement développée avec l'essor du numérique et des techniques de plus en plus affûtées. Les sociétés européennes se sont mobilisées à différentes échelles. D'une part, nous pouvons remarquer des initiatives de la part d'organismes publics (1 et 2) mais aussi d'acteurs privés (3).

1. LES ACTEURS PUBLICS À L'ÉCHELLE EUROPÉENNE

Après l'agression armée de la Russie en Ukraine le 24 février 2022, l'UE renforce son engagement dans la lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger en mentionnant dans sa boussole stratégique de la même année la création d'une boîte à outils spécifique à ces menaces [114]. Les multiples outils de l'UE peuvent être répartis en quatre catégories : la connaissance de la situation et le partage d'informations ; le renforcement de la résilience, par des actions de sensibilisation, de soutien aux médias et de formation d'une culture numérique ; la mise en place d'obstacles réglementaires, afin de collaborer notamment avec le secteur privé ; des réponses diplomatiques, telles que des sanctions ou des déclarations publiques. À partir de cette grille de lecture, nous allons nous pencher sur quelques actions majeures de lutte contre la désinformation déployées par l'UE.

a. La désinformation comme enjeu de politique extérieure de l'UE : l'action du Service européen pour l'action extérieure

L'UE apporte tout d'abord une réponse de politique étrangère à l'enjeu de la désinformation. Considéré comme une menace extérieure provenant principalement de la Fédération de Russie, le sujet est amené dans les instances européennes en mars 2015 par le Conseil européen, qui invite le Haut représentant pour l'UE, en coopération avec les institutions européennes et les Etats-membres, à réaliser un plan d'action de communication stratégique d'ici le mois de juin de la même année. Mandaté pour lutter contre les campagnes de désinformation russes, le plan d'action amène à la création d'une cellule de communication stratégique, appelée la East Strat Com task force [115], spécialisée sur l'Europe orientale et intégrée à la division « Communication stratégique et analyse de l'information » du SEAE. Cela fait plus de dix ans que la Russie développe une

[114] Conseil européen. « Une boussole stratégique en matière de sécurité et de défense - Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales », 21 mars 2022. [Lien](#).

[115] Nous utiliserons le terme task force, qui signifie groupe de travail en anglais, pour la désigner dans la suite du texte.

stratégie de soft power par laquelle elle tente, en plus d'améliorer son image, de discréditer celle de l'UE. En effet, les « révolutions de couleur » au début du XXI^{ème} siècle, telles que la Révolution orange en Ukraine de 2004, symbolisent la perte de son influence sur les pays de l'ex-URSS et marque le point de départ de sa guerre informationnelle contre les démocraties occidentales. Ses campagnes de désinformation sont à destination des pays de l'Est de l'Europe, certains étant candidats à l'adhésion à l'UE, pour dénigrer les politiques de cette dernière et la dépeindre comme une entité décadente moralement et au bord de l'effondrement économique.

L'UE répond ainsi aux campagnes de désinformation russes par une politique extérieure en matière de communication stratégique.

Cette dernière est définie comme « *une série systématique d'actions soutenues et cohérentes, menées aux niveaux stratégique, opérationnel et tactique, et qui permettent d'identifier des publics cibles et des canaux efficaces pour favoriser et soutenir des types particuliers de comportement* » [116]. Appartenant aux outils de la diplomatie publique, la communication stratégique s'adresse donc à la société civile pour faire connaître les valeurs, les intérêts et les actions de politique extérieure d'une institution, afin de soutenir des comportements, ici concernant l'attitude et l'opinion des populations envers l'UE et leur potentielle adhésion.

La création de cette cellule en 2015 intervient suite à l'annexion illégale de la Crimée par la Russie un an plus tôt. En 2017, elle sera rejointe par deux task force supplémentaires sur d'autres régions prioritaires, une sur les Balkans occidentaux (Task Force Western Balkans) et l'autre sur les pays du Moyen-Orient, de l'Afrique du Nord et de la région du Golfe (Task Force South). Le choix de ces zones géographiques situées hors de l'UE repose ainsi sur une logique de complémentarité entre la dénonciation de la désinformation dans les pays voisins de l'UE et la lutte contre ce problème au sein de l'Union elle-même. Pour ce faire, le mandat de la task force East Strat Com se déploie à travers trois missions.

La première vise à diffuser les politiques de l'UE auprès des pays du Partenariat oriental à travers des campagnes de communication, en collaboration avec les délégations de l'UE sur le terrain. Elle a aussi comme volonté de renforcer l'environnement des médias dans le voisinage oriental et dans les États-membres en soutenant la liberté et l'indépendance des médias, en appui aux programmes régionaux de la DG NEAR de la Commission européenne [117]. Pour la période 2020-2023, elle a par exemple soutenu un programme de 11 millions d'euros destiné aux médias indépendants des pays du Partenariat oriental (« EU4 Indepen-

[116] Steve A Tatham. *Strategic Communication: A Primer*. Defence Academy of the United Kingdom, Advanced Research and Assessment Group, 2008. [Lien](#)

[117] Direction générale du voisinage et des négociations d'élargissement.

dent Media »). Enfin, elle est chargée d'améliorer la capacité de l'UE à prévoir, traiter et répondre aux campagnes de désinformation pro-Kremlin. Afin de remplir cette dernière mission, la task force a développé en 2015 le projet EUvsDisinfo spécifique aux ingérences du gouvernement russe et complété par la suite par une section sur la désinformation chinoise. Le principal apport de cette plateforme est la mise à disposition en accès public d'une base de données répertoriant des milliers de cas de désinformation et les réponses apportées par la task force. Elle dispose d'un système de surveillance systématique des médias et reçoit des contributions d'acteurs extérieurs. Publiant également une revue hebdomadaire et des articles d'analyse, ce projet a pour objectif de sensibiliser le grand public et les décideurs politiques aux techniques d'ingérence par la désinformation en recensant publiquement et en déconstruisant le maximum d'exemples. Le SEAE adopte une approche globale de la lutte contre la désinformation, en mobilisant tous les acteurs qui s'y sont engagés, issus de la société civile, des médias, des universités, des organisations internationales et des entreprises. Le système d'alerte rapide mis en place en 2018 vise à faciliter le partage de données entre tous ces acteurs et à encourager une réponse coordonnée.

La Cour des comptes européenne a cependant émis des critiques en 2021 sur les trois task forces du SEAE, pointant leur manque de ressources financières et matérielles ainsi qu'une actualisation trop occasionnelle de leurs missions face aux menaces émergentes [118]. La division de la Communication stratégique a tout de même évolué au fil du temps : composée de 9 employés à temps plein en 2015, elle en emploie 16 en 2021, provenant de divers corps de métiers (journalisme, sciences sociales, communication) et dotés de compétences dans les langues concernées. Le budget de la task force est passé de 1,1 million d'euros en 2018 à 4 millions en 2020, sous l'effet des élections européennes de 2019 et du renforcement de la vigilance [119]. Suite aux conséquences de la guerre d'invasion opérée par la Russie en Ukraine, le SEAE disposait en 2022 d'un budget d'environ 15,3 millions d'euros dirigé uniquement aux actions de communication stratégique [120].

b. Une approche législative de l'UE

De nombreux documents politiques ont engagé l'UE sur le terrain de la lutte contre la désinformation. En 2018, le Conseil européen demande au Haut Représentant pour l'Union de préparer une stratégie coordonnée de l'Union face au défi de la désinformation, ce qu'elle fait dans un plan d'action de la même année [121]. La Commission européenne publie au même moment un Code de bonnes pratiques sur la désinformation, non contraignant et renforcé en 2022. Une grande partie des plateformes numériques (Google

[118] Cour des Comptes européennes. « La désinformation concernant l'UE : un phénomène sous surveillance mais pas sous contrôle », 2021. [Lien](#)

[119] SEAE. « Questions and Answers about the East StratCom Task Force », 27 octobre 2021. [Lien](#)

[120] Parlement européen. « Report on Discharge in Respect of the Implementation of the General Budget of the European Union for the Financial Year 2022, Section X - European External Action Service », 13 mars 2024. [Lien](#)

[121] SEAE. « Plan d'action Contre La Désinformation », 5 décembre 2018. [Lien](#)

et TikTok par exemple) ainsi que des acteurs de la publicité se sont engagés à le respecter [122]. Après les élections européennes de 2019, le Parlement européen s'est emparé du sujet en créant une commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE 1) dont une résolution a été votée en 2022, qui sera reconduite (INGE 2) et aboutira à la publication d'un rapport en 2023 [123]. Parmi leurs recommandations, les députés européens plaident notamment pour un cadre juridique commun en matière de vérification des faits, la promotion de l'éducation aux médias, l'établissement de clauses miroir selon lesquelles l'ouverture de l'espace européen de l'information aux pays tiers serait proportionnelle à l'accès dont disposent les médias européens dans ces pays. Le rapport recommande également d'exclure l'utilisation d'équipements et de logiciels provenant de fabricants établis dans des pays dit à haut risque, tels que la Chine, au vu des risques concernant la confidentialité et l'intégrité des données et des services. Plus récemment, le Parlement européen a créé le 18 décembre 2024 une commission spéciale sur le « bouclier européen de la démocratie » chargée d'évaluer la législation existante protégeant les processus démocratiques contre les ingérences étrangères, en se concentrant clairement sur les menaces que représentent les techniques de désinformation [124].

Un enjeu majeur auquel fait face l'UE est que la désinformation n'est en soi pas illégale. Elle ne peut donc pas l'interdire au risque de compromettre la liberté d'expression, mais seulement réduire sa propagation, en régulant le contenu des plateformes en ligne et en les sanctionnant, ou encourager des pratiques et des structures d'information libre et indépendante, à travers ses programmes et législations de garantie et de soutien à la liberté des médias.

La régulation des plateformes en ligne et des médias

Utilisant les armes dont elle dispose, c'est-à-dire le droit et le marché intérieur, l'UE a décidé de soumettre les plateformes numériques et les moteurs de recherche à des règles juridiques plus strictes sur son territoire par le biais de deux directives, entrées en application en août 2023 : le règlement sur les marchés numériques (Digital Markets Act - DMA) et le règlement sur les services numériques (Digital Services Act - DSA). Agir sur les plateformes en ligne est un levier d'autant plus important que le numérique est la principale source d'information des citoyens. Une étude menée par l'Institut Reuters et l'Université d'Oxford parue en 2024 montre que 62% des Français s'informent en ligne via des contenus numériques, dont 35% uniquement sur les réseaux sociaux [127].

[122] Commission européenne. « The 2022 Code of Practice on Disinformation », 16 juin 2022. [Lien](#)

[123] Parlement européen. « Rapport sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation », 15 mai 2023. [Lien](#)

[124] Parlement européen. Décision du Parlement européen du 18 décembre 2024 (2024/2999(RSO)) (2024). [Lien](#)

[125] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 (Digital Markets Act) (2022). [Lien](#)

[126] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act) (2022). [Lien](#)

[127] Newman, Nic, et al. « Reuters Institute Digital News Report 2024 ». Reuters Institute, 2024. [Lien](#)

Le DMA est davantage centré sur le droit de la concurrence et les activités économiques des grandes plateformes numériques mais le DSA apporte plusieurs contraintes pertinentes au regard de la désinformation. Suivant le mot d'ordre « *ce qui est illégal hors ligne doit également être illégal en ligne* », son but premier est d'interdire les contenus illicites (haineux, pédopornographiques, terroristes, etc.), y compris ceux provenant de médias, et la vente de produits illicites. Si le règlement ne peut imposer le retrait de contenu de désinformation du fait de leur caractère uniquement préjudiciable et non illégal, l'obligation de transparence d'une part impose aux plateformes d'explicitier le fonctionnement de leurs algorithmes, en particulier leurs systèmes de recommandation de contenu, et pour les très grandes entreprises, de proposer un système alternatif qui ne soit pas fondé sur le suivi des intérêts de l'utilisateur. D'autre part, l'obligation d'atténuation des risques les contraignent à évaluer et prendre des mesures face à la diffusion de contenus de désinformation. Les plateformes sont ainsi tenues, sous contrôle de la Commission européenne, de mieux configurer les algorithmes qui facilitent la propagation de fausses informations.

La responsabilité des plateformes numériques est d'ailleurs bel et bien rappelée par la Commission, qui a déjà ouvert six enquêtes à l'encontre de certaines d'entre elles pour cause de dérogations aux obligations du DSA, dont plusieurs relatives à des manquements dans la modération de contenus, notamment politiques, la transparence de la publicité ou encore d'accès aux données. Meta et X sont notamment accusés mais la dernière enquête ouverte le 17 décembre 2024 est à l'encontre du réseau social chinois TikTok, déjà ciblé deux fois au cours de l'année [128]. Les autorités roumaines accusent le réseau d'avoir permis une opération d'influence provenant de Moscou en pleine période électorale présidentielle en faveur du candidat prorusse Calin Georgescu, l'amenant à remporter le premier tour. TikTok aurait ainsi manqué à son obligation d'atténuer les risques d'ingérence étrangère en modérant les publicités et contenus politiques sponsorisés et en sécurisant ses algorithmes.

Si les enquêtes venaient à confirmer les accusations, le DSA prévoit une sanction des plateformes jusqu'à 6% de leur chiffre d'affaires annuel, voire une interdiction d'activité sur le territoire européen en cas de violations graves et répétées.

En matière de sanction, la Commission européenne a également interdit en Europe les médias d'Etat russe, *Russia Today* et *Sputnik*, après le début de l'invasion russe en Ukraine en 2022, en raison de leur diffusion de propagande russe.

[128] Commission européenne. « La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques en ce qui concerne les risques liés à l'intégrité des élections », 17 décembre 2024. [Lien](#)

Le soutien à la liberté et à l'indépendance des médias

Face aux risques de désinformation dans les médias ou par le biais de professionnels de l'information, que ce soit par la propriété étrangère de médias européens ou la corruption de journalistes, une des récentes législations de l'UE s'attache justement à protéger le pluralisme, l'indépendance et la liberté des médias en Europe. En vigueur depuis le 7 mai 2024, le règlement européen sur la liberté des médias (European Media Freedom Act, EMFA) tente de répondre aux défis rencontrés par la presse [129] : la multiplication des ingérences publiques et privées dans les décisions éditoriales, le manque de transparence dans la nomination du personnel, la dépendance aux revenus publicitaires ou encore la concentration des médias privés dans les mains de quelques propriétaires.

Le règlement prévoit alors de garantir le pluralisme et l'indépendance éditoriale en renforçant la transparence dans les processus de nomination ou de révocation des directeurs des médias publics et en leur garantissant un financement stable. Il invite également à évaluer les impacts des concentrations des médias sur leur liberté. Afin de mieux encadrer la publicité politique d'Etat, une pratique courante dans les pays de l'Est de l'Europe, les États seront tenus de transmettre les informations concernant les dépenses publicitaires versées à chaque média, tout comme les médias devront publier les fonds reçus par des autorités publiques. Il protège également les sources journalistiques en interdisant l'utilisation de logiciels d'espionnage à l'encontre de journalistes. Ce sujet était déjà au cœur des préoccupations des institutions, notamment du Parlement européen, suite au rapport publié en 2023 de la commission d'enquête sur l'utilisation du logiciel espion Pegasus et autres logiciels de surveillance équivalents par les gouvernements des Etats-membres notamment à l'encontre de journalistes.

La création d'un Comité européen pour les services de médias, rassemblant les autorités de régulation de chaque État-membre, devrait permettre de créer un rôle de superviseur des concentrations de médias jugées dangereuses pour la démocratie.

Les difficultés de financement étant l'un des problèmes identifiés par l'UE pour accéder à l'indépendance, la Commission a dirigé une partie de ses fonds européens vers le soutien à un journalisme de qualité. En outre, elle investit également dans l'éducation aux médias et la formation d'une culture numérique auprès des populations.

[129] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 (European Media Freedom Act) (2024). [Lien](#)

Elle a annoncé en octobre 2024 un budget de 16 millions d'euros pour trois appels à projet dans le cadre du programme Europe créative [130]. L'un d'entre eux vise par exemple à créer un système de surveillance de la propriété des médias. Elle propose également des outils pédagogiques à destination des enseignants afin de former les élèves du primaire et du secondaire aux effets néfastes de la désinformation. Ces initiatives font partie d'un plan d'action plus global de la Commission visant à protéger la démocratie européenne : en renforçant la résilience des citoyens, ces derniers deviennent moins vulnérables et sensibles aux manipulations de l'information. Certains chercheurs préconisent de compléter l'éducation aux médias et à l'information par une éducation à l'esprit critique car ils observent avant tout des mécanismes psychosociaux au contact de fausses informations [131].

c. Le rôle de la société civile : les actions de plaidoyer auprès des institutions européennes

La société civile s'est également engagée dans la lutte contre la désinformation, à l'image de l'organisation indépendante et non-lucrative EU Disinfo Lab (EUDL), basée à Bruxelles. Par ses travaux d'investigation et de recherche, elle développe une expertise sur le sujet de la désinformation en Europe afin d'accroître les capacités de détection, de lutte et de prévention ainsi que de soutenir la résilience de la société civile et des médias indépendants. Son activité est centrée sur le plaidoyer, à travers lequel elle élabore des recommandations de politiques publiques aux institutions européennes et aux Etats-membres. Son approche étant résolument horizontale, elle organise de nombreux événements, tels que des forums ou des webinaires, rassemblant des acteurs de la société civile, des ONG, des gouvernements, de l'industrie technologique et numérique ou encore des médias. Sa conférence annuelle est un des rares lieux qui rassemble la communauté d'acteurs investis dans la lutte contre la désinformation et en particulier dans la régulation des plateformes. La dernière, organisée à Riga le 9 et 10 octobre 2024, a permis de rassembler 560 personnes. Dans un rapport de novembre 2024, elle propose un nouveau cadre de réponse aux manipulations de l'information qui va au-delà des simples contre-mesures individuelles, souvent en réponse à un seul cas spécifique [132]. Elle fabrique ainsi des outils d'aide à la décision publique.

[130] Commission européenne. « La Commission met 16 millions d'euros à disposition pour soutenir le journalisme et l'éducation aux médias dans toute l'Europe », 22 octobre 2024. [Lien](#)

[131] Présidence de la République. « Les lumières à l'ère numérique », 11 janvier 2022. [Lien](#)

[132] Miguel Serrano, Raquel, et Maria Giovanna Sessa. « Beyond Disinformation Countermeasures: Building a Response-Impact Framework ». EU DisinfoLab, 29 novembre 2024. [Lien](#)

2. LES ACTEURS PUBLICS NATIONAUX

A l'échelle des Etats membres de l'UE, des initiatives de différentes natures ont émergé afin de contrer des campagnes de désinformation lancées dans le cadre d'ingérences étrangères. Trois approches différentes adoptées par les pays européens ont été identifiées. L'approche centralisée consiste à créer un service ou un département, au sein d'un organisme public existant, consacré à la lutte contre les ingérences étrangères sous la forme de désinformation. L'approche en réseau revient à créer une structure de type task force réunissant différents acteurs, notamment publics et privés, dans une collaboration pour lutter contre la désinformation et qui s'inscrit dans un événement précis ou une période déterminée. Enfin, l'approche décentralisée consiste à créer un organisme public indépendant, à part des autorités publiques mais en collaboration avec elles, et dédié à la lutte contre la désinformation.

a. Approche centralisée, l'exemple de VIGINUM en France

L'approche centralisée peut être illustrée par le service VIGINUM. Il s'agit du service technique et opérationnel de l'État français chargé de la vigilance et de la protection contre les ingérences numériques étrangères. Ce service est une des composantes du Secrétariat général de la défense et de la sécurité nationale (SGDSN) qui est lui-même placé sous l'autorité du Premier ministre. Créé en juillet 2021, son objectif principal est de protéger le débat public des « *manipulations de l'information provenant de l'étranger* » sur les plateformes numériques.

Son action principale est de détecter et caractériser les « ingérences numériques étrangères » et d'en rendre compte aux autorités et au public. Pour VIGINUM, les ingérences numériques étrangères se définissent comme des « phénomènes inauthentiques » qui affectent le débat public dans l'espace numérique et qui combinent quatre critères : « *une atteinte potentielle aux intérêts fondamentaux de la Nation ; un contenu manifestement inexact ou trompeur ; une diffusion artificielle ou automatisée, massive et délibérée* » ainsi que « *l'implication, directe ou indirecte d'un acteur étranger (étatique, paraétatique ou non-étatique)* ». Ce service d'investigation en ligne analyse les agissements, modes opératoires et moyens mis en œuvre par des acteurs étrangers « malveillants » pour propager des contenus portant atteinte aux intérêts et valeurs du pays.

Ce service est composé de spécialistes en investigation et analyse numérique mais aussi de data scientists pour l'analyse et le traitement des données. Ils travaillent exclusivement à partir de contenus publiquement accessibles sur les plateformes en ligne, les sites internet et les médias web en utilisant la méthode d'information en sources ouvertes - Open Source Intelligence (OSINT). Cela désigne « *un ensemble hétéroclite de pratiques d'investigation et d'analyse visant à dévoiler une information préalablement dissimulée en récoltant, croisant ou analysant des données numériques disponibles en source ouverte* » [133], c'est-à-dire à partir de sources d'information publique. Le service VIGINUM est surtout mobilisé en période électorale pour sécuriser les scrutins mais aussi lors de grands événements susceptibles d'être instrumentalisés par des acteurs étrangers malintentionnés.

Ce fut le cas récemment avec la tenue des Jeux Olympiques et Paralympiques à Paris à l'été 2024. Dans ce cadre, VIGINUM a publié deux guides en amont de l'événement, un à destination des médias et journalistes [134] et un autre à destination des acteurs économiques [135], afin de faire connaître la « menace informationnelle » et de diffuser des bonnes pratiques à adopter pour s'en prémunir. A la suite de l'événement, VIGINUM a publié un rapport [136], faisant le bilan de la désinformation, provenant notamment d'acteurs étrangers, autour des Jeux Olympiques et Paralympiques. Selon ce rapport, 43 « manœuvres informationnelles » ont été repérées et deux campagnes de désinformation numériques planifiées et coordonnées ont été caractérisées, dont l'une s'intitulait « OLIMPIYA » et impliquait des acteurs pro-azerbaïdjanais. Le rapport fait état de tentatives de déstabilisation via de nombreuses méthodes de désinformation comme la création de contenus inauthentiques, notamment générés grâce à l'intelligence artificielle ou en usurpant l'identité d'organisations officielles, le recours non transparent à des influenceurs, la création et l'amplification d'hashtags.

VIGINUM effectue donc un travail important de surveillance et de ciblage des actions de désinformation d'origine étrangère en France. Cependant, certaines limites peuvent être identifiées concernant leur action. D'abord, VIGINUM a une mission défensive et se concentre majoritairement sur la détection des ingérences numériques étrangères, dont le service rend compte. Néanmoins, la question de la sensibilisation et de la formation à un large public n'est pas encore présente parmi ses missions alors qu'il s'agit d'un pan important de la lutte contre la désinformation dans le cadre d'ingérences étrangères. Par ailleurs, il semble pertinent de poser la question de l'impact des actions de lutte contre la désinformation menées par VIGINUM sur la population. Selon une enquête de la Fondation

[133] Kévin Limonier et Maxime Audinet. « De l'enquête au terrain numérique: les apports de l'Osint à l'étude des phénomènes géopolitiques ». *Hérodote*, 11 octobre 2022. [Lien](#)

[134] Secrétariat général de la défense et de la sécurité nationale. « Guide de sensibilisation à la menace informationnelle à destination des médias et journalistes fact-checkeurs », 25 juillet 2024. [Lien](#)

[135] Secrétariat général de la défense et de la sécurité nationale. « Guide de sensibilisation à la menace informationnelle à destination de l'écosystème des acteurs économiques associés aux JOP24 », 20 juin 2024. [Lien](#)

[136] Secrétariat général de la défense et de la sécurité nationale. « Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024 », 13 septembre 2024. [Lien](#)

Jean Jaurès [137], les pratiques de lutte contre la désinformation font l'objet de nombreuses critiques. Cette enquête montre, par exemple, qu'une majorité de Français sont d'avis que le fait de qualifier dans le débat public un fait ou une information comme de la désinformation revient à de la censure, notamment politique, et donc à restreindre la liberté d'expression. Cela montre que l'impact des actions de lutte contre la désinformation pourrait s'avérer finalement mitigé au sein de la population française.

b. Approche en réseau, l'exemple du Bureau électoral national d'Estonie

Le deuxième type d'approche, dite en réseau, peut être illustré par l'initiative du Bureau électoral national d'Estonie en matière de lutte contre la désinformation. Dans le contexte des tentatives d'influence et de désinformation sur les élections américaines de 2016 par des groupes proches de la Russie, le directeur du Bureau électoral national d'Estonie, Priit Vinkel, a créé, en 2016, le groupe de travail « election communications task force » pour protéger la population de la désinformation dans un contexte électoral [138]. Cette initiative a été mise en place notamment en prévision des élections locales de 2017 ainsi que nationales et européennes de 2019. Le mandat de cette task force concernait la surveillance de tous les messages liés aux élections, en particulier la désinformation.

Le directeur du Bureau électoral national estonien a adopté cette « approche en réseau » afin de combler le manque de personnel et de moyens. Par ailleurs, le Bureau électoral national a un mandat qui limite ses activités aux élections. La désinformation électorale étant souvent mélangée à d'autres messages concernant la politique étrangère de l'Estonie ou ses politiques intérieures à l'égard de la minorité russe du pays, la collaboration en réseau avec d'autres acteurs était essentielle pour le directeur du Bureau. Au sein de la task force, il y a d'abord eu une coopération étroite avec d'autres entités publiques et gouvernementales estoniennes. Plusieurs membres du Bureau du gouvernement (« Government Office »), de l'Autorité des systèmes informatiques, du ministère des Affaires étrangères et du ministère de l'Intérieur estoniens faisaient partie de ce groupe de travail.

Ensuite, le groupe de travail a établi des partenariats avec les représentants régionaux des grandes entreprises de média sociaux, comme Facebook, Twitter, Google et Microsoft, pour endiguer des campagnes de désinformation sur ces plateformes. L'Estonie, par le biais de cette task force, s'est rapprochée de ses pays voisins pour mettre en place un échange de bonnes pratiques dans la lutte contre la désinformation. Le pays a aussi établi une coopération avec l'Union européenne sur ces sujets, s'impliquant dans la East StratCom Task Force et le site web EUvsDisinfo.

[137] Guillaume Caline et Laurence Vardaxoglou. « Regard des Français sur la lutte contre la désinformation ». Fondation Jean Jaurès, 5 novembre 2024. [Lien](#).

[138] Tyler McBrien. « Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016-2020, *Innovations for Successful Societies*, Princeton University, 2020. [Lien](#)

Enfin, les membres de la task force se sont rapprochés des journalistes et rédacteurs en chef des médias et journaux les plus importants d'Estonie pour multiplier la portée de leur travail. Ces différentes collaborations ont été créées grâce à l'approche en réseau utilisée par le Bureau électoral national estonien pour lutter contre la désinformation.

Les actions de la task force se divisaient en deux volets. Le premier pan de ces actions est un travail de surveillance et de détection de la désinformation sur les médias traditionnels et les réseaux sociaux. Le Bureau électoral national estonien s'est appuyé sur les ressources humaines et techniques de ses partenaires au sein de la task force afin de détecter la désinformation électorale. Dans ce cadre, la task force s'est aussi appuyée sur la société civile, notamment Propastop, un blog indépendant animé par des volontaires anonymes qui analyse les campagnes et narratifs de désinformation provenant de la Russie. Le deuxième volet des actions de la task force est les actions de sensibilisation et de formation aux médias (« media literacy »). De nombreuses formations ont été organisées auprès de la société civile, des médias et de la presse.

Durant cette période, le gouvernement estonien a augmenté les fonds octroyés à l'éducation dans ce domaine et a aussi introduit dans les programmes un cours obligatoire sur le sujet de la manipulation de l'information.

Le groupe de travail « election communications task force » a donc œuvré pour la lutte contre la désinformation d'origine étrangère en Estonie par ses actions en réseau de surveillance et de sensibilisation. Cependant, plusieurs limites à ce modèle peuvent être identifiées. La première limite est la frontière entre la désinformation et la liberté d'expression, qui est un des obstacles auxquels la task force a eu à faire face. Il s'agit d'une question épineuse car assurer la liberté d'expression revient aussi à assurer la « *liberté de mentir* », selon une des personnes interrogées par Tyler McBrien [139]. Une deuxième limite est que l'action de la task force était restreinte au seul sujet des élections. Même si les périodes électorales sont des terrains particulièrement fertiles à la désinformation, elle peut aussi avoir lieu dans d'autres contextes lors desquels cette task force ne peut agir. Une dernière limite est celle qui était déjà posée dans le cadre de l'analyse des actions de VIGINUM : la question de l'impact des actions de la task force sur la population estonienne dans le cadre des élections de 2017 et 2019. Étant impossible d'établir des indicateurs assez précis, le gouvernement estonien a conduit des sondages d'opinion pour essayer de mesurer l'influence de la désinformation sur les citoyens estoniens. Plus de la moitié des répondants affirment savoir reconnaître des fausses informations dans les médias et sur les

[139] McBrien, Tyler. *Op. cit.*

réseaux sociaux. Seulement une minorité de répondants pense que la désinformation est un sujet d'inquiétude. Les personnes interrogées ont également déclaré qu'elles réagissaient plus souvent aux fausses informations identifiées en ligne en les ignorant ou en les partageant délibérément parce qu'elles étaient amusantes qu'en réagissant de manière plus constructive, par exemple en les vérifiant auprès de sources plus fiables, en informant les plateformes de médias sociaux de leur existence ou en commentant l'information pour la réfuter. Malgré ces résultats, il est difficile d'évaluer le véritable impact des actions de la task force sur les citoyens estoniens.

c. Approche décentralisée, l'exemple de l'Agence de défense psychologique suédoise

Enfin, l'Agence de défense psychologique de Suède est un exemple pour le dernier type d'initiative des Etats membres de l'UE en matière de lutte contre la désinformation, l'approche décentralisée. Créée en 2022, il s'agit d'un organisme public à part du gouvernement suédois mais auquel celui-ci a donné mandat d'agir en tant que coordinateur principal des efforts en matière de défense psychologique. L'objectif principal de cette agence est de diriger la coordination et le développement des actions menées par les autorités et les autres acteurs de la défense psychologique de la Suède, de soutenir ces actions et de contribuer à accroître la résilience de la population en cas de paix ainsi qu'en cas de crise. Elle aide notamment les autorités régionales et locales, les entreprises et les organisations non gouvernementales à renforcer leur résilience en matière de défense psychologique.

Selon le dernier rapport de l'Agence suédoise de défense psychologique [140], quatre principes permettent de définir la défense psychologique. Le premier principe est la résilience qui se traduit par les efforts pour renforcer la résistance de la société à des menaces et réduire les vulnérabilités dans les systèmes et les institutions. Le deuxième principe est le fait de comprendre et traquer les menaces extérieures (« threat intelligence »). Le troisième principe est la dissuasion (« deterrence ») qui consiste à renforcer les mesures politiques et opérationnelles dont dispose un pays pour protéger sa population et, dans la mesure du possible, atténuer le comportement des acteurs de la menace. Le quatrième principe est la communication stratégique (« strategic communication ») qui se définit par la capacité à se préparer, à réagir et à façonner l'environnement informationnel afin de minimiser l'impact des menaces d'origine étrangère sur le public. La désinformation établie dans le cadre d'ingérences étrangères fait partie du

[140] James Pamment et Elsa Isaksson. « Psychological Defence: Concepts and Principles for the 2020s ». Lund University Psychological Defence Research Institute, juin 2024. [Lien](#)

champ d'application du concept de défense psychologique de l'agence suédoise, en ce qu'elle s'apparente à une « propagande étrangère hostile » (« hostile foreign propaganda »).

L'Agence de défense psychologique suédoise est chargée de coordonner les actions menées dans le cadre de ces quatre principes mais d'autres agences ont des mandats spéciaux à agir dans l'un ou l'autre de ces principes. Un premier pan important des actions de cette agence est qu'elle doit identifier, analyser et contrer les activités d'information et d'influence étrangères malveillantes et les autres formes de désinformation dirigées contre la Suède ou ses intérêts. Ce volet d'actions est mené par le département des opérations de l'agence (« operation department ») dont sont issus des rapports qui analysent les modes opératoires des campagnes de désinformation, les vulnérabilités et les acteurs menacés et qui recommandent des mesures pour les contrer. Le deuxième volet d'actions de l'agence est la sensibilisation et la formation à la défense psychologique. Il s'agit d'un pan d'activités très développé qui consiste à améliorer et développer la capacité globale de la société en matière de défense psychologique. Ces actions sont menées par le département pour le développement des capacités (« capability development department »). Cela implique principalement le développement de la recherche, de la formation et des partenariats internationaux. Un exemple révélateur est la campagne « Don't get fooled » qui vise à donner les outils à chaque individu d'apprendre à reconnaître de fausses informations. L'Agence de défense psychologique de Suède est érigée en modèle d'organisation de lutte contre la désinformation, en particulier dans le cadre d'ingérences étrangères.

Il est pertinent de se poser la question de la reproductibilité d'un tel modèle à l'échelle européenne voire d'envisager une agence européenne de défense psychologique.

Ce type d'approche nécessite néanmoins une importante coordination et une volonté égale de la part de chaque partie prenante à lutter contre la désinformation. Cela impliquerait également que tous les États membres soient en accord sur le type de menaces qui seraient gérées par une telle agence. Le manque de définitions communes au niveau européen complique la mise en place d'une agence européenne de défense psychologique. Par ailleurs, d'après un rapport d'une commission d'enquête au Sénat à ce sujet [141], cette agence fonctionnerait en Suède car elle est adaptée au système et à la population, qui démontre d'une « forte confiance » envers les autorités et les principaux médias.

[141] Sénat. « Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide », 23 juillet 2024. [Lien](#)

3. LES ACTEURS PRIVÉS

Si les institutions européennes et nationales de chaque État-membre de l'UE ont réagi à ces vagues de désinformation en créant des structures, des normes ou encore en sensibilisant les cibles, elles ne peuvent agir seules. En effet, elles doivent agir de concert avec les acteurs qui contrôlent les flux d'information sur internet et ceux qui la produisent. Par conséquent, si les entreprises du numérique sont incontournables dans la gestion de la désinformation (b), il convient aussi de s'intéresser aux journalistes, potentiels relayeurs de désinformation (a).

a. Les entreprises de presse : agences de fact-checking et collectifs de journalistes

Alors que publier une information sourcée et sûre est ce qui caractérise le métier de journaliste, il n'en demeure pas moins qu'ils sont eux-aussi confrontés à la désinformation. Les techniques de désinformation la rendant de plus en plus crédibles (deep fakes, IA), les journalistes doivent renforcer leur vérification de l'information avant de la diffuser. Pour autant, l'évolution du métier permet de moins en moins de prendre ce temps. En effet, la profession de journaliste se précarise et ces derniers effectuent de plus en plus de piges plutôt que d'être rattachés à une entreprise de presse. Par conséquent, le rythme devient très important et mène certains journalistes à moins bien vérifier leurs sources. Ainsi, les entreprises et agences de presse mettent en place des systèmes de fact checking qui permettent de croiser les informations pour la produire. Si cette technique est destinée aux professionnels, la sensibilisation du public reste la priorité.

Le fact checking : à destination des journalistes, du grand public et des entreprises

Le fact checking, ou « vérification des faits », est une nouvelle technique journalistique permettant aux professionnels de l'information de relayer des nouvelles sourcées. Elle se développe dans un premier temps sous l'influence de fausses informations. En effet, le premier est le corollaire de l'autre car sans désinformation, il y aurait moins besoin de fact checking. Pour autant, aujourd'hui, tous les journaux européens disposent d'une cellule dédiée à la vérification des faits tel que le leader de l'information en France, l'Agence France Presse (AFP).

L'AFP crée en 2017 l'AFP Fact Check. Dès sa création, 21 journalistes sont dédiés à cette tâche et en un an, sont écrits 654 articles vérifiant des cas de désinformation. Aujourd'hui, l'AFP Fact Check est un service payant adressé aux entreprises de presse et aux journalistes. Il joue un rôle essentiel dans la lutte contre la désinformation en vérifiant les faits de manière rigoureuse et transparente. Grâce à une équipe dédiée de journalistes, plus étoffée qu'en 2017, répartie dans le monde entier, l'AFP identifie les fausses informations circulant sur internet, notamment sur les réseaux sociaux, et publie des analyses détaillées pour en démontrer l'inexactitude. En s'appuyant sur des outils sophistiqués, tels que la recherche inversée d'images et l'analyse de données, ainsi que sur des sources fiables, l'AFP démystifie les rumeurs et corrige les informations erronées. Pour autant, leur travail ne se limite pas à dénoncer les fausses informations : ils expliquent également les processus de vérification, sensibilisant ainsi le public à l'importance de consulter des sources fiables. Ce service est un atout majeur pour les journalistes, car il leur fournit des informations vérifiées et des méthodologies solides pour leurs enquêtes. En collaborant avec des plateformes numériques, l'AFP contribue également à limiter la propagation de fausses informations à grande échelle.

En fin de compte, leur travail renforce la confiance dans les médias professionnels et soutient un écosystème médiatique basé sur la vérité et la transparence.

Pour autant, en France, il est arrivé que des journalistes soient impliqués dans des affaires de désinformation. En 2017, des soupçons ont notamment émergé autour de Rachid M'Barki, présentateur de BFMTV, accusé d'avoir diffusé des contenus non validés par sa rédaction et potentiellement fournis par des agences impliquées dans des campagnes de manipulation de l'information. Alors même que sa chaîne d'information est liée à l'AFP Fact Check, les segments insérés dans ses journaux télévisés portaient sur des sujets sensibles favorisant les intérêts de clients privés, remettant en question les standards d'indépendance journalistique. Cette controverse a conduit à une enquête approfondie qui a révélé un réseau bien plus large de désinformation organisé.

Pour se prévaloir de ces ingérences qui passent par des sites internet ou encore les réseaux sociaux, Guillaume Kuster a créé un logiciel permettant d'identifier, pour ceux qui l'achètent, des cas de désinformation. Basée à Helsinki, l'entreprise CheckFirst joue un rôle clé dans la lutte contre la désinformation grâce à ses logiciels et méthodologies innovantes. Spécialisée dans le développement d'outils de veille et d'analyse, elle détecte les réseaux de propagande, analyse leurs techniques et établit des liens entre différentes opérations et acteurs responsables. CheckFirst vend ces outils à des fact-checkers et orga-

nisations, renforçant ainsi les capacités de lutte contre la désinformation. Elle publie aussi des rapports, comme celui sur l'opération Overload, qui a mis en lumière des campagnes russes visant à saturer les fact-checkers. En entretien, G. Kuster nous a aussi spécifié que l'entreprise collabore également avec des acteurs internationaux, notamment dans des initiatives en Afrique francophone avec l'Organisation Internationale de la Francophonie. Elle suit aussi de près l'application du DSA de l'UE, qu'elle considère comme une avancée majeure en matière de régulation des plateformes.

Enfin, en enquêtant sur des campagnes de manipulation, comme l'utilisation de publicités sur Meta pour contourner la modération, CheckFirst alerte sur les défaillances des algorithmes et des politiques des plateformes. Elle documente aussi des phénomènes sur des plateformes, comme la présence de livres anti vaccins sur le Kindle Store d'Amazon. Par conséquent, CheckFirst combine expertise technique et compétences journalistiques pour analyser les ingérences, enquêter sur les algorithmes et inciter les plateformes à adopter des pratiques plus transparentes. Ainsi, si ces techniques de lutte contre la désinformation sont essentiellement pour les professionnels, des médias de fact checking veillent aussi à sensibiliser le grand public.

Médias de lutte contre la désinformation à destination du grand public

Si les journalistes doivent se prévaloir de la désinformation, des médias sont spécialisés dans la vérification des faits. A cet égard, l'initiative du média *Les Surligneurs* est intéressante. Il s'agit d'un collectif de juristes spécialisés dans le fact-checking des déclarations publiques et en particulier celles des responsables politiques. Leur mission est de détecter et corriger les usages erronés ou trompeurs du droit dans les discours, une facette souvent négligée de la désinformation selon Vincent Couronne, le fondateur du média [142]. En analysant des propos relatifs à des sujets comme l'économie, l'environnement, ou les droits fondamentaux, ils montrent comment des concepts juridiques sont parfois déformés pour influencer l'opinion publique. À cet égard, V. Couronne nous a expliqué que les Surligneurs utilisent une approche pédagogique : leurs analyses, publiées sous forme d'articles courts, expliquent le cadre légal réel en contrastant avec les affirmations incorrectes ou exagérées des personnalités publiques. Ils rendent leurs sources accessibles et compréhensibles pour que le grand public puisse s'appropriier les éléments juridiques et mieux déceler les manipulations. Leur travail repose également sur un respect strict de l'éthique journalistique et s'inscrit dans le mouvement mondial de fact checking, notamment au sein du réseau International Fact-Checking Network (IFCN). Ainsi, leur action aide les citoyens à comprendre les implications réelles des discours politiques et constitue aussi un outil précieux pour les journalistes, qui peuvent ainsi disposer de bases solides pour des enquêtes approfondies et critiques. Par conséquent, la sensibilisation du grand public à la désinformation est une priorité de leur travail.

[142] Propos confiés lors de l'entretien réalisé par notre équipe le 29 septembre 2024.

Des initiatives d'envergure européenne sont également remarquables, comme en témoigne le cas du European Digital Media Observatory (EDMO). EDMO est une initiative du plan d'action de la Commission européenne contre la désinformation, visant à renforcer la coopération entre les États membres et l'UE dans plusieurs domaines stratégiques. Géré par un consortium dirigé par l'Institut universitaire européen de Florence, en collaboration avec l'Athens Technology Center, l'Université Aarhus et Pagella Politica, l'EDMO bénéficie d'une gouvernance totalement indépendante des pouvoirs publics, y compris de la Commission. Cette structure comprend un conseil consultatif, chargé de définir les règles et la stratégie, ainsi qu'un conseil exécutif, responsable de la mise en œuvre des actions.

EDMO agit sur quatre axes majeurs : améliorer la détection de la désinformation, coordonner les réponses, collaborer avec les plateformes et sensibiliser les citoyens pour les rendre plus résilients face aux fake news. Parmi ses activités, EDMO publie des rapports mensuels sur les tendances de la désinformation, des guides de bonnes pratiques, mène des enquêtes collaboratives, cartographie les organisations de fact checking en Europe, propose une base de données multilingue de vérifications et organise des formations pour les vérificateurs de faits. En outre, EDMO développe des lignes directrices pour les pouvoirs publics et promeut l'éducation aux médias, contribuant ainsi à un écosystème européen plus transparent et résistant à la manipulation en ligne. Par ailleurs, à l'occasion d'un entretien, l'agence pointait aussi l'importance du maillage qu'elle avait créé. En effet, chaque journal ou entreprise peut rejoindre le consortium pour effectuer des formations ou même participer à la sensibilisation à la désinformation en relayant les lignes directrices. Pour autant, EDMO s'abstient de travailler et de collaborer avec les institutions nationales car cela rompt avec leur vision où la sensibilisation directe est la meilleure des manières pour lutter contre la désinformation.

Ainsi, le grand public est une cible privilégiée par les agences de fact checking. Pour autant, la majorité de l'information recueillie par les citoyens européens provient des réseaux sociaux.

En effet, 61% des internautes hongrois, 50% des internautes polonais et 43% des internautes belges utilisent les réseaux sociaux comme source d'information [143].

L'encadrement et la vérification des flux sur ces plateformes est donc capital.

[143] Valentine Fourreau. « Réseaux sociaux : où sont-ils les plus utilisés pour s'informer ? » Statista, 11 mars 2024. [Lien](#)

b. L'action des grandes entreprises du numérique dans la lutte contre la désinformation

Google, Meta, X ou encore Telegram structurent une grande partie de l'accès à l'information mondiale et ont une responsabilité majeure dans la lutte contre la manipulation de l'opinion publique et les ingérences étrangères. Le déploiement d'instruments adaptés par ces acteurs est indispensable pour compléter les efforts des journalistes et garantir un écosystème numérique fiable et sécurisé. Par conséquent, nous proposons une analyse de la réponse de quelques plateformes et leurs réactions face à des situations portant atteinte à l'opinion publique tout en montrant les limites. En effet, même si les instruments déployés sont importants, ils ne sont pas suffisants dans la lutte contre la désinformation.

Google : un acteur clé dans la lutte contre la désinformation à l'ère numérique

Avec 85 milliards de visites en 2024, Google est la première plateforme visitée au monde [144]. Son action est par conséquent déterminante dans la lutte contre la désinformation. Ainsi, Google déploie une stratégie renforcée pour contrer la désinformation en ligne s'appuyant sur des initiatives variées, alliant éducation, sécurité et innovation technologique.

Pour offrir un espace sûr, Google mobilise ses plateformes et ses outils. Le Fonds européen pour les médias et l'information (EMIF), auquel l'entreprise contribue à hauteur de 25 millions d'euros sur 5 ans, a permis de financer 70 projets dans 24 pays, axés sur la vérification des faits et l'éducation aux médias. Google et son unité Jigsaw ont également lancé des campagnes de pré-bunking, visant à sensibiliser les citoyens en amont aux tactiques de désinformation, comme la décontextualisation ou la sélection biaisée d'informations. Des vidéos éducatives ont aussi été créées et seront diffusées en France, en Allemagne, en Italie, en Belgique et en Pologne.

Par ailleurs, Google renforce ses efforts pour identifier et limiter les contenus synthétiques trompeurs, tels que les deepfakes. Par exemple, les annonceurs électoraux doivent désormais signaler tout contenu manipulé, et YouTube affiche des avertissements clairs sur ces vidéos. Ces mesures s'accompagnent d'outils de protection avancée, comme *Project Shield*, qui protège les sites web de responsables politiques contre les attaques DDoS (attaques par déni de service où l'affluence est telle que le site internet plante), ou encore

[144] Statista. « Les sites internet les plus consultés au monde en 2024 », juin 2024. [Lien](#)

le programme de protection avancée, destiné à sécuriser leurs comptes.

Google s'engage également auprès des équipes de campagne, en leur fournissant des formations en cybersécurité et un accès à un centre d'information dédié aux élections européennes. Par exemple, lors du scrutin de 2019, plus de 2 500 responsables de campagne ont bénéficié de ces sessions. À cela s'ajoutent les analyses de *Mandiant Intelligence*, qui surveille les opérations d'influence et les campagnes de cyberespionnage, tout en collaborant avec les autorités publiques pour partager des informations sur les menaces émergentes.

Pour autant, si Google est important dans ce travail de lutte, Facebook (Meta), troisième plateforme la plus consultée au monde [145] déploie aussi des outils notamment après le scandale de « Cambridge Analytica ».

Les limites de Meta face aux enjeux de désinformation et de protection des données

L'affaire « Cambridge Analytica », révélée en 2018, a exposé une exploitation massive et abusive des données personnelles à des fins de manipulation politique, mettant en lumière les failles de Facebook en matière de protection de la vie privée. Cambridge Analytica, une société britannique spécialisée dans le marketing politique, avait collecté les données personnelles de plus de 87 millions d'utilisateurs de Facebook via une application tierce, un quiz prétendument destiné à des recherches académiques. En réalité, ces informations ont servi à créer des profils psychologiques détaillés, permettant de cibler des publicités politiques extrêmement personnalisées. Ces campagnes de « microciblage » ont été utilisées pour influencer des scrutins majeurs, notamment la campagne présidentielle américaine de 2016, où Cambridge Analytica a travaillé pour Donald Trump, et le référendum sur le Brexit. Ce scandale, révélé par Christopher Wylie en 2020 [146], montre des lacunes importantes dans la gouvernance de Facebook, qui n'avait pas détecté ni empêché l'utilisation abusive des données et a tardé à informer les utilisateurs. En conséquence, Facebook a été condamné à une amende record de 5 milliards de dollars par la Federal Trade Commission (FTC), et l'affaire a accéléré les appels à une réglementation stricte des données personnelles, comme le RGPD en Europe. Ce cas emblématique a mis en évidence les risques de manipulation démocratique à l'ère numérique et la responsabilité des grandes plateformes dans la sécurisation des informations de leurs utilisateurs.

Par conséquent, Facebook, devenu Meta en 2020, a réagi en créant l'instrument *Crowd Tangle*. Sous l'influence du Congrès américain, l'outil permet d'avoir accès de manière totalement transparente aux publications les plus likées ou encore les plus vues par les

[145] Statista. *Op. cit.*

[146] Christopher Wylie. *Mindfuck: le complot Cambridge Analytica pour s'emparer de nos cerveaux*, 2020. [Lien](#)

utilisateurs. Cela a permis à des journalistes d'analyser par ordre croissant les publications les plus vues pour mieux les analyser et prouver la désinformation lorsqu'elles en relataient. Pourtant, depuis le 14 août 2024, sous l'influence de la législation du DSA, Meta remplace cet outil par le *Meta Content Library*. Les professionnels dont G. Kuster, CEO de CheckFirst, dénoncent une moins bonne couverture de la désinformation alors que l'ancien était plus performant. En effet, seuls des chercheurs peuvent avoir accès aux données de Meta alors qu'ils ne sont pas assez nombreux pour répondre efficacement à la désinformation. Par ailleurs, à partir du 14 août dernier, date à laquelle Meta supprime l'outil Crowd Tangle, 76 Etats dans le monde organisent des élections, dont les Etats-Unis. Si la porte-parole de Meta met en avant les nouveautés permises par la nouvelle bibliothèque créée, selon Melanie Smith, directrice de recherche de l'Institute for Strategic Dialogue « *la suppression de l'accès à Crowd Tangle limitera considérablement la surveillance indépendante des dommages* » causés par la désinformation et aura une influence sur l'opinion publique [147].

Ce n'est pas le seul changement qu'opère Meta dans ses pratiques de modération : Mark Zuckerberg a annoncé le 7 janvier 2025 « mettre fin à son programme de fact-checking » aux Etats-Unis.

Invoquant des raisons « *idéologiques* », il souhaite le remplacer par un système de *community notes*, déjà utilisé sur X, et se rapproche ainsi de la politique du réseau d'Elon Musk, qui joue sur la fine ligne entre liberté d'expression et désinformation. En effet, X a aussi été épinglé dans son rôle limité dans la lutte contre la désinformation.

Les défis de la modération sur X : entre liberté d'expression et dérives

Après le rachat de Twitter par Elon Musk le 14 avril 2022, le programme *Birdwatch*, lancé en 2021, a été supprimé. Il impliquait directement les utilisateurs dans le signalement et l'annotation des tweets potentiellement problématiques. Par ailleurs, la plateforme avait interdit les publicités politiques dès 2019, estimant qu'elles pouvaient nuire à la démocratie. Twitter s'appuyait également sur des algorithmes pour limiter la visibilité des contenus nuisibles et mettait en avant des informations fiables lors de crises majeures, comme la pandémie ou les élections. Ces efforts étaient complétés par des partenariats avec des organisations de fact-checking et des institutions comme l'Organisation Mondiale de la Santé. Toutefois, après le rachat par Elon Musk, certaines de ces politiques ont été remises en question ou supprimées, suscitant des inquiétudes quant à l'intégrité de l'information sur la plateforme.

[147] L'Express. « Désinformation : quelles conséquences après la suppression de CrowdTangle par Meta ? » 2 avril 2024. [Lien](#)

En effet, Musk joue sur la fine ligne qui sépare liberté d'opinion, d'expression et désinformation. Dès son achat, le milliardaire explique vouloir faire de X une plateforme ouverte où la liberté d'expression est garantie. Pour autant, même si la désinformation est toujours une cible pour la plateforme, les plans mis en œuvre luttant contre cette dernière sont minces et les publications relayant de la désinformation sont peu supprimées. Le dirigeant du réseau social est par ailleurs lui-même un relai de désinformation comme le montre un article publié par *Le Monde* [148]. Le 30 octobre 2022, il relaie par exemple une théorie complotiste homophobe et le 16 novembre 2022, il refuse de modérer une rumeur de mort. Enfin, depuis le 7 octobre 2023, un déferlement de fausses informations après l'attaque du Hamas est perceptible sur la plateforme. En outre, l'observatoire international de la désinformation sur le climat, le CAAD, publie un rapport [149] évaluant l'action des cinq principaux réseaux sociaux et X y est classé dernier. Le rapport cible que la plateforme « *va dans la mauvaise direction* ». Elle souligne aussi que l'affaiblissement de la modération et la politique du *free speech* d'Elon Musk ont conduit à une forte augmentation du climatoscepticisme sur la plateforme.

Enfin, on remarque de plus en plus de proximité entre les plateformes et les candidats politiques. En témoigne par exemple l'affaire Cambridge Analytica dans laquelle Facebook était impliquée, mais aussi la proximité entre X, E. Musk et D. Trump, ou encore le don de Google en soutien à la candidature de K. Harris aux dernières élections présidentielles américaines. Il apparaît ainsi que les plateformes sont proches du système politico-institutionnel. Cette même proximité est similairement perceptible entre TikTok et les intérêts géopolitiques chinois.

TikTok et la désinformation : enjeux géopolitiques et manipulations électorales

TikTok, application prisée par des millions d'utilisateurs [150], suscite des craintes croissantes en Europe en raison de ses liens avec Pékin et de son potentiel à diffuser de la désinformation. Une tribune dans *Le Monde*, publiée par la juriste Isabelle Feng [151], révèle que des changements majeurs dans la gouvernance de ByteDance, maison mère de TikTok, ont permis à des entités étatiques chinoises, comme la Cyberspace Administration of China, d'acquérir un contrôle stratégique. En 2021, celles-ci ont obtenu un siège au conseil d'administration avec droit de veto, tandis que le fondateur de ByteDance, Zhang Yiming, a cédé ses parts à une société mystérieuse, Xiamen Xingchen Qidian Technology. Ces manœuvres renforcent la suspicion que TikTok pourrait être influencé politiquement par le Parti communiste chinois (PCC), comme l'illustre la nomination de Wu Shugang, cadre du PCC connu pour ses positions anti-droits humains.

[148] William Audureau et Manon Romain. « Un an de désinformation et d'errements stratégiques d'Elon Musk sur Twitter, puis sur X en 40 dates clés ». *Le Monde*, 27 octobre 2023. [Lien](#)

[149] « Deny, Deceive, Delay (Vol 3): Climate Information Integrity Ahead of COP28 ». Climate Action Against Disinformation, 29 novembre 2023. [Lien](#)

[150] Statista. *Op. cit.*

[151] Isabelle Feng. « Derrière TikTok se profile l'ombre du Parti communiste chinois ». *Le Monde*, 14 avril 2023. [Lien](#)

L'élection présidentielle roumaine de 2023 illustre de manière inquiétante le rôle que TikTok peut jouer dans la propagation de la désinformation et les manipulations politiques à grande échelle. À l'approche du scrutin, des rapports de renseignement ont révélé une activité suspecte sur la plateforme: 25 000 comptes TikTok sont devenus soudainement très actifs à la mi-novembre, soit deux semaines avant le premier tour de l'élection. Ces comptes, vraisemblablement coordonnés, ont amplifié des messages favorables à Călin Georgescu, un candidat d'extrême droite largement considéré comme prorusse.

Ce soutien numérique, jugé illicite et présumément orchestré par Moscou, a bouleversé la campagne. Initialement crédité de seulement 1% des intentions de vote en septembre, Georgescu a créé la surprise en arrivant en tête du premier tour avec 22,94 % des suffrages. Cette ascension soudaine a soulevé des soupçons sur la légitimité de son soutien en ligne, renforcés par des accusations de recours à des influenceurs payés pour diffuser de la propagande ciblée. Les autorités roumaines ont signalé que cette campagne sur TikTok s'inscrivait dans une stratégie plus large visant à déstabiliser le processus électoral. Face à ces révélations, la Cour constitutionnelle roumaine a pris une décision sans précédent en annulant les résultats de l'élection présidentielle.

Cette annulation met en lumière la puissance des réseaux sociaux dans les démocraties modernes, où une campagne numérique peut potentiellement modifier les résultats électoraux et influencer les perceptions publiques.

Par ailleurs la plateforme TikTok a reconnu de manière indirecte ces influences en supprimant des « réseaux » de centaines de milliers de comptes dans les jours qui ont suivi le premier tour [152]. Le cas roumain a également attiré l'attention de l'UE, qui a ouvert une enquête sur TikTok dans le cadre de ses nouvelles règles sur les services numériques (DSA).

Cette enquête vise à déterminer si TikTok a manqué à ses obligations de transparence et de lutte contre la désinformation, en particulier dans un contexte aussi sensible que celui d'une élection présidentielle. Ursula von der Leyen, présidente de la Commission européenne, a rappelé l'importance de protéger les démocraties contre toute forme d'ingérence étrangère, déclarant que l'UE agirait fermement à chaque fois que des soupçons d'ingérence sont soulevés.

[152] Stéphane Sicard. « Présidentielle annulée en Roumanie : Des centaines de milliers de faux comptes, des millions de faux abonnés, 85.000 cyberattaques, usage intensif de l'IA... Comment TikTok a été utilisé par l'extrême droite ». *L'Indépendant*, 7 décembre 2024. [Lien](#)

Ainsi, on peut remarquer un intense lien entre politique et technologie où l'un pourrait servir l'autre. Sur chaque cas étudié, les arguments se basent sur la même ligne : la défense de la liberté d'opinion et d'expression. La défense de cette liberté se retrouve particulièrement dans le discours et les actions de Musk et de X mais aussi de Télecram.

Telegram: Entre sécurité de l'information et dérives de la modération

Telegram est une application de messagerie instantanée créée en 2013 par les frères Pavel et Nikolaï Durov. Cette plateforme, qui compte aujourd'hui plus de 500 millions d'utilisateurs actifs mensuels, s'est imposée comme un acteur majeur dans le domaine des communications numériques. Telegram est connu pour ses nombreuses fonctionnalités, parmi lesquelles le chiffrement des messages pour garantir la confidentialité, les canaux publics et privés permettant à des millions d'utilisateurs de partager du contenu, la gestion de groupes massifs pouvant inclure des centaines de milliers de membres, le partage de fichiers sans limite de taille et des outils d'automatisation tels que des chatbots.

Cependant, Telegram présente une dualité fonctionnelle. Si son accessibilité et son efficacité sont largement saluées, la plateforme est aussi critiquée pour les dérives qu'elle facilite. En raison de sa nature décentralisée et de sa politique de modération minimaliste, Telegram est parfois utilisé pour diffuser de la propagande, des théories complotistes ou des informations manipulées. Cela est particulièrement visible dans le contexte de conflits internationaux comme celui entre Israël et le Hamas, où Telegram joue un rôle central dans la diffusion de vidéos de propagande, d'appels à la mobilisation et d'informations non vérifiées. Par exemple, à l'été 2022, l'Unesco révélait que la moitié des contenus liés à la Shoah sur Telegram étaient négationnistes.

La plateforme permet également la création de communautés fermées où peuvent se développer des idées radicales, ce qui contribue à polariser les débats et à importer des conflits internationaux dans des pays étrangers. En France, par exemple, Telegram a été utilisé pour attiser des tensions communautaires, exacerbant des fractures sociales déjà existantes. C'est la raison pour laquelle son directeur a été arrêté par les autorités françaises : en effet, on lui reproche de ne pas partager assez les données de l'application à la justice. Ainsi, si cette arrestation peut être une forme de régulation des plateformes, d'autres sont développées.

[152] Sicard, Stéphane. « Présidentielle annulée en Roumanie : Des centaines de milliers de faux comptes, des millions de faux abonnés, 85.000 cyberattaques, usage intensif de l'IA... Comment TikTok a été utilisé par l'extrême droite ». *L'Indépendant*, 7 décembre 2024. [Lien](#)

c. Les tentatives de régulation nationales

Si le DSA est la réponse européenne à la désinformation en créant des labels vérifiés qui permettent d'alerter les plateformes de comportements désinformationnels en priorité ou encore une régulation dans les publicités, des initiatives nationales sont aussi à noter.

D'une part, les États généraux du numérique français proposent de faire payer celui qui héberge (plateforme) les fausses informations qu'il héberge (idée de pollueur/payeur) et que l'argent récolté irait dans un organisme indépendant pour financer des instruments de lutte contre la désinformation.

Par ailleurs en Allemagne, la loi *Netzwerkdurchsetzungsgesetz* (NetzDG), entrée en vigueur en 2017, oblige les plateformes comptant plus de 2 millions d'utilisateurs à retirer les contenus illégaux, y compris les discours de haine et certaines formes de désinformation, dans un délai de 24 heures sous peine d'amendes allant jusqu'à 50 millions d'euros. Cette loi a conduit à une amélioration notable des efforts de modération des grandes entreprises numériques et renforcé la transparence grâce à des rapports réguliers exigés des plateformes.

En Finlande, l'approche repose davantage sur l'éducation, mais avec des politiques intégrées visant à inclure dans les programmes scolaires la littératie médiatique, qui se définit comme la capacité à accéder, analyser et comprendre l'ensemble des médias et outils d'information et de communication. Cette stratégie a permis de développer une population mieux armée pour détecter et contrer les fausses informations, faisant de la Finlande un modèle en matière de sensibilisation aux médias en Europe.

Enfin, l'Irlande, en tant que siège européen de nombreuses grandes plateformes numériques (Meta, X), a renforcé la régulation à travers son *Online Safety and Media Regulation Bill*. Cette loi, entrée en vigueur en 2022, crée une autorité de régulation indépendante chargée de surveiller les contenus nuisibles en ligne, y compris la désinformation, et d'imposer des sanctions aux plateformes non conformes.

Les régulations nationales et européennes commencent à poser des cadres plus stricts pour la modération, mais ces mesures nécessitent encore un renforcement pour être véritablement efficaces. En fin de compte, la lutte contre la désinformation, en particulier dans le cadre d'ingérences étrangères, est un travail collectif, qui implique non seulement les acteurs privés mais aussi les gouvernements, les institutions et les citoyens, afin de garantir un environnement numérique fiable, sécurisé et démocratique.

CONFRONTATIONS EUROPE



Confrontations - Bruxelles

Avenue des Arts 46

1000 Bruxelles

Confrontations - Paris

Avenue de Versailles 77

75016 Paris



@confrontations



@ConfrontationsEurope



www.confrontations.org



communication@confrontations.org

Confronter les idées, construire l'Europe