CONFRONTATIONS EUROPE

INGÉRENCE ÉTRANGÈRE ET DÉSINFORMATION : TECHNIQUES DE DIFFUSION ET MOYENS DE LUTTE

Sciences Po Strasbourg
École
de l'Université de Strasbourg

Dossier spécial

CONFRONTATIONS EUROPE

CONFRONTER LES IDÉES

CONSTRUIRE L'EUROPE

Janvier 2025

Sciences Po Strasbourg et le Master d'Etudes européennes et internationales pour Confrontations Europe

Les propos tenus dans ce rapport n'engagent que la responsabilité de leurs auteurs.

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.

SOMMAIRE

REMERCIEMENTS

À l'heure de rendre le présent rapport, représentant l'aboutissement d'un travail qui nous a occupé ces quatre derniers mois, l'ensemble des membres du groupe de travail tient à adresser ses sincères remerciements à toutes les personnes qui ont contribué à la réalisation de ce rapport.

Nous remercions avant tout l'équipe administrative et pédagogique de Sciences Po Strasbourg, pour l'opportunité de réaliser un travail professionnalisant avec des intervenants extérieurs, et sans qui le partenariat avec le think tank Confrontations Europe n'aurait pas eu lieu. Nous remercions particulièrement Thomas Lanson et Magdaléna Hadjiisky pour leur accompagnement.

Nous remercions également l'équipe de Confrontations Europe, et plus particulièrement notre encadrant pour ce projet, Jérôme Quéré, pour son temps, ses recommandations et ses précieux conseils qui nous ont guidé à travers tout le processus de travail.

Nous tenons également à remercier les divers professionnels avec qui nous avons échangé au cours d'entretiens et qui ont largement contribué à approfondir nos recherches et à enrichir notre travail académique d'une vision plus pratique et professionnelle : Vincent Couronne, fondateur du média *Les Surligneurs* ; Laurent Esquenet-Goxes, ancien député français (MoDem), vice-président d'une commission d'enquête sur les ingérences étrangères à l'Assemblée nationale ; Guillaume Kuster, cofondateur de l'entreprise CheckFirst ; Paula Gori et Lisa Ginsborg de l'Observatoire européen des médias numériques (EDMO).

LISTE DES ABRÉVIATIONS

AfD : Alternative für Deutschland / Alternative pour l'Allemagne
AFP : Agence France Presse
CE : Commission européenne
CIB : Coordinated Inauthentic Behavior / Comportement inauthentique coordonné
DDoS : Distributed Denial of Service attack / Une attaque par déni de service
DMA : Digital Markets Act / Règlement sur les marchés numériques
DSA : Digital Services Act / Règlement sur les services numériques
DVM : Désinformation visuelle et multimodale
EDMO : European Digital Media Observatory / Observatoire européen des médias numériques
EMIF : European Media and Information Fund / Fonds européen pour les médias et l'information
GIEC : Groupe d'experts intergouvernemental sur l'évolution du climat
IA : Intelligence artificielle
IFCN : International Fact-Checking Network / Réseau international de fast-checking
INGE 1 et 2 : Commissions spéciales du Parlement européen sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation
NetzDG : Netzwerkdurchsetzungsgesetz / Loi sur l'amélioration du traitement des contenus illicites par les réseaux sociaux
ONG : Organisation non gouvernementale
OSINT : Open Source Intelligence / Renseignement d'origine sources ouvertes
OTAN : Organisation du traité de l'Atlantique nord
PCC : Parti communiste chinois
RGPD : Règlement général sur la protection des données
RN : Rassemblement national
RRN : Recent Reliable News
SEAE : Service européen pour l'action extérieure
SEO : Search engine optimization / Optimisation pour les moteurs de recherche
UE : Union européenne
VIGINUM : Service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères

Un dossier réalisé par les étudiants du master Europe de Sciences Po Strasbourg, en collaboration avec Confrontations Europe

LE DOSSIER EN UNE PAGE

LA DÉSINFORMATION DANS LE CADRE D'INGÉRENCES ÉTRANGÈRES

Une diffusion intentionnelle de fausses informations à l'initiative d'un Etat ou d'un acteur non-étatique relié à un Etat, visant à tromper ou manipuler la population d'un Etat tiers pour atteindre des objectifs politiques

CONSTRUCTION D'UN DISCOURS DE DÉSINFORMATION

En lien avec des thèmes d'actualité à forte charge politique ou émotionelle (guerre en Ukraine, Covid-19, élections européennes...)

...adapté aux différents publics cibles (en fonction des priorités locales, de la vulnérabilité des cibles...)

Forme écrite : efficace du fait d'un mode de lecture rapide/superficiel en ligne, couplé à des choix langagiers qui influencent le lecteur

Forme visuelle (vidéos, images, photos décontextualisées, copie de sites internets officiels) : captation immédiate de l'attention et meilleure crédibilité

DIFFUSION MASSIVE AU NIVEAU NATIONAL

Par la captation d'intermédiaires influents (élus, journalistes, professeurs...)

...et l'automatisation numérique de la diffusion (bots, optimisation du référencement, achat d'espace publicitaire...)

ACTEURS DE LUTTE CONTRE LA DÉSINFORMATION

Des initiatives publiques :

- européennes : UE, organisation de société civile (EU Disinfo Lab)
- nationales : VIGINUM (France), Bureau électoral national (Estonie), Agence de défense psychologique (Suède)...

et privées :

- entreprises de presse : agences de fact-checking (*AFP fact Checking, CheckFirst*....) et collectifs de journalistes (*Les Surligneurs*)
- grandes entreprises du numérique (Google, Meta, Twitter/X ...)

Mais une implication parfois limitée : les instruments *Crowd Tangle* (Facebook) et *Birdwatch* (Twitter/X) supprimés récemment

TECHNIQUES DE LUTTE

Législations : INGE 1 & 2, Digital Markets Act & Digital Services Act (UE), NetzDG (Allemagne)...
-> Pour une meilleure modération des contenus et un encadrement de la publicité politique

Protection du pluralisme et de l'indépendance des médias

Investissement pour le soutien à un journalisme de qualité et l'éducation aux médias

Recherche & investigation pour augmenter les capacités de détection de la désinformation

Surveillance en ligne, notamment en périodes électorales

INTRO

À l'ère des réseaux sociaux, des bots et des deep fakes, la notion de vérité est constamment questionnée. Les technologies numériques, en constante évolution, ont offert des outils redoutables pour manipuler l'opinion publique et déstabiliser les institutions démocratiques. Dans ce contexte, l'ingérence étrangère, longtemps perçue comme une problématique marginale, s'impose désormais comme une menace majeure, notamment au sein de l'Union européenne (UE).

Les campagnes de désinformation en sont un levier central, utilisé pour fragiliser les systèmes démocratiques, éroder la confiance des citoyens et influencer les processus décisionnels stratégiques. Dans le cadre des institutions européennes, l'ingérence étrangère est un sujet sensible, particulièrement lorsque des États ou des acteurs extérieurs cherchent à influencer les décisions politiques et les orientations stratégiques de l'Union européenne, que ce soit par le biais de campagnes de désinformation, de soutien à certains partis politiques ou de manipulation économique. Ainsi, lutter contre la désinformation nécessite de prendre la mesure de l'enjeu de l'identification d'une source et de savoir distinguer une source fiable d'une autre qui ne l'est pas.

Cependant, définir l'ingérence étrangère reste complexe, car il n'existe pas de consensus au sein de l'UE sur une définition standard. Selon le rapport « *Conceptualizing Foreign Interference in Europe* » publié par l'Alliance for Securing Democracy, deux critères clés – l'intention et la transparence – permettent de mieux cerner ce concept.

L'intention vise à comprendre les objectifs de l'acteur étranger : cherche-t-il à manipuler, déstabiliser ou nuire aux institutions démocratiques ? Plusieurs facteurs existent ainsi pour la déterminer : le *timing*, la coordination qui découle de l'action et l'ampleur de l'effet produit. La transparence, quant à elle, met en lumière le caractère souvent secret et dissimulé des actions d'ingérence. Le rapport de la commission spéciale INGE 2 du Parlement européen, reprenant des travaux de Chatham House, enrichit cette définition en y intégrant les différentes formes que peut prendre l'ingérence, qu'elle soit externe (cyberattaques, campagnes de désinformation, etc.) ou interne (corruption, influence de politiciens travaillant pour des régimes étrangers, etc.).

Par ailleurs, le rapport INGE 2 déclare que l'ingérence étrangère peut être exercée par « *un Etat ou des acteurs non étatiques* ». Ainsi, là où l'influence a vocation à souligner, faire valoir la puissance d'un État pour lui-même, l'ingérence pourrait se définir comme l'immixtion dissimulée d'un État ou d'un acteur non étatique au sein d'un autre État dans le but de manipuler, déstabiliser voire nuire à son système démocratique, ses valeurs et sa population. Dans le cadre de l'UE, l'ingérence semble cibler le plus souvent les institutions européennes ainsi que les sociétés européennes. Ce dernier terme fait référence à l'ensemble des sociétés des pays de l'UE, à la fois considérées comme une entité partageant des caractéristiques culturelles, historiques, politiques et sociales communes mais aussi impliquant des diversités nationales et régionales. Toutefois, si la théorie permet de plus ou moins distinguer influence et ingérence, la réalité rend parfois cette distinction plus floue.

Parmi les méthodes d'ingérence employées, la désinformation occupe une place prépondérante. Si elle trouve ses origines dans des stratégies anciennes – comme le montre Sun Tzu dans *L'Art de la guerre* – son impact s'est démultiplié avec l'émergence des outils numériques. En réalité, la désinformation « moderne » fusionne et remodèle les vieilles techniques d'espionnage utilisées durant la Guerre froide avec les nouveaux outils numériques.

La désinformation se distingue par la diffusion intentionnelle de fausses informations, visant à tromper ou manipuler les publics pour atteindre des objectifs politiques, économiques ou sociaux. La définition élaborée par Claire Wardle dans son rapport *Information disorder: Toward an interdisciplinary framework for research and policy making* permet de faire une distinction entre fausse information (*mis-information* : diffusion d'une information fausse, sans intention de nuire), désinformation (*dis-information* : diffusion délibérée d'une information fausse dans l'intention de nuire) et information malveillante (*mal-information* : diffusion d'une information vraie dans l'intention de nuire, généralement en divulguant une information censée rester confidentielle), soulignant ainsi la spécificité et la dangerosité des intentions malveillantes qui animent ces pratiques.

La désinformation et l'ingérence étrangère partagent des caractéristiques fondamentales, notamment une intention de nuire et un manque de transparence. Ainsi, la désinformation peut être vue comme l'un des instruments les plus puissants et insidieux de l'ingérence étrangère, utilisé pour influencer les institutions et les sociétés européennes.

Ce rapport s'attachera donc à comprendre comment les techniques de désinformation sont utilisées pour influencer les institutions et les sociétés européennes, et quelles stratégies ces dernières mettent en place pour y faire face. Pour répondre à cette question, ce rapport adoptera une approche en trois temps. Premièrement, il s'agira de comprendre la construction du discours de la désinformation (forme et fond) (I) pour mieux cerner les méthodes de propagation à un large auditoire (II). Enfin, il s'agira de traiter les acteurs et techniques de lutte contre la désinformation (III).

CONFRONTATIONS EUROPE

Sciences Po Strasbourg
École
de l'Université de Strasbourg

DOSSIER SPÉCIAL DÉSINFORMATION
& INGÉRENCE ÉTRANGÈRE

FORME ET FOND DE LA DÉSINFORMATION

ÉLABORATION ET MATÉRIALISATION DU DISCOURS DE DÉSINFORMATION

La désinformation s'articule autour d'une élaboration stratégique, combinant un discours politique et idéologique soigneusement construit avec une forme adaptée à ses objectifs. Cette première partie se propose d'analyser la conception de ces contenus, en étudiant leur message sous-jacent en fonction de leurs cibles (1), ainsi que le choix des formats mobilisés, écrits (2) ou imagés (3). Une approche systématique de ces dimensions permet d'appréhender les raisons pour lesquelles ces contenus parviennent à manipuler les perceptions, influencer les comportements et fragmenter les sociétés.

1. L'ÉLABORATION DU DISCOURS DE DÉSINFORMATION

a. L'élaboration d'un discours politique...

La désinformation vise à diviser les sociétés et à discréditer les gouvernements ciblés. Pour atteindre ces objectifs, des discours sont minutieusement élaborés en s'appuyant sur des thématiques d'actualité. Ces thématiques sont souvent déformées, manipulées ou sorties de leur contexte d'origine afin de maximiser leur impact. L'élaboration d'un tel discours consiste également à construire des narratifs contradictoires, semant ainsi le doute et la confusion dans l'esprit des populations ciblées.

Dans certains cas, l'origine du discours est identifiable et renvoie à des acteurs étatiques ou non-étatiques clairement identifiés. Par exemple, dans le cadre de la guerre en Ukraine, les campagnes de désinformation orchestrées par la Russie illustrent cette dynamique. L'opération russe « Portal Kombat » a ainsi visé plusieurs pays occidentaux soutenant activement l'Ukraine, notamment la France, l'Allemagne, la Pologne et les États-Unis. Cette opération a consisté à diffuser des contenus dénigrant l'Ukraine et ses alliés dans le but de rallier l'opinion publique internationale à la cause russe. Dans d'autres cas, où la source est moins immédiatement identifiable, l'analyse des discours permet d'en déduire l'origine. Un exemple significatif est celui des comptes allemands baptisés « Odetta » : des profils Facebook fictifs, prétendant appartenir à des employées de Netflix, publiaient des messages pro-russes et des fake news concernant la guerre en Ukraine [1]. Ces messages prenaient la forme de courts posts ou de commentaires sous des publications existantes, rendant l'opération plus discrète et éclatée que celles orchestrées via des réseaux structurés comme l'opération Portal Kombat.

[1] Wienand, Von L., S Steurenthaler, et S Loelke. « Putins Troll-Armee greift Deutschland an », 30 août 2022. Lien

La construction de cette dernière a été minutieusement réalisée par l'entreprise russe Tiger Web, créée en 2015 et domiciliée depuis en Crimée, dont la mission principale était le développement et le maintien de sites dans des secteurs comme la restauration, le sport ou la médecine [2]. Les sites qu'elle aurait créés ne produisaient aucun contenu original mais relayaient massivement des publications issues majoritairement d'agences de presse russes, qui étaient ensuite propagées sur les réseaux sociaux. Cependant, malgré leur discrétion, l'orientation clairement pro-russe du discours des **«** Odetta **»** a permis de relier ces comptes à des initiatives étatiques russes [3].

Certains moments se révèlent particulièrement propices à la diffusion de désinformation en raison de leur charge politique ou émotionnelle. Les périodes électorales, par exemple, sont un moment particulièrement opportun, et ce pour différentes raisons. D'abord, la désinformation exploite la charge émotionnelle liée aux élections pour influencer les opinions et les comportements.

En effet, les messages émotionnellement chargés, alarmistes, indignés ou prometteurs, captent davantage l'attention que les informations factuelles et nuancées.

Les récits dramatiques, comme ceux suggérant une fraude massive ou des conspirations, activent des réponses émotionnelles comme la peur, la colère ou l'indignation, rendant les individus plus enclins à partager ces contenus sans vérifier leur véracité. De plus, dans un contexte électoral, les opinions sont souvent déjà polarisées. Les individus cherchent instinctivement des informations qui confirment leurs croyances préexistantes, un mécanisme appelé le biais de confirmation [4]. Ainsi, les campagnes de désinformation exploitent ce mécanisme en ciblant les différents segments de la population avec des récits personnalisés, amplifiant ainsi les divisions. De plus, les élections, par nature, sont limitées dans le temps, créant une impression d'urgence. Cette contrainte temporelle diminue la capacité des individus à vérifier l'information, augmentant leur vulnérabilité face aux manipulations. Cela s'est particulièrement illustré lors des élections européennes de juin 2024, moment clé pour l'Union européenne qui a été marqué par une multiplication des campagnes de désinformation. Ces campagnes ont promu des récits sur de prétendues fraudes électorales, critiqué le rôle du Parlement européen et cherché à encourager l'abstention en cultivant l'idée d'une opposition irréconciliable entre les élites et le peuple. Les efforts pour manipuler l'opinion publique à ces occasions visent à fragiliser la légitimité des institutions européennes.

[2] Secrétariat général de la défense et de la sécurité nationale. « Portal Kombat : un réseau structuré et coordonné de propagande prorusse », 12 février 2024. Lien
[3] Wienand, Von L. et al. *Op.cit.*
[4] Fakt. « Le biais de confirmation, un vecteur non négligeable vers la désinformation », 10 septembre 2024. Lien

Cependant, les moments politiquement sensibles ne sont pas les seuls à être exploités. La désinformation s'appuie également sur des sujets de société, parfois éloignés des débats politiques immédiats, mais capables de diviser les populations et de provoquer des tensions sociales. Ainsi, les thématiques environnementales, les questions de genre et de sexualité ou encore les débats sur l'immigration et l'asile sont régulièrement instrumentalisés. De même, la pandémie de Covid-19, bien qu'en recul dans les préoccupations médiatiques, continue d'être utilisée comme levier par des réseaux complotistes actifs sur des plateformes comme X (anciennement Twitter). Ces réseaux diffusent des récits visant à décrédibiliser les gouvernements et les institutions scientifiques, montrant que même des sujets moins actuels peuvent être recyclés pour servir des objectifs de désinformation.

b. … Adapté à un public cible

La désinformation ne s'adresse pas à un public homogène. Elle cible, au contraire, des groupes spécifiques pour maximiser ses effets. Comme le souligne Claire Wardle dans un rapport pour le Conseil de l'Europe [5], la désinformation *« exacerbe les divisions socio-culturelles en jouant sur les tensions nationalistes, ethniques, raciales et religieuses »*. Ces discours stratégiquement orientés exploitent les failles psychologiques et sociétales pour amplifier leur impact.

Pour maximiser leur impact, les discours de désinformation sont soigneusement adaptés à leurs cibles. Bien qu'aucun profil type de victime n'existe, certaines caractéristiques augmentent la vulnérabilité à ces manipulations, notamment l'isolement social, les polarisations idéologiques et les crises identitaires. Les masculinistes illustrent parfaitement cette dynamique. Ce groupe, caractérisé par une idéologie anti-féministe extrémiste, mobilise les réseaux sociaux pour propager des discours polarisants et recruter de nouveaux membres. Leur succès repose souvent moins sur l'adhésion aux idées qu'ils véhiculent que sur le sentiment d'appartenance qu'ils offrent à des individus isolés ou en quête de repères.

Les adolescents constituent un autre groupe particulièrement vulnérable à la désinformation, en raison de biais cognitifs tels que l'effet de confirmation et l'ancrage mental [6]. L'effet de confirmation pousse les individus à privilégier les informations qui confortent leurs croyances préexistantes, tandis que l'ancrage mental les rend sensibles aux premières informations reçues, même si elles sont erronées. Ces biais, décrits notamment par Pennycook et Rand [7], facilitent la manipulation des jeunes esprits, souvent exposés à des campagnes subtiles sur des plateformes comme les forums de jeux vidéo.

[5] Claire Wardle, et Hossein Derakhshan. « Information Disorder: Toward an interdisciplinary framework for research and policymaking ». Council of Europe, 2017. Lien
[6] Marine Lemaire, Mathieu Cassotti, et Grégoire Borst. « Development of fake detection during adolescence ». septembre 2022. Lien
[7] Gordon Pennycook et David G. Rand. « The Psychology of Fake News ». *Trends in Cognitive Sciences*, 1 mai 2021. Lien

Ces espaces numériques servent de portes d'entrée vers des réseaux plus fermés comme Telegram ou Discord, où les discours complotistes ou illibéraux se diffusent plus intensément. Les personnes âgées sont également une cible privilégiée, notamment sur des plateformes comme Facebook, où elles sont souvent moins averties des dangers de la désinformation. Elles se retrouvent exposées à des fake news soigneusement élaborées pour jouer sur leurs émotions et leur méfiance envers les institutions.

Les techniques de diffusion de la désinformation varient également en fonction des contextes culturels et géographiques. Le géorepérage, par exemple, permet d'ajuster les discours aux priorités locales. L'opération russe Portal Kombat illustre bien cette approche, en particulier à travers son écosystème « Pravda », un réseau sophistiqué de sites ciblant des audiences spécifiques. Lancé en juin 2023, l'écosystème Pravda constitue l'un des trois ensembles majeurs de Portal Kombat. Contrairement à l'« écosystème historique », centré depuis 2013 sur les audiences russes et ukrainiennes, ou à l'« écosystème -news.ru », créé en 2022 pour les russophones d'Ukraine, l'écosystème Pravda s'adresse directement à plusieurs pays occidentaux affichant un soutien à l'Ukraine. Il comprend cinq sites : pravda-fr pour la France, pravda-de pour l'Allemagne, l'Autriche et la Suisse, *pravda-pl.com* pour la Pologne, *pravda-es.com* pour l'Espagne et *pravda-en.com*, destiné au Royaume-Uni et aux États-Unis [8]. Cette segmentation rend le contenu plus pertinent pour les cibles visées tout en réduisant la visibilité extérieure, rendant l'opération plus difficile à tracer. Un autre exemple frappant est celui d'une radio locale à Nice, rachetée par un oligarque russe. Initialement axée sur des informations en français favorables au Kremlin, elle s'est progressivement transformée en une station diffusant exclusivement en russe, renforçant ainsi son influence auprès des diasporas russophones.

Les impacts psychologiques de la désinformation sont nombreux et préoccupants. Elle contribue à l'érosion de la confiance dans les institutions, alimente l'anxiété sociale et augmente la violence sociale et politique.

Par ailleurs, la désinformation peut avoir des conséquences factuellement dangereuses : un rapport du Conseil des académies canadiennes révèle qu'en 2021, au moins 13 000 hospitalisations et 3 000 décès auraient pu être évités si la désinformation autour de la Covid-19 n'avait pas promu des traitements inefficaces ou dangereux [9]. Ces chiffres témoignent de l'impact potentiellement mortel de la manipulation de l'information, qui peut aller bien au-delà de simples divisions idéologiques.

[8] SGDSN. *Op.cit.*
[9] « La désinformation peut-elle tuer? » *Science-Presse*, 29 mars 2023. Lien

2. LE CONTENU ÉCRIT

Dans un monde souvent qualifié d'infodémie [10] en raison de la surabondance d'informations, le contenu écrit occupe une place centrale dans la diffusion de la désinformation. Cette prolifération est amplifiée par les réseaux sociaux, où les informations se propagent en simultanée et à une vitesse vertigineuse sur une multitude de plateformes. Cependant, l'impact de ces contenus ne peut être compris sans une analyse des processus cognitifs qu'ils mobilisent. La lecture, sur des supports numériques comme matériels, engage des mécanismes complexes d'attention, de mémorisation et d'interprétation. Ces derniers, souvent biaisés par des raccourcis cognitifs ou des schémas préexistants, rendent les lecteurs vulnérables à la désinformation subtilement conçue. Cette réalité soulève ainsi des questions cruciales sur la manière dont le type de contenu influence les décisions individuelles et collectives dans des contextes sensibles (élections, débats environnementaux…).

a. Entre désinformation écrite et visuelle, des approches complémentaires de manipulation cognitive

Il est essentiel, dans un premier temps, d'examiner les différences de réception de la désinformation selon qu'elle provienne d'un contenu écrit ou visuel. Bien que la partie suivante se concentre davantage sur les implications cognitives et pratiques propres aux contenus visuels, il convient dès à présent de souligner que le traitement cognitif, l'attention accordée et la mémorisation des fausses informations diffèrent significativement selon le type de contenu.

Les contenus écrits et visuels illustrent ainsi deux approches distinctes dans la désinformation, chacune exploitant des mécanismes spécifiques pour influencer le public. La désinformation écrite s'appuie sur des récits narratifs détaillés qui imitent des formats journalistiques crédibles ou encore des sites internet officiels comme lors des opérations Doppelgänger, nous y reviendrons par la suite. Ces contenus jouent ainsi sur la logique et la cohérence pour convaincre et manipuler la perception du lecteur.

[10] Organisation Mondiale de la Santé. « Gestion de l'infodémie sur la COVID-19 : Promouvoir des comportements sains et atténuer les effets néfastes de la diffusion d'informations fausses et trompeuses », 20 septembre 2020. Lien

En revanche, les stratégies comme les *deep fakes* (utilisation de l'intelligence artificielle), les *shallowfakes* (association de textes à des images sorties de leur contexte) ou les *cheapfakes* (modifications simples d'images) illustrent une manipulation où l'aspect visuel tend à renforcer la crédibilité perçue et l'adhésion au message. Ainsi, alors que les textes sollicitent une analyse plus approfondie et un traitement critique, les contenus visuels court-circuitent souvent ces processus. La désinformation visuelle semble donc être multimodale [11] (vidéos, images, émoticônes ou photos décontextualisées) et tend à amplifier l'impact émotionnel du lecteur, rendant encore plus difficile la distinction entre le vrai et le faux.

L'influence des contenus visuels est également amplifiée par leur capacité à capter immédiatement l'attention et à exploiter notre tendance naturelle à accorder plus de foi aux images qu'aux textes. En cela, les images requièrent généralement moins d'efforts cognitifs à interpréter que les textes, qui peuvent être limités par des obstacles linguistiques ou des niveaux variables d'alphabétisation [12]. Les fausses rumeurs visuelles, souvent plus persistantes et rapidement diffusées grâce à leur attrait sensationnel [13], semblent donc d'autant plus efficaces dans la manipulation des perceptions et des opinions avec les avancées de l'intelligence artificielle.

b. La manipulation cognitive à travers les contenus écrits

Néanmoins, si les contenus visuels captivent par leur immédiateté et leur pouvoir émotionnel, les contenus écrits, eux, usent de techniques plus subtiles et ciblées pour influencer les perceptions et les croyances. La manipulation cognitive ne se limite donc pas à l'image ; elle trouve également un terrain fertile dans la lecture, notamment à l'ère numérique où l'attention est souvent sacrifiée au profit de la rapidité. En effet, les particularités du contenu écrit – sa capacité à structurer des récits cohérents et à mobiliser des procédés linguistiques précis – offrent un levier puissant pour façonner les opinions. Mais comment ces mécanismes opèrent-ils ? Quels procédés linguistiques et biais cognitifs entrent en jeu dans la construction et la diffusion de fausses informations écrites ? Pour comprendre ces dynamiques, il est essentiel de s'intéresser à la manière dont la lecture numérique modifie l'assimilation des informations et favorise la propagation de la désinformation.

[11] « Comprendre les menaces et les défis – Désinformation visuelle et multimodale (DVM) ». Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa. Lien
[12] *Ibid.*
[13] Catherine Beauvais. « Fake news: Why do we believe it? » *Joint Bone Spine*, 1 juillet 2022. Lien

L'impact de la lecture numérique sur l'assimilation de l'information

À l'ère d'Internet, où la majorité des informations que nous consommons passe par des supports numériques, la manière dont nous intégrons ces contenus a radicalement changé. La lecture en ligne favorise une assimilation différente, souvent exploitée pour amplifier la propagation de fausses informations et manipuler les perceptions [14]. Contrairement à la lecture sur papier, qui invite généralement à une expérience plus immersive et approfondie, notamment parce que nous nous engageons souvent à lire entièrement un contenu acheté, la lecture numérique se caractérise par une approche plus rapide et superficielle. La navigation sur papier est moins aisée, mais elle encourage une concentration accrue et limite la fatigue visuelle, permettant un traitement cognitif plus profond des informations. En revanche, la lecture sur écran favorise une approche non linéaire : le lecteur parcourt le texte en balayant l'article ou le site du regard, ce qui réduit l'attention et la profondeur du traitement cognitif. Dans ce contexte, les réseaux numériques offrent un terrain privilégié pour la diffusion de contenus écrits manipulatoires, qui exploitent pleinement ces biais d'attention pour influencer les opinions.

Les techniques linguistiques de manipulation dans les contenus écrits

Pour exploiter le biais de lecture moins attentive, particulièrement présent sur les réseaux sociaux, des chercheurs ont mis en lumière l'usage de stratégies linguistiques précises visant à manipuler la perception des contenus. Ces stratégies révèlent comment les choix langagiers peuvent influencer les attitudes et les croyances. L'une des approches marquantes est la grammaire fonctionnelle systémique, développée par Michael Halliday [15]. Selon cette théorie, la langue est un système de choix où chaque décision revêt une fonction idéologique ou socioculturelle. En cela, l'analyse de la transitivité explore comment influencer la perception d'un texte via le choix du verbe principal ou encore l'utilisation d'adverbe. Selon que l'auteur utilise « probablement » ou « assurément », l'assimilation de l'information par le lecteur sera différente et permet de transmettre des perspectives et opinions implicites. Cette méthode trouve une application particulièrement marquante dans les tweets de Donald Trump [16], où il utilise habilement la grammaire pour asseoir ses propos et renforcer l'impact de ses opinions. Par la répétition de verbes tels que « croire » ou « vouloir » et l'emploi d'adjectifs ou d'adverbes valorisants comme « meilleur » ou « incroyable », ses messages créent une impression d'argumentation solide et cohérente. Ce choix stratégique de langage tend à légitimer ses affirmations, rendant parfois plus difficile pour les lecteurs de discerner le vrai du faux, surtout dans un contexte où l'attention est déjà fragmentée.

[14] Stefan Gaillard, Zoril A. Oláh, Stephan Venmans, et Michael Burke. « Countering the Cognitive, Linguistic, and Psychological Underpinnings Behind Susceptibility to Fake News: A Review of Current Literature With Special Focus on the Role of Age and Digital Literacy ». *Frontiers in Communication*, 2021. Lien
[15] Citation des travaux de Michael Halliday dans Gaillard et al. *Ibid.*
[16] Florent Montaclair. « Du Tic à La Tactique : Les Mécanismes Grammaticaux de l'infox à Travers Les Tweets de Donald Trump ». *The Conversation*, 1 septembre 2022. Lien

Par ailleurs, un fait marquant, renforçant la désinformation est son caractère répétitif. La répétition d'une information augmente la probabilité qu'elle soit perçue comme vraie, même si elle est incorrecte. Ce phénomène connu sous le nom d'exposition préalable et d'effet de vérité illusoire [17], repose sur un mécanisme psychologique : plus une information est répétée, plus elle devient familière et donc facile à traiter cognitivement, ce qui incite les individus à la considérer comme crédible.

L'opération Doppelgänger : Un exemple de manipulation à grande échelle

Dans le cadre de l'opération Doppelgänger, l'ampleur de la désinformation a été particulièrement frappante. Lancée par la Russie en mai 2022, cette campagne a ciblé l'Europe en produisant des centaines de faux sites officiels et de faux articles imitant des médias européens de renom, comme The Guardian, Le Monde, ou encore RBC Ukraine. Parmi les exemples les plus emblématiques figure un faux site du ministère de l'Europe et des Affaires étrangères français qui diffusait de prétendus communiqués de presse. L'objectif de cette opération, menée au lendemain de l'invasion de l'Ukraine, était d'une part, de discréditer l'Ukraine en la présentant comme un État défaillant, et d'autre part, de promouvoir un narratif pro-Kremlin [18]. Ces campagnes massives, qui ont touché plusieurs pays européens, notamment la France, l'Ukraine, et le Royaume-Uni, reposaient sur une stratégie de répétition à grande échelle. Au total, 355 noms de site usurpant l'identité de médias dans neuf pays d'Europe, d'Amérique et du Moyen-Orient ont été recensés par VIGINUM [19]. La diffusion massive de ces contenus dans différents cercles sociaux, combinée aux algorithmes des réseaux sociaux, a permis la création de « chambres d'écho » [20] en ligne. Ces dernières exposent les utilisateurs à des contenus similaires, consolidant leurs croyances tout en rendant la remise en question des fausses informations de plus en plus difficile.

L'impact de cette opération est notamment dû à la méthode utilisée afin de créer de faux domaines internet : celle du *typosquatting*, c'est-à-dire, la création de faux sites internet via l'exploitation des erreurs de frappe courantes dans les noms de domaine. Par exemple, une simple faute de saisie par un utilisateur peut le conduire vers un site frauduleux imitant un média ou une institution de confiance [21]. Ce procédé permet de construire un écosystème de fausses références, comprenant des sites officiels et des médias mainstream détournés.

[17] Catherine Beauvais. « Fake news: Why do we believe it? » Joint Bone Spine, 1 juillet 2022. *Lien*
[18] Alexandre Alaphilippe, Gary Machado, Raquel Miguel, et Francesco Poldi. « Doppelganger - Media Clones Serving Russian Propaganda ». EU Disinfo Lab, 27 septembre 2022. Lien
[19] Franceinfo. « Guerre en Ukraine : ce que l'on sait de l'opération de désinformation russe "Doppelgänger" qui a visé la France », 14 juin 2023. Lien.
[20] Gaillard et al. *Op.cit.*
[21] Secrétariat général de la défense et de la sécurité nationale. « RRN : une campagne numérique de manipulation de l'information complexe et persistante », 13 juin 2023.Lien

Ces faux sites, combinés à des techniques de géoblocage et de redirection intelligente selon l'emplacement des utilisateurs [22], amplifient les narratifs pro-Kremlin tout en légitimant les informations erronées grâce à l'apparence crédible des plateformes imitées. Le *typosquatting*, en usurpant l'apparence et la légitimité de médias reconnus, soulève une problématique cruciale : celle du rôle des experts dans la propagation de la désinformation. En effet, en adoptant l'identité visuelle et la crédibilité de sites perçus comme des gardiens de l'information, ces faux sites exploitent la confiance du public pour diffuser des contenus erronés. Dans cette dynamique, ces derniers publiant des articles destinés à être relayés massivement, introduisent un autre levier stratégique : l'utilisation de « faux experts ».

c. Les « faux experts » : manipulation de l'expertise et légitimation des fausses informations

Nous pourrions croire que face à l'abondance d'informations, la parole des experts gagnerait en autorité incontestée. Cependant, la réalité est bien différente. Les fausses informations qui influencent l'opinion publique, déforment également l'image des scientifiques, alimentant ainsi une méfiance croissante. Elles renforcent les stéréotypes, creusant davantage le fossé entre les scientifiques partisans du climat et les climatosceptiques. Ces derniers se retrouvent donc souvent victimes de préjugés qui affectent leur crédibilité, particulièrement dans le cadre du débat sur l'environnement. Cette représentation duale des experts est parfois exploitée pour propager des récits qui contredisent le consensus scientifique, notamment en matière de climat. Cela s'inscrit dans une dynamique qui met en avant de faux experts, souvent utilisés pour remettre en question les faits établis. Ainsi, certains discours d'experts peuvent légitimer des opinions minoritaires, nourrissant de fait la désinformation. Par exemple, malgré les multiples avertissements du GIEC sur la réalité du réchauffement climatique, certains « experts » climatosceptiques continuent de nier ces faits. Ces prises de position trouvent un large écho sur les réseaux sociaux, renforçant la polarisation des opinions et affaiblissant le consensus scientifique bien établi.

Par ailleurs, dans son analyse de la désinformation, Catherine Beauvais [24] souligne que les plateformes en ligne favorisent ce qu'elle appelle un « *marché public de l'information* ».

[22] EU Disinfo Lab. *Op.cit.*
[23] Isabelle Boyer et Luciana Radut-Gaghi. « Des stéréotypes à l'ère des fake news ». *Communication. Information médias théories pratiques*, 11 octobre 2021. Lien.
[24] Catherine Beauvais. « Fake news: Why do we believe it? » Joint Bone Spine, 1 juillet 2022. Lien

Cette idée illustre comment l'abondance de plateformes en ligne et la diversité des individus qui y participent ont transformé les hiérarchies de légitimité dans la transmission des connaissances. Les détenteurs classiques de savoir – scientifiques, journalistes et autres experts – se trouvent désormais concurrencés par des figures médiatiques telles que les youtubeurs et les influenceurs. Ces derniers, grâce à leur large audience et à leur visibilité, acquièrent une forme de légitimité et de crédibilité aux yeux du public, parfois perçue comme équivalente, voire supérieure, à celle des experts traditionnels, malgré l'absence d'une véritable expertise dans le domaine qu'ils abordent.

Cette inversion des rôles questionne la validité de l'expertise dans un contexte marqué par l'inflation informationnelle, où la quantité de données disponibles dépasse souvent la capacité des individus à les analyser de manière critique.

L'opération d'influence pro-Chine Shadow Play illustre de manière frappante ce phénomène. Plus de 45 000 vidéos ont été produites par une trentaine de chaînes YouTube [25], dont une douzaine en langue française, comme « Sophie Décrypte ». Ces vidéos ont relayé des contenus désinformationnels en reprenant des narratifs déjà bien connus, précédemment diffusés sous forme écrite, mais cette fois adaptés au format vidéo. Cette stratégie vise à conférer une légitimité accrue à ces fausses informations, tout en élargissant leur portée auprès d'un public diversifié. L'objectif principal est double : mener une guerre informationnelle contre les États-Unis et promouvoir une image positive des actions du gouvernement chinois. Chaque vidéo est soigneusement adaptée à son public cible. Par exemple, dans le cas de « Sophie Décrypte », le contenu s'adresse spécifiquement aux francophones en s'inspirant du nom d'une chaîne reconnue pour ses analyses politiques et sociales, renforçant ainsi l'illusion de crédibilité. À cela s'ajoute la stratégie de l'agence de communication russe Fazze, qui a approché des youtubeurs influents, comme « Dirty Biology », afin de promouvoir le vaccin Spoutnik V tout en discréditant Pfizer [26].

Ainsi, l'expertise, loin de protéger contre la désinformation, peut, dans certains cas, être détournée pour véhiculer des messages trompeurs. Les réseaux sociaux jouent un rôle crucial dans ce processus, facilitant la diffusion rapide et massive de discours polarisants et de fausses informations, tout en mettant en valeur des figures qui, parfois, ne relèvent d'aucune autorité scientifique réelle.

[25] Jacinta Keast. « Shadow Play: A pro-China and Anti-US Influence Operation Thrives on YouTube ». Australian Strategic Policy Institute, 15 décembre 2023. Lien
[26] *Courrier international*. « Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée ». 26 mai 2021. Lien

d. L'ambiguïté entre satire et désinformation : quand l'humour brouille les frontières

Si certains exemples de désinformation sont clairement identifiés et bien documentés, la frontière devient plus floue lorsqu'il s'agit de contenus humoristiques. Certains sites exploitent cette ambiguïté en publiant des articles ou des caricatures qui oscillent entre satire et désinformation. Cette stratégie délibérée joue sur l'interprétation subjective du lecteur, rendant difficile la distinction entre une intention humoristique légitime et une tentative de manipulation. Une tentative de différenciation entre satire et désinformation consiste à considérer que les fausses nouvelles cherchent à tromper en imitant des formats sérieux et crédibles, tandis que la satire s'appuie sur l'humour ou l'ironie, sans volonté de duper [27]. Cependant, des similarités linguistiques entre ces deux genres rendent leur classification complexe. Cette définition traditionnelle de la satire mérite ainsi d'être nuancée, d'autant plus que l'essor des réseaux sociaux brouille encore davantage les frontières entre ces deux formes de contenu.

L'avènement de nouveaux supports de diffusion semble alors avoir profondément modifié le paysage de la satire politique [28]. Un exemple frappant est le Babylon Bee, un site d'information satirique américain aux orientations conservatrices, qui jouit d'une grande popularité aux États-Unis. Selon une étude menée par l'Université de l'Ohio, 28 % des républicains et 14 % des démocrates interrogés ont admis croire aux informations satiriques publiées par le Babylon Bee [29]. Ce problème est particulièrement préoccupant, car bien que les textes soient de plus en plus souvent vérifiés et les informations démenties, les plateformes numériques continuent de relayer massivement des contenus satiriques sans fournir le contexte nécessaire. Cette absence de cadre explicatif accentue l'ambiguïté et permet à la satire d'échapper aux mécanismes de contrôle et de vérification. En cela, l'étude de l'Université de l'Ohio a également révélé que les articles du Babylon Bee figuraient parmi les contenus les plus inexacts mais aussi les plus partagés sur les réseaux sociaux.

Ce phénomène devient particulièrement visible dans le cadre de campagnes de désinformation comme celle des *Reliable Russian News* (RRN), révélée en mars 2022, peu après l'invasion de l'Ukraine par la Russie.

[27] Jwen Fai Low, Benjamin C. M. Fung, Farkhund Iqbal, et Shih-Chia Huang. « Distinguishing between fake news and satire with transformers ». *Expert Systems with Applications*, 1 janvier 2022. Lien
[28] Phil Simon. « La liberté d'expression face à la satire politique : un équilibre fragile ». *Actualités Juridiques*, 15 octobre 2024. Lien
[29] R. Kelly Garrett, Robert Bond, et Shannon Poulsen. « Too Many People Think Satirical News Is Real ». The Ohio State University, 16 août 2019. Lien.

Cette opération avait pour objectif de légitimer l'opération militaire spéciale russe tout en discréditant l'État ukrainien et ses alliés occidentaux. Pour ce faire, de nombreux faux comptes en ligne ont été créés, diffusant des caricatures anti-occidentales et pro-russes via des plateformes comme memhouse[.]online, le canal Telegram @VoxCartoons, ou encore des comptes fictifs tels que « Milana Krystel » sur Facebook [30]. En exploitant l'humour et les codes de la satire, ces caricatures ont servi d'outils de manipulation cognitive, minimisant les critiques tout en renforçant les narratifs pro-russes. Lorsqu'elles sont diffusées via des canaux diplomatiques, tels que le compte Twitter de l'ambassade de Russie en France, ou présentées sous de fausses identités, ces formes de satire brouillent la frontière entre humour et désinformation, rendant leur véritable intention difficile à identifier.

Nous nous trouvons ainsi face à une véritable zone grise où distinguer les fausses nouvelles de la satire, du sarcasme et de l'ironie représente un défi de taille. Ces genres partagent parfois des caractéristiques stylistiques similaires aux textes trompeurs, rendant leur identification encore plus complexe. L'humour peut ainsi devenir un outil de désinformation lorsqu'il exploite la méconnaissance du public, son attrait pour le sensationnalisme ou ses biais cognitifs, notamment le désir de se sentir informé [31]. En effet, les fausses nouvelles influencent souvent les individus en renforçant leurs croyances préexistantes ou en s'appuyant sur des expériences personnelles. Ce biais de confirmation [32] amène les individus à privilégier les informations qui confortent leurs convictions. Ces derniers peuvent ainsi avoir l'impression de « découvrir » un problème caché, comme une conspiration, et y adhérer fermement. Dans ce contexte, l'ironie et la caricature, perdent leur vocation initiale et deviennent des outils potentiels de manipulation de l'opinion publique.

La satire, bien plus qu'une simple forme d'humour critique, peut alors se transformer en un instrument redoutable de désinformation, brouillant davantage les frontières entre humour légitime et manipulation intentionnelle.

Bien que les biais cognitifs jouent un rôle important dans la création et la crédibilité des faux contenus écrits, il est désormais important d'examiner plus en détail l'impact des images. Analyser la manipulation de ces dernières permet de mieux comprendre leur influence dans la propagation de la désinformation ainsi que la fragilisation de la confiance envers les systèmes d'information.

[30] Secrétariat général de la défense et de la sécurité nationale. « RRN : une campagne numérique de manipulation de l'information complexe et persistante », 13 juin 2023. Lien
[31] Beauvais. *Op.cit.*
[32] *Ibid.*

3. LE POUVOIR DES IMAGES : LES ÉLÉMENTS VISUELS DANS LA DÉSINFORMATION NUMÉRIQUE

De nos jours, la désinformation s'accompagne de plus en plus d'éléments visuels, qu'il s'agisse de photos ou de vidéos (comme les réels ou autres formats), tandis que les éléments textuels eux, sont souvent associés à des composants graphiques. Cette tendance est désignée dans la littérature scientifique francophone par le terme de « désinformation visuelle et multimodale » [33] et dans la recherche anglo-saxonne, par celui de « visual disinformation ». Les images jouant un rôle prédominant dans la sphère numérique, il semble évident que certains acteurs les utilisent afin de diffuser des informations malveillantes dans l'objectif d'impacter négativement les structures démocratiques, la construction personnelle et collective de valeurs ainsi que l'accès fiable à des informations basées sur des faits. Pourtant, le rôle de la composante visuelle dans les campagnes de désinformation numériques reste largement inexploré en tant qu'objet de recherche en sciences sociales [34]. Il est clair que les médias sociaux jouent un rôle déterminant dans le processus de mise à disposition intentionnelle d'informations malveillantes. Ainsi, dans le contexte du présent rapport, cette partie tentera dans un premier temps de donner un bref aperçu de l'état actuel des connaissances concernant les effets des éléments visuels et multimédias dans le contexte de la désinformation, puis, s'attachera à l'étude de l'importance des images en tant que partie intégrante de la désinformation numérique.

a. L´élément visuel : un catalyseur pour la désinformation numérique

Le Center for Data Ethics and Innovation du gouvernement britannique rapporte que depuis plus de 150 ans, des formats visuels sont utilisés pour influencer la formation de l'opinion publique en faveur de certains acteurs (rapport CDEI). L'impact considérable des images dans l'espace numérique est souvent sous-estimé, de sorte que l'ampleur des effets négatifs à cet égard est également très peu connue. Il est donc important, dans un premier temps, de rappeler brièvement l'état actuel des connaissances sur l'impact des formats visuels dans le monde numérique en général.

[33] « Comprendre les menaces et les défis - Désinformation visuelle et multimodale (DVM) ». Laboratoire sur l´intégrité de l´information de l'Université d'Ottawa. Lien
[34] Viorela Dan, Britt Paris, Joan Donovan, Michael Hameleers, Jon Roozenbeek, Sander van der Linden, et Christian von Sikorski. « Visual Mis- and Disinformation, Social Media, and Democracy ». Journalism & Mass Communication Quarterly, 25 août 2021. Lien.

Les chercheurs ont fréquemment souligné l'influence de l'information visuelle sur les utilisateurs des médias, que ce soit dans le choix et la sélection des informations [35], dans les émotions suscitées ou encore dans les comportements qu'elle engendre chez les consommateurs [36]. Dans l'ouvrage *The role of images in framing new stories*, Messaris et Abraham affirment que ces effets seraient dus au sentiment d'une garantie implicite de la part du consommateur de se trouver « *plus près de la vérité que d'autres formes de communication* » [37], dès lors que les images font partie de leur apport d'informations. De plus, comme le rapporte le Laboratoire sur l'intégrité de l'information, l'interprétation de contenus visuels nécessiterait « *habituellement moins d'efforts cognitifs* » [38]. Il semble alors assez aisé d'affirmer que les images, couplées à une information, ont un pouvoir persuasif sur le consommateur.

Ce constat est appuyé par de nombreuses sources scientifiques, notamment le Laboratoire sur l'intégrité de l'information qui a pu observer que les contenus visuels manipulés (comme les deepfakes, sur lesquels nous reviendrons plus tard) « peut être (mal) utilisé comme un type de « preuve » crédible ». Même si la recherche isolée concernant l'effet des images - puisqu'il s'agit dans la plupart des cas de contenus multimédias - est très difficile à mettre en œuvre d'un point de vue méthodologique, les scientifiques sont unanimes sur cet effet précis de persuasion. En effet, à travers l'étude de l'interaction entre les formes multimédias de désinformation et les processus de décision politique, Hameelers et d'autres chercheurs ont conclu que « la désinformation multimodale est considérée comme légèrement plus crédible que la désinformation textuelle » [39].

Cela suggère à nouveau que les contributions visuelles ont tendance à avoir un effet « catalyseur », c'est-à-dire un effet de renforcement, dès que la contribution s'adresse à la conviction du consommateur. Dans le cadre d'une analyse à méthodologie mixte réalisée en 2021 sur la désinformation visuelle dans le cadre de reportages numériques pendant la pandémie de Covid-19, les chercheurs ont constaté que la composante visuelle de plus de la moitié des reportages examinés « servait explicitement de preuve pour de fausses allégations, dont la plupart sont mal étiquetées plutôt que manipulées » [40]. Outre les effets des contributions visuelles dans le contexte de la désinformation, la question de la marge d'interprétation de l'observateur se pose également. Dans tous les cas, il est important de prendre en compte les effets psychologiques et sociaux à long terme dans le contexte de la désinformation numérique, qu'elle soit véhiculée par l'image ou le texte.

[35] Dolf Zillmann, Silvia Knobloch, et Hong-sik Yu. « Effects of photographs on the selective reading of news reports ». *Media Psychology*, 2001. Lien.
[36] *Ibid.*
[37] Paul Messaris et Linus Abraham. « The Role of Images in Framing News Stories ». In Framing public life: Perspectives on media and our understanding of the social world. Routledge, 2001. Lien
[38] Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa. *Op.cit.*
[39] Michael Hameleers, Thomas E. Powell, Toni G.L.A. Van Der Meer, et Lieke Bos. « A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media ». Political Communication, 3 mars 2020. Lien
[40] J. Scott Brennen, Felix M. Simon, et Rasmus Kleis Nielsen. « Beyond (Mis)Representation: Visuals in COVID-19 Misinformation ». The International Journal of Press/Politics, janvier 2021. Lien

Par ailleurs, le support d'information, qu'il soit papier ou numérique, influence la manière dont les informations sont perçues et traitées, influence la perception et le traitement des contenus, ce qui conditionne leur crédibilité et la confiance que les individus leur accordent.

Il est essentiel de retenir que les contenus intégrant des éléments visuels ont une plus grande probabilité d'être mémorisés par leurs consommateurs, ce qui amplifie évidemment leur impact en cas de diffusion d'informations factuellement incorrectes.

En conséquence, pour l'ensemble des informations accessibles au public, le fossé entre les personnes qui ont tendance à croire aux informations correctes et celles qui ont plutôt tendance à croire aux informations fausses ne cesse d'augmenter. Cependant, les connaissances dans ce contexte restent peu étudiées, de sorte que les effets divers et variés de la désinformation visuelle et multimodale nécessiteraient de plus amples recherches qui seraient pertinentes pour les scientifiques spécialisés. Dans ce contexte, les contenus visuels exercent également une influence plus profonde, dans la mesure où ils deviennent et produisent une certaine forme d'autorité, servant de fait, à la légitimation de l'action politique.

b. Quels défis et responsabilités dans l'évolution des techniques visuelles et multimodales ?

Les éléments visuels en tant que source d'information (ou source partielle) ne posent pas seulement des questions quant à la fiabilité des contenus médiatiques en général, mais aussi quant au degré d'avancement de la conception technique de ces derniers. Il est frappant de constater que le degré de sophistication peut varier considérablement. L'un des « outils » déjà évoqués et connus est ce que l'on appelle les *deep fakes*. Étymologiquement, le mot est composé du terme « deep learning », qui exprime dans ce contexte l'utilisation de l'intelligence artificielle, et du mot « fake », que l'on traduit de l'anglais par « faux » [41] (l'information ici est factuellement fausse).

[41] Nadine Liv et Dov Greenbaum. « Deep Fakes and Memory Malleability: False Memories in the Service of Fake News ». *AJOB Neuroscience*, 2 avril 2020. Lien

Bien qu'il soit quasiment impossible de prouver des exemples concrets de désinformation utilisant des *deep fakes*, le pouvoir potentiel de telles techniques sur le débat sociopolitique dans l'espace public actuel est évident. Les *deep fakes* représentent alors une menace considérable, notamment lorsqu'ils ont pour but de manipuler la perception du public et d'influencer les modèles de comportement. Les *deep fakes* sont également connus pour charger divers contenus de manière humoristique, ce qui, en résumé, soulève également des questions quant à la fiabilité des contenus médiatiques en général.

Néanmoins, dans le contexte du vaste champ de la désinformation visuelle et multimodale, les contenus visuels complexes, techniquement sophistiqués et basés sur l'IA ne représentent qu'une partie des méthodes rencontrées. Dans leur analyse sur la désinformation et les reportages durant la crise de la Covid-19, Brennen, Simon et Nielson ont également constaté que les fausses sources d'informations visuelles avaient en réalité toutes été créées à l'aide d'outils très simples [42]. A fortiori, qu'aucune n'avait été créée à l'aide de *deep fakes* ou d'autres technologies basées sur l'IA. À cet égard, le laboratoire sur l'intégrité de l'information rapporte que le traitement numérique des images est devenu beaucoup plus accessible depuis les années 1990, entre autres du fait de l'introduction de Photoshop [43]. Le même rapport explique également que les méthodes de DVM peuvent être catégorisées en *cheap fakes* et *shallow fakes*, dont le contenu est dans les deux cas moins complexe que le contenu des *deep fakes* [44]. Ces dernières années, le développement de logiciels basés sur l'IA pour l'utilisation et la création de tels contenus en libre accès a connu une croissance significative : citons par exemple Transformers (Google, 2017), Bert (Google, 2018) et surtout GPT2, 3 et 4 (respectivement OpenAI 2019, 2020, 2023) [45]. Cela complique également l'analyse scientifique de l'impact de la désinformation car les contenus de désinformation sous des formes « hybrides » circulent désormais en grande quantité sur les réseaux, atteignant des niveaux significatifs.

Dans tous les cas, il est certain que les utilisateurs ont beaucoup plus de mal à faire confiance aux informations et aux messages [46]. En conséquence, les médias sociaux ont pris le rôle de « gardien » de l'information, remplaçant ainsi les médias traditionnels. Ils permettent désormais aux politiciens et autres acteurs de communiquer directement avec le public, contournant les mécanismes de contrôle et de médiation journalistique. Le microciblage, l'utilisation des préférences de profil et préjugés, rendent plus difficile l'identification du danger. A cela s'ajoute la rentabilité économique : en raison des faibles coûts d'accès, de production et de diffusion des nouvelles et des contenus, la quantité de désinformation/d'informations erronées augmente [47].

[42] Brennen et al. *Op.cit.*
[43] Laboratoire sur l´intégrité de l´information de l'Université d'Ottawa. *Op.cit.*
[44] *Ibid.*
[45] *Ibid.*
[46] Rachel Armitage et Cristian Vaccari. « Misinformation and disinformation ». In The Routledge Companion to Media Disinformation and Populism, 2021.
[47] *Ibid.*

Les différents médias sociaux constituent ainsi un espace de communication numérique global, influencé par divers mécanismes sociologiques et psychologiques. Ces dynamiques génèrent des effets divers, encore insuffisamment étudiés, tout en créant un lien fort avec les consommateurs et de fait, des conséquences aux niveaux individuel et collectif. Dans ce contexte, les médias sociaux semblent être pour les utilisateurs des médias (par exemple les propriétaires de médias sociaux tels que le conglomérat Meta, les influenceurs ou les activistes) une manière de (se) vendre, au sens économique comme au sens sociologique du terme. Les médias sociaux eux-mêmes agissent comme un instrument pour la transmission des quantités gigantesques d'informations qui, comme nous avons pu l'observer, laissent plus que jamais une marge d'interprétation grâce à la combinaison d'éléments visuels et écrits. L'information qui se trouve au cœur de chaque contribution médiatique (reels, photo, vidéo, etc.) donne l'impression d'être « cachée » ou, du moins, d'être de plus en plus reléguée au second plan de l'ensemble des informations disponibles sur le réseau. Cela a pour conséquence, d'une part, l'élargissement du champ d'informations erronées, donc de la désinformation. Mais également celle d'une remise en doute de la fiabilité des mesures visant à un traitement de l'information plus transparent et basé sur des faits (comme par exemple l'organisation Fact-Checking). C'est peut-être pour cette raison qu'une part de plus en plus importante de la population se demande « à quelle vérité dois-je accorder du crédit ».

Enfin, tout cela peut aussi conduire, même si nous ne pouvons encore dire dans quelle mesure, à des malentendus sur des convictions fondamentales personnelles et collectives, qui se traduisent par des débats sociopolitiques, des polémiques, voire des conflits trans- et internationaux. Des études montrent que seule une minorité d'utilisateurs évite systématiquement les contenus politiques avec lesquels ils ne sont pas d'accord. Ainsi, la grande majorité d'entre eux renforcent leurs convictions préexistantes sur les réseaux [48].

Il semble finalement que la responsabilité de remédier à la tendance actuelle vers une (re)production accrue de désinformation, ainsi que la diversification croissante des techniques de désinformation qui en découle dans l'espace numérique, doivent être considérées sous plusieurs angles. Dans ce sens, différents acteurs à différents niveaux - journalistique, privés et/ou publics dans le cadre européen/UE ou national - auraient également des domaines de responsabilité individuels. C'est à cette condition que le défi très vaste de la désinformation pourrait être abordé de manière appropriée dans son ampleur, afin de garantir un traitement transparent, démocratique et équitable de l'information au sens le plus large du terme.

[48] Armitage et al. *Op.cit.*

CONFRONTATIONS EUROPE

Sciences Po Strasbourg
École
de l'Université de Strasbourg

DOSSIER SPÉCIAL DÉSINFORMATION
& INGÉRENCE ÉTRANGÈRE

LA PROPAGATION DE LA DÉSINFORMATION À UN LARGE AUDITOIRE

VECTEURS PHYSIQUES ET NUMÉRIQUES DE DIFFUSION DU DISCOURS DE DÉSINFORMATION

Afin de propager la désinformation à une audience la plus large possible, les Etats ingérants utilisent plusieurs relais. Ces relais de désinformation peuvent être des intermédiaires influents au niveau national (1). Le contenu désinformationnel est également diffusé massivement par une utilisation efficace des outils numérique et une automatisation de cette diffusion (2). Enfin, les différentes techniques de propagation sont généralement croisées et la désinformation est diffusée via plusieurs vecteurs qui opèrent simultanément (3).

1. LA DIFFUSION PAR UN INTERMÉDIAIRE

En étant relayée par des intermédiaires divers qui disposent de la confiance de la population et d'une certaine autorité et/ou crédibilité, la désinformation peut atteindre un public le plus large possible. Le lien entre le relais de désinformation et sa source est souvent rendu explicite par le fait qu'il y ait un transfert d'argent. Pourtant, la motivation des intermédiaires n'est pas systématiquement d'ordre financier. Il peut s'agir de droits et de privilèges qui sont octroyés en échange de la diffusion de désinformation. Parfois même, un relais de désinformation peut avoir cette position sans en avoir conscience. Il peut par exemple être convaincu de la vérité du discours qu'il propage. Dans ce cas, sa motivation est d'ordre idéologique. Mais l'intermédiaire peut également être victime d'usurpation de son identité, dans ce cas son nom et son influence servent à la propagation d'un discours à son insu.

Ainsi, différentes sphères sont régulièrement les cibles de ceux qui cherchent des relais de désinformation. Parmi des individus crédibles et capables de transmettre le message à un grand nombre, on retrouve les sphères politiques et gouvernementales, les universités et le monde médiatique. Plus récemment, les influenceurs sur les réseaux sociaux sont également la cible d'États tentant de diffuser de fausses informations, notamment visant un public plus jeune.

a. Les élus et sphères gouvernementales

Les élus sont des intermédiaires de choix lorsqu'il s'agit de véhiculer de fausses informations. En mesure d'orienter les décisions publiques ou les législations, ceux-ci sont en effet contactés par des États tiers à la recherche de plaidoyer en leur faveur au sein de diverses institutions. Leur influence peut être « achetée » financièrement, il est pourtant également possible que leur autorité soit utilisée à leur insu, notamment via l'usurpation de leur identité.

L' « achat » des voix politiques par la corruption financière

La corruption par l'échange d'argent constitue une des méthodes « traditionnelles » de l'influence et de la désinformation. Elle est encore abondamment utilisée aujourd'hui. Le cas récent le plus emblématique est le scandale du Qatargate de 2022 au cours duquel l'eurodéputée grecque Eva Kaïlí, alors vice-présidente du Parlement européen, mais également Pier Antonio Panzeri, Président de la sous-commission des droits de l'Homme du Parlement entre janvier 2017 et juillet 2019 et d'autres acteurs de milieux proches des sphères décisionnelles (confédérations syndicales, organisations non-gouvernementales) [49] sont accusés d'avoir plaidé en faveur du Qatar, affirmant notamment son exemplarité en termes de droits des travailleurs. En parallèle étaient pourtant révélées les très mauvaises conditions de travail des ouvriers sur les chantiers de construction des infrastructures destinées à accueillir la Coupe du monde de football. En échange des voix de ces officiels, il apparaît que le Qatar leur a versé des sommes d'argent considérables. Plus d'un million d'euros en liquide ont en effet été saisis par la police fédérale belge en charge de l'enquête [50].

Le soutien financier peut d'ailleurs être accordé plus globalement à des partis politiques. Le Parlement européen mentionne ainsi de véritables « *relations de dépendances avec certains partis politiques européens* » notamment liés à leur financement et/ou à l'accord de prêt russes. Sont ainsi pointés du doigt des partis d'extrême droite, notamment l'AfD allemand et le RN français [51]. Le discours pro-russe de membres de ces deux partis semble ainsi lié, au moins en partie, à cette dépendance financière [52]. C'est ainsi via la corruption financière que les voix de diverses personnalités politiques peuvent être « achetées » et qu'il va être possible pour une puissante ingérante d'orienter le débat public.

[49] Jean-Philippe Leffief. « Qatargate » : ce que l'on sait des soupçons de corruption au Parlement européen ». *Le Monde*, 15 décembre 2022. lien.
[50] Valentin Ledroit. « Qatargate : tout comprendre au scandale de corruption qui touche le Parlement européen ». Touteleurope.eu, 3 octobre 2023. lien.
[51] Parlement Européen. Proposition de résolution et résolution sur le Russiagate 8 février 2024.
[52] Romain Geoffroy et Maxime Vaudano. « Quels sont les liens de Marine Le Pen avec la Russie de Vladimir Poutine ? » Le Monde, 20 avril 2022. lien.

Usurper l'identité par le piratage : l'utilisation de l'influence des responsables politiques à leur insu

Il est également possible d'utiliser l'influence de personnalités politiques et de faire circuler de fausses informations en leur nom à leur insu. C'est ce que le rapport du réseau de journalistes Forbidden Stories montre dans son enquête sur l'entreprise israélienne de désinformation "Team Jorge"[53]. Leur rapport montre la capacité de l'entreprise à pirater et prendre le contrôle de messageries privées de responsables politiques (en l'occurrence de hauts responsables africains), notamment leurs adresses Gmail et leurs comptes Telegram. Il est alors non seulement possible d'avoir accès librement à tout le contenu relié à ces comptes (drive et carnet d'adresses), mais également d'usurper l'identité de la victime et d'envoyer des mails et messages à sa place et en son nom.

Cette technique aurait notamment été utilisée dans le contexte de l'élection kényane de 2022 [54]. Si une telle technique n'a, a priori, pas été utilisée à l'encontre de responsables européens jusqu'à aujourd'hui, il semble pourtant impératif d'avoir conscience de son éventualité et d'être préparés à la déstabilisation qui pourrait en résulter, notamment lors d'événements institutionnels clés tels que les élections.

b. Les universités et la recherche

L'université est elle aussi le terrain d'action des stratégies d'influence étrangère et au sein de laquelle il est intéressant pour des puissances étrangères de diffuser de la désinformation, notamment dans le but de façonner une certaine image et une meilleure réputation étatique.

Plusieurs institutions européennes se sont saisies de la question et ont pointé du doigt ces influences. La Commission Européenne s'est notamment penchée sur la question des ingérences étrangères dans la recherche et l'innovation [55]. Au niveau national, différents organismes se sont également inquiétés de la situation, c'est le cas de la fondation suédoise pour la coopération internationale dans la recherche et l'éducation supérieure [56], ou encore le Sénat français qui a publié en septembre 2021 un rapport d'information [...] sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences [57].

[53] Cécile Andrzejewski. « "Team Jorge" : Révélations sur les manipulations d'une officine de désinformation ». Forbidden Stories (blog), 15 février 2023. lien.
[54] *Ibid.*
[55] UE, « Tackling R&I Foreign Interference: Staff Working Document », 2022. lien.
[56] Stefan Östlund, Tommy Shih, et Albin Gaunt. « Responsible Internationalisation : Guidelines for Reflection on International Academic Collaboration ». STINT, The Swedish Foundation for International Cooperation in Research and Higher Education, 2020. lien.
[57] André Gattolin. « Rapport d'information (...) sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences ». Direction de l'information légale et administrative, Sénat, 2021. lien.

C'est particulièrement la restriction de la liberté académique qui inquiète. Celle-ci se remarque dans le cas d'une dépendance financière des chercheurs à un État tiers, mais également dans le cadre de pressions quant à l'accès au territoire étudié, par exemple via l'attribution de visas.

Le financement étranger des universités et de la recherche, source de remise en question de la liberté académique

Tous les rapports cités précédemment décrivent un paramètre commun : le lien entre le financement étranger des universités et la dépendance académique qui peut en résulter.

La problématique touche d'abord les chercheurs financés par une puissance étrangère. Le risque pour ces chercheurs de transformer le discours, les focus académiques voire le résultat des recherches est ainsi avéré dans le cas d'une dépendance financière à un État tiers pour la tenue des travaux de recherches.

Or, les financements étrangers abondent dans les universités européennes. La Chine est ainsi l'un des États qui finance le plus de recherches en Europe et a ainsi développé le programme « 1000 talents », exclusivement destiné à recruter des chercheurs étrangers dans des domaines scientifiques clés [58]. C'est ainsi 203 projets de recherche en République tchèque dont le financement provient exclusivement de sources chinoises. En Autriche, 284 universitaires voient également leurs recherches financées exclusivement par la Chine. Pour autant, il faut noter que le phénomène est hétérogène à travers l'Europe, en Slovaquie par exemple, moins d'une vingtaine d'universitaires sont concernés [59]. Cette dépendance financière serait rendue possible par une relative insuffisance des ressources budgétaires allouées aux chercheurs dans le contexte européen [60]. Les pays occidentaux investissent des moyens relativement importants par rapport au reste du monde. Pourtant, de fortes disparités persistent, c'est ainsi les pays anglo-saxons et d'Europe du Nord qui dotent le mieux leurs universités, tandis qu'en Europe continentale et du sud, les dépenses sont beaucoup plus restreintes [61].

[58] Aneta Zachová, Laura Miraglia, Pekka Vanttinen, et Sofia Mandilara. « L'ingérence croissante de la Chine au sein des universités européennes ». Euractiv, 1 décembre 2022. lien.
[59] *Ibid.*
[60] *Ibid.*
[61] Julian Garritzmann. « Higher Education Funding across the Globe ». Education International, 15 mai 2024. lien.

Toujours en termes d'influence financière, certaines universités, particulièrement au Royaume-Uni, sont assez largement dépendantes des inscriptions d'étudiants étrangers, notamment chinois. Les universités britanniques accueillent ainsi « davantage d'étudiants chinois que le reste de l'Europe combiné » [62]. C'est ainsi une quinzaine d'universités britanniques qui tire de l'inscription d'étudiants chinois dans leur établissements plus d'un cinquième de leurs revenus [63]. Cette dépendance crée une fois de plus une difficulté à résister aux pressions chinoises, et se manifeste par de l'auto-censure et par une forte réticence des chefs universités à émettre des critiques à l'égard du gouvernement chinois.

L'attribution des visas comme moyen matériel de création de dépendance

D'autres moyens peuvent créer une dépendance des universités et chercheurs à un pays tiers. La Chine utilise par exemple sa capacité à délivrer (ou à refuser) des visas pour entrer sur son territoire comme un moyen de s'assurer une non critique du régime, ou encore pour se garantir la non évocation de thèmes sensibles, tels que le Tibet ou le Xinjiang et les Ouighours, Taiwan, ou encore les manifestations de la place Tian'anmen. Cette politique de restriction d'accès au territoire vise surtout les spécialistes de la Chine dont le travail requiert de se rendre dans leur pays d'étude [65].

Finalement, la dépendance des universités et des chercheurs européens à un État-tiers, qu'elle soit financière ou non, est un terreau fertile pour la propagation de désinformation au sein de la sphère universitaire.

La désinformation dans le cadre universitaire prend souvent la forme d'une « auto-censure » des chercheurs quant aux thèmes abordés et aux conclusions données.

[62] Charles Parton. « China-UK Relations: Where to Draw the Border Between Influence and Interference? » Royal United Services Institute for Defence and Security Studies, février 2019. lien.
[63] Paul Charon et Jean-Baptiste Jeangène Vilmer. Les opérations d'influences chinoises - Un moment machiavélien. Editions Des Equateurs, 2024.
[64] Ingrid D'Hooghe, Annemarie Montulet, Marijn de Wolff, et Frank N. Pieke. « Assessing Europe-China Collaboration in Higher Education and Research ». Leiden Asia Centre, 2018. lien.
[65] Amaury Renaudie. « La stratégie d'influence chinoise dans le monde universitaire français ». Enderi, 28 juillet 2023. lien.

c. Les médias et professionnels de l'information

Les médias et les professionnels du journalisme sont le relais de l'information par excellence. Plusieurs devoirs lient les journalistes, selon les modalités notamment décrites dans la Déclaration de Munich de 1971 [66]. Le journaliste doit ainsi « *Respecter la vérité, quelles qu'en puissent être les conséquences pour lui-même, […]. Rectifier toute information publiée qui se révèle inexacte* ». Il doit également « *S'interdire […] de recevoir un quelconque avantage en raison de la publication ou de la suppression d'une information* » et « *n'accepter de directives rédactionnelles que des responsables de la rédaction* ».

Ces précautions érigées à la base même du métier de journaliste sont le reflet du pouvoir potentiel d'une information erronée diffusée via les médias. Il y apparaît également que des personnes tierces pourraient être effectivement tentées d'influencer le discours médiatique.

La captation de journalistes en échange d'argent

Il arrive pourtant que des médias soient la cible d'ingérences étrangères et se transforment en relais de désinformation. En témoigne l'affaire M'Barki documentée notamment par l'enquête « Story Killers » menée par un consortium de journalistes européens pour Forbidden stories [67].

Début février 2023, Rachid M'Barki, figure historique de BFMTV, diffuse ainsi plusieurs contenus qui n'ont au préalable pas suivi le cursus habituel de validation par la rédaction. Parmi les propos qui questionnent se trouve notamment l'utilisation inhabituelle au sein du paysage médiatique français de l'expression « *Sahara marocain* », mais aussi des informations en lien avec la Russie et sa diaspora d'oligarques à Monaco qui risquerait des difficultés économiques en lien avec des sanctions de l'UE contre la Russie. Des propos attaquant l'ancien procureur général du Qatar, Ali Bin Fetais Al-Marri ont également été diffusés. Ce qui interroge alors, c'est l'incohérence du contenu de ces brèves par rapport à la ligne éditoriale de la chaîne. Il apparaît finalement que R. M'Barki aurait diffusé ces contenus en réponse à une demande du lobbyiste Jean-Pierre Duthion, lui-même a priori mandaté par l'entreprise Team Jorge, selon l'enquête de Forbidden Stories. Si les liens financiers sont encore flous aujourd'hui, il semble bien qu'il y ait eu des versements d'argent [68].

66] « Charte de déontologie de Munich ». CFDT Journalistes. lien.
[67] Cécile Andrzejewski. « "Team Jorge" : Révélations sur les manipulations d'une officine de désinformation ». Forbidden Stories (blog), 15 février 2023. *lien*.
[68] Ouest France. « Soupçons d'ingérence à BFMTV. « J'étais manipulé » : Rachid M'Barki aurait reconnu avoir été payé ». 19 janvier 2024, sect. BFMTV. lien.

L'entreprise « Team Jorge » avait notamment été impliquée dans l'affaire de Cambridge Analytica et a pour clients des États, des entreprises et de riches individus, répartis a minima dans une soixantaine de pays. C'est ainsi un total d'une douzaine de sujets problématiques qui ont été diffusés par R. M'Barki, au profit notamment du Qatar et du Maroc, mais également d'intérêts privés russes.
Parmi les raisons qui semblent motiver un journaliste à enfreindre la charte de déontologie de son métier, Laurent Esquenet, député et vice-Président de la Commission de lutte contre les ingérences étrangères en 2023 [69] estime qu'une certaine précarisation du métier de journaliste pourrait expliquer l'appât que représente la diffusion de désinformation en échange de sommes d'argent conséquentes. Pourtant, pour le député européen Serguey Lagodinsky [70], bien que les financements soient une partie du problème, l'éthique des journalistes serait également en partie responsable. Il insiste enfin sur la nécessité de structures organisées de journalistes pour faire face aux tentatives d'ingérences étrangères.

Les risques liés à la propriété étrangères de médias européens

Un autre risque de diffusion de désinformation au sein des médias européens réside dans la possession par des États tiers d'actions dans les capitaux de médias européens. La plupart des États européens établissent ainsi des limites à la possession étrangère d'un média. La Grèce limite par exemple la propriété par des non-résidents à 25% du capital pour une chaîne de télévision et à 49% pour le capital d'une compagnie de radio. En Italie, la loi sur la télévision privée interdit plus largement aux ressortissants extra-communautaires de prendre des actions dans le capital de chaînes de télévision, à moins qu'un accord bilatéral ne les y autorise. Une forte disparité réglementaire entre les États européens transparaît donc. Jusqu'à très récemment, le Royaume-Uni ne fixait ainsi aucune limitation aux participations étrangères. Pourtant en mars 2024, le Daily Telegraph frôle la faillite et une offre de rachat du fonds privé IMI, possédé par le cheikh Mansour Ben Zayed, de la famille régnante d'Abou Dabi, et vice-président des Emirats arabes unis, fait scandale. Les inquiétudes se multiplient. Fraser Nelson, rédacteur en chef du *Spectator* estime ainsi que [71] :

« Si les gouvernements se mettent à posséder un journal, que ce soit le gouvernement britannique, ou un gouvernement européen ou arabe, la liberté de la presse serait mortellement compromise. »

[69] Propos confiés lors d'un entretien réalisé par notre équipe le 18 octobre 2024
[70] Dans une interview accordée à Euractiv pour le rapport « The state of media freedom in Europe, challenges and protections », 30 novembre 2024 lien
[71] Eric Albert. « Le Royaume-Uni interdit l'acquisition de journaux par des Etats étrangers ». Le Monde, 15 mars 2024. lien.

En réaction, le gouvernement britannique a modifié la loi qui empêche désormais toute acquisition d'un journal ou d'un magazine par un « *État étranger* » et par des « *agents de gouvernements étrangers qui opèrent à titre privé* » [72]. Un cas effectif d'ingérence de ce type a par ailleurs été rapporté par une étude pour le projet MapInfluenCE [73] en République tchèque. Ainsi, en 2015, la société chinoise CEFC20 a obtenu des actions dans l'entreprise Empresa Media. Grâce à ces dernières, la société s'est garantie l'accès à une chaîne de télévision (TV Barrandov) et à plusieurs magazines. L'enquête a révélé que cette acquisition a eu un impact profond sur le discours des médias de l'entreprise quant à la Chine qui ont dès lors commencé à n'évoquer ce pays que sous un angle positif et élogieux.

d. Les influenceurs

Plus récemment, les influenceurs actifs sur divers réseaux sociaux se sont imposés en tant que nouvelle sphère à fort pouvoir de dissémination d'informations. Dotés de communautés d'internautes qui les suivent en général de manière très régulière et qui leur accordent une certaine confiance, les influenceurs ont en effet un fort pouvoir d'orientation de l'opinion de ceux qui les suivent. Enfin, ils permettent de cibler une catégorie de la population souvent plus jeune par rapport aux intermédiaires décrits précédemment (figures politiques, universités, presse traditionnelle).

Cette confiance accordée par une communauté à un internaute est ainsi un vecteur très efficace pour la diffusion de désinformation. Les influenceurs sont en effet régulièrement approchés par des acteurs désireux de propager de la désinformation.

La désinformation par des influenceurs rémunérés

Dans le contexte de la crise du Covid-19, plusieurs influenceurs européens (notamment le youtubeur français Léo Grasset, détenteur de la chaîne « Dirty Biology » et Sami Ouladitto détenteur du compte Instagram « Et ça se dit médecin » ou encore l'allemand Mirko Drostchmann) ont été démarchés par l'entreprise russe Fazze pour dénigrer le vaccin Pfizer au profit de Spoutnik V [74]. Il était notamment demandé d'affirmer que le vaccin russe avait un taux de mortalité bien inférieur au Vaccin Pfizer. Là encore, l'entreprise a proposé des sommes d'argent conséquentes en échange de la diffusion de son message par les influenceurs. Il faut noter qu'il ne s'agit pas d'une simple demande de publicité ou de promotion, mais bien d'une tentative malhonnête d'influence de l'opinion.

[72] amendement de l' « Enterprise Act 2002 » par le « Digital Markets, Competition and Consumers Act 2024 »
[73] Ivana Karásková, Tamás Matura, Richard Q. Turcsányi, et Matej Šimalčík. « Central Europe for Sale: The Politics of China's Influence ». Association for International Affairs (AMO), 16 avril 2018. lien.
[74] Courrier international. « Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée ». 26 mai 2021. lien.

En témoignent par exemple les instructions envoyées aux influenceurs. Dans les mails reçus, était notamment soulignée l'importance de faire passer le message comme incarnant leur « propre point de vue indépendant ». Le mail demandait également explicitement à ce que l'entreprise Fazze ne soit pas mentionnée et que l'audience ne s'aperçoive pas qu'il s'agissait d'un contenu sponsorisé - payé par un tiers. Le but global de l'opération était donc explicitement que le message « *apparaisse comme un conseil à votre audience* » [75]. Il est donc clair que l'entreprise est consciente qu'il ne s'agissait pas simplement de faire simplement de la publicité pour un produit mais bien d'influencer l'opinion via des informations erronées - la mortalité prétendue moins élevée du vaccin russe. Des techniques similaires sont utilisées par le régime chinois qui propose des rémunérations financières ou d'autres avantages matériels, par exemple des voyages en Chine dans des hôtels de luxe [76].

La désinformation via des influenceurs idéologiquement convaincus

Par ailleurs si certains profils d'influenceurs sont susceptibles de céder à de telles demandes en raison des profits potentiels, d'autres sont d'abord poussés par des motivations idéologiques [77]. Selon le chercheur Paul Charon, c'est notamment l'adhésion aux thèses soutenues par le Parti Communiste chinois ou par la Russie, ou encore une convergence des deux sur la base d'anti-américanisme qui va pousser des influenceurs à adopter un discours désinformationnel, qui frôle parfois le complotisme, en lien en particulier avec la Chine ou la Russie.

Finalement, il faut insister sur le fait que les différents intermédiaires décrits sont généralement les maillons d'une chaîne plus complexe.

Les cas d'interférences ne se cantonnent pas à l'utilisation d'un seul intermédiaire. Au contraire, dans une recherche d'efficacité des campagnes de désinformation, c'est en général plusieurs intermédiaires issus de sphères différentes qui sont approchés simultanément. Par ailleurs, toujours en vue d'une propagation large et rapide, plusieurs moyens numériques de renforcer la propagation de désinformation existent et sont vecteurs d'une distribution massive de cette dernière.

[75] Courrier international. « Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée ». 26 mai 2021. lien.
[76] Interview de Paul Charon par Jérémy André. « Chine : désinformation, manipulations et agents d'influence sur les réseaux sociaux ». *Le Point*, 17 février 2024. lien
[77] *Ibid.*

2. LES TECHNIQUES NUMÉRIQUES DE PROPAGATION MASSIVE DE DÉSINFORMATION

Avec l'évolution des outils numériques, les campagnes de désinformation s'appuient sur des techniques sophistiquées pour massifier leur propagation. Automatisation de la diffusion, optimisation du référencement et exploitation de l'espace publicitaire sont autant de moyens utilisés pour manipuler les perceptions et amplifier des récits fallacieux. Le numérique est devenu l'outil majeur de la lutte informationnelle, qui est l'ensemble d'actions visant à garantir une supériorité sur l'adversaire par l'usage de l'information. Cette partie explore ainsi les principales techniques numériques utilisées pour propager la désinformation.

a. L'automatisation massive de la diffusion de désinformation par les bots

Les bots sont des comptes automatisés actifs sur les réseaux sociaux. Ils exécutent en majorité des tâches répétitives et prédéfinies et sont un large vecteur de propagation de désinformation en ligne. Les premiers bots développés étaient relativement simplistes. Leur tâche était notamment de poster différents liens de spams sur le plus de plateformes possibles, mais les comptes étaient souvent peu crédibles et le message final peu soigné, ce qui les rendait faciles à détecter. À l'inverse, les « *social bots* » sont des programmes plus sophistiqués qui reproduisent les comportements humains afin de gagner la confiance d'autres utilisateurs en ligne. Une fois cette confiance acquise, ces bots peuvent diffuser de la désinformation qu'il sera plus difficile pour un utilisateur de détecter et de se méfier [78].

Le phénomène est de très grande ampleur. Ainsi, en 2017 sur le total des comptes présents sur Twitter, jusqu'à 15% étaient en réalité des bots [79]. Selon Imperva, une filiale de Thalès, c'est 16 % du trafic internet mondial qui est généré par des bots. Autour de moments politiques cruciaux, la part de trafic générée par des bots grimpe encore. Durant le premier impeachment de D. Trump par exemple, c'est plus de 30% des tweets générés en lien avec ce thème qui étaient publiés par des bots [80].

[78] Susan Morgan. « Fake news, disinformation, manipulation and online tactics to undermine democracy ». *Journal of Cyber Policy*, 2 janvier 2018. lien
[79] Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, et Alessandro Flammini.
« Online Human-Bot Interactions: Detection, Estimation, and Characterization », 27 mars 2017.
lien.
[80] Michael Rossetti et Tauhid Zaman. « Bots, disinformation, and the first impeachment of U.S. President Donald Trump ». *PLOS ONE*, 8 mai 2023. lien.

La manière dont fonctionne la diffusion de désinformation à partir des bots est double. D'une part, par la publication massive de fausses informations, les bots amplifient la part de désinformation présente sur les réseaux sociaux. Celle-ci est donc plus fréquente sur les fils d'actualité des utilisateurs. Par ailleurs, une même information, diffusée de manière coordonnée par plusieurs bots, a plus de chances de devenir une « tendance » que l'algorithme du réseau social va souvent lui-même mettre en avant. Les bots eux-mêmes participent au « succès » d'une publication en la partageant et en lui ajoutant des « *likes* ». D'autre part, l'abondance de désinformation sur les réseaux sociaux a également un rôle dissimulateur. C'est-à-dire que les informations légitimes vont avoir moins de chances d'être vues par les utilisateurs du fait de la surabondance de fausses informations qui « prennent la place » des premières [81].

Par ailleurs, si les bots sont initialement programmés par des humains, la place de l'intelligence artificielle dans ces réseaux est croissante et permet un développement encore supérieur en termes de quantité de rapidité, et finalement en termes d'efficacité.

Très récemment, c'est dans le cadre des élections présidentielles croates que le phénomène a été pointé du doigt. Un grand réseau de bots a été découvert par le Centre for Information Resilience [82]. De nombreux faux comptes diffusant des messages pro-russes, anti-UE et anti-OTAN, en concordance avec les propos du président Zoran Milanovic dont la réélection n'est pas assurée, ont ainsi été mis en lumière. Ces algorithmes avaient une activité significativement supérieure à la moyenne, avec parfois plus de cent publications par jour. Nombre d'entre eux étaient dotés de photos de profil générées par IA. Dans cet exemple, la volonté d'atteindre une audience le plus large possible est très perceptible. Les bots publiaient effectivement dans au moins six langues différentes (anglais, français, espagnol, italien, serbe et croate) [83].

Finalement, si la place du numérique tend à prendre de l'ampleur, l'activité humaine dans ce cadre n'est pas négligeable pour autant. Plusieurs études ont ainsi montré que l'efficacité des bots est d'autant plus grande lorsqu'elle est étroitement couplée à une activité ou supervision humaine. Certains parlent de « cyborg », pour décrire ce mode d'action mi-humain mi-robot [84].

[81] Michael Rossetti et Tauhid Zaman. « Bots, disinformation, and the first impeachment of U.S. President Donald Trump ». PLOS ONE, 8 mai 2023. lien.
[82] Centre for Information Resilience. « Disinformation Campaign Uncovered by Researchers Ahead of Croatian Presidential Run-Off », 8 janvier 2025. lien
[83] Starcevic, Seb. « Russian Bots Boosted NATO Critic Ahead of Croatian Election, Researchers Say ». *POLITICO*, 9 janvier 2025.lien
[84] *Ibid.*

b. L'optimisation du référencement du contenu

Pour que les campagnes de désinformation atteignent leur plein potentiel, une optimisation minutieuse du référencement des contenus sur les moteurs de recherche, les réseaux sociaux et d'autres plateformes numériques est cruciale. Ce référencement consiste à améliorer la visibilité des messages dans les résultats de recherche ou les fils d'actualité des utilisateurs, souvent par le biais de mots-clés stratégiques ou d'algorithmes de classement spécifiques. Ces actions peuvent être menées par des acteurs étatiques ou privés, qui adaptent continuellement leur stratégie pour contourner les mécanismes de modération ou tirer parti des changements dans les algorithmes des plateformes.

Une première méthode clé, mentionnée par VIGINUM dans son rapport technique de février 2024 sur le réseau numérique de propagande prorusse Portal Kombat [85], est l'optimisation du référencement sur les moteurs de recherche par le biais d'une promotion SEO (Search Engine Optimization [86]). Le SEO correspond à ce que l'on appelle le « *référencement naturel* », c'est-à-dire l'ensemble des manipulations reconnues pouvant aider à ce qu'un site soit plus visible sur un moteur de recherche. Lorsque l'on fait référence à ce terme, il s'agit essentiellement de manipulations qui sont autorisées. Pour figurer sur Google, un site doit par exemple se référer aux *Essentiels de la recherche* [87], qui forment les principes fondamentaux nécessaires à l'apparition des contenus sur le moteur.

Parmi ces essentiels, il y a premièrement des exigences techniques, ainsi que des règles concernant le spam. Ces dernières visent à lutter contre certaines méthodes abusives, qui peuvent également booster le référencement, comme l'emploi massif de textes ou liens cachés [88] (texte blanc sur fond blanc, caché derrière une image, opacité zéro, etc.). L'amélioration du SEO est à l'inverse recommandée, puisque cela renvoie au troisième et dernier principe, qui concerne les bonnes pratiques clés, le but étant de permettre aux moteurs de recherche et aux utilisateurs de trouver plus facilement les sites pertinents.

Pour autant, VIGINUM montre que l'emploi des techniques SEO constitue également un levier important pour l'optimisation du référencement des contenus désinformateurs sur les moteurs de recherche. Effectivement, l'enquête révèle que les différents sites de l'écosystème de désinformation russe « pravda » semblent bénéficier d'une telle optimisation. Concrètement, les manipulations SEO correspondent à l'utilisation de mots-clés stratégiques, ou encore à la création de « liens entrant » ou « backlinks » pour augmenter la crédibilité du site.

[85] Secrétariat général de la défense et de la sécurité nationale. « Portal Kombat : un réseau structuré et coordonné de propagande prorusse », 12 février 2024. lien.
[86] Google Search Central. « Bien débuter en référencement naturel (SEO) : principes de base ». lien.
[87] Google Search Central. « Essentiels de la recherche Google ». lien.
[88] Google Search Central. « Règles concernant le spam dans la Recherche sur le Web Google ». lien.

Les backlinks sont des liens hypertextes émanant de sites web externes et qui renvoient vers des pages précises d'autres sites. Essentiels pour le référencement naturel, ils sont interprétés par les moteurs de recherche comme des votes de confiance, renforçant la visibilité et la crédibilité d'un contenu. Dans le cadre de la désinformation, ils deviennent des outils stratégiques pour amplifier la diffusion de contenus trompeurs. Les acteurs malveillants créent en général des réseaux de sites interconnectés, ou exploitent des plateformes légitimes pour générer ces liens. Cela leur permet alors de manipuler les algorithmes des moteurs de recherche et de donner une apparence de fiabilité à leurs contenus. En multipliant ces liens entrants, ils augmentent les probabilités pour les informations mensongères d'être mieux classées dans les résultats de recherche, atteignant ainsi un public plus large, tout en brouillant la distinction entre vérité et désinformation.

Une autre technique qui mérite toute notre attention est la saturation du référencement. Basée sur un concept assez simple, cette méthode consiste à saturer un espace médiatique, avec des articles ou des posts, dans le but de noyer les contenus indésirables aux yeux de la puissance qui ingère. Ce mode d'action a notamment été documenté par les organismes membres [89] du projet européen CrossOver [90], qui visait à surveiller et analyser les algorithmes des plateformes en ligne pour lutter contre la désinformation. Leur rapport de février 2023 [91] concernant l'influence de la Chine dans le traitement médiatique du Xinjiang sur Google News pour les internautes francophones belges, est à ce titre édifiant. Parmi les parties prenantes de cette investigation se trouve CheckFirst, une start-up finlandaise spécialisée dans le développement de logiciels et de méthodes de lutte contre la désinformation. Lors de l'entretien qu'il nous a accordé, son CEO Guillaume Kuster explique que :

A la suite de la publication d'un rapport d'Amnesty International sur les droits humains en Chine et les Ouïghours, la Chine a déployée d'importants moyens pour noyer les contenus francophones traitant du sujet.

En effet, le rapport montre que pour les utilisateurs belges francophones, c'est 13% des sources Google analysées entre le 1er février 2022 et le 1er février 2023, reliées au mot clés « Xinjiang », qui furent produites par des médias contrôlés par le gouvernement chinois.

[89] EU DisinfoLab, the Dutch-language media outlet Apache, the French media education association Savoir Devenir, and the Finnish start-up Check First.
[90] EU DisinfoLab. « Past Project: CrossOver ». lien.
[91] CheckFirst. « Are State-Controlled Chinese sources trying to dominate Xinjiang coverage on Google News? », 22 février 2023. lien.

Sur la période, 209 organismes ont également couvert ce sujet sur Google News. Or sur cet ensemble, les six plus gros médias sous contrôle chinois ont été auteurs à eux seuls de 27% des articles francophones sur le Xinjiang. Le contenu de ces articles était lui consacré à des aspects dénués de lien avec la question des droits humains, comme le tourisme ou l'agriculture. Cet exemple témoigne de la capacité de diffusion massive dont disposent certaines puissances comme la Chine, et donc du risque associé quant au référencement du contenu, avec une possibilité de dilution des contenus européens fiables au milieu des vagues de désinformation étrangères.

c. L'achat d'espace publicitaire

L'achat d'espace publicitaire est parfois une composante des campagnes de désinformation, permettant d'amplifier leur portée et de cibler des audiences spécifiques de manière précise. Cette méthode exploite les outils marketing mis à disposition par les plateformes numériques pour maximiser l'exposition des contenus manipulatoires.

Ceux qui désinforment identifient des segments de population selon des critères tels que l'âge, la localisation, les centres d'intérêt ou les comportements en ligne. Ces publicités sont intégrées dans le flux des utilisateurs, rendant leur caractère manipulatoire difficile à détecter.
Par exemple, pour attiser les tensions autour du sujet israelo-palestinien, des campagnes de désinformation pour le compte de la Russian Internet Agency, la société de désinformation liée à Wagner, a dépensé près de 35 000€ de publicité pour rendre leurs contenus plus visibles, incluant des achats de likes et d'abonnés. Ici, pour dissimuler leur origine, les campagnes publicitaires recourent souvent à des comptes fictifs ou des entreprises-écrans [92].

Le Règlement pour la transparence et le ciblage des publicités politiques, adopté en 2024, s'inscrit dans la stratégie globale et normative de l'Union européenne de lutte contre la désinformation et les ingérences étrangères. Le règlement exige que la publicité à caractère politique soit clairement étiquetée, permettant aux citoyens de voir pourquoi ils ont été ciblés, qui a parrainé la publicité, combien cela a coûté et à quelles élections ou référendums elle se rapporte. Le parrainage de publicités provenant de l'extérieur de l'UE est interdit pendant la période de trois mois précédant les élections. En réaction, Google a choisi d'interdire la publicité politique en Europe sur ses plateformes, estimant le règlement européen trop compliqué à appliquer [94].

[92] Leloup, Damien. « Graffitis d'étoiles de David : des liens établis avec d'autres opérations d'ingérence en Europe ». Le Monde, 15 août 2024. lien.
[93] Parlement européen. « L'essentiel de la plénière 26-29 février 2024 - Session plénière Strasbourg », 22 février 2024. lien.
[94] Le Monde. « Google va cesser de diffuser des publicités politiques dans l'ensemble de l'Union européenne ». 15 novembre 2024. lien.

Il est également à noter que la désinformation est aussi un business lucratif. D'après une étude de NewsGuard et Comscore, la désinformation représente 2,6 milliards de dollars de revenus publicitaires estimés versés aux diffuseurs chaque année par les annonceurs [95].

En conclusion, l'automatisation joue un rôle central dans la propagation à grande échelle de la désinformation. Il est possible de créer, publier et partager des contenus faux ou trompeurs à une vitesse et à une ampleur qui seraient impossibles à atteindre manuellement.

3. LES MÉTHODES DE DÉSINFORMATION CROISÉES

Au-delà d'une désinformation que l'on pourrait considérer comme « classique », où les fausses informations relayées vont servir à promouvoir une vision méliorative de la puissance qui ingère, une nouvelle tendance se développe. En effet, si ce type de désinformation est toujours pratiqué, nous remarquons qu'il s'agit de plus en plus pour les puissances étrangères de déstabiliser en profondeur les sociétés visées, plutôt que d'y inséminer leurs idéologies. Vincent Couronne, fondateur du média de fact checking Les Surligneurs, nous parlait ainsi d'un « *phénomène nouveau* » apparu il y a quelques années. Ce dernier se caractérise par une moindre place accordée aux sujets pro-russe ou pro-chinois par exemple, pour privilégier des narratifs visant à exacerber des fractures déjà existantes au sein des sociétés européennes.

Pour cette désinformation qui vise à accentuer les clivages internes, les canaux de diffusion tels que les intermédiaires d'influence ou les réseaux numériques sont bien sûr mobilisés. Toutefois, il existe également d'autres modes opératoires, qui sont particulièrement prisés et efficaces pour relayer ce type de désinformation. Effectivement, un nouveau champ de techniques, consistant à combiner des méthodes de désinformation classiques avec des pratiques issues d'autres domaines d'action, semble en plein essor. Nous explorerons ici les spécificités de ces techniques contemporaines, que nous définirons comme « techniques de désinformation croisées ».

[95] NewsGuard, et ComScore. « Advertising on Misinformation », 23 août 2021. lien.

Qu'entendons-nous donc par techniques de désinformation croisées et pourquoi les définir ainsi ? Au cours de nos recherches, il est apparu essentiel d'accorder une place à ce type de techniques dans le rapport. De fait, elles étaient mentionnées de manière récurrente comme élément important de la désinformation contemporaine, que ce soit au travers des rapports institutionnels sur la désinformation, par des médias de fact-checking ou des personnalités politiques. Bien que systématiquement évoquées comme des méthodes bien particulières, ces techniques ne faisaient pas l'objet d'une définition spécifique dans les différentes sources consultées. Et pour cause, il est assez difficile de les classer dans les catégories de désinformation déjà existantes.

En quelque sorte à la croisée des chemins entre divers domaines d'action, ces techniques reposent sur la « *création d'évènements qui n'existent pas* » [96], qui vont venir servir d'appuis au développement d'un narratif ensuite relayé sur les canaux précédemment évoqués. Concrètement, cela signifie que :

Avant de diffuser sa fausse information, la puissance étrangère va orchestrer la réalisation d'une action tangible pour les sociétés européennes, qui va constituer une sorte de preuve pour les discours qui vont être émis.

Cela s'appuie dans plusieurs cas sur une action de terrain, comme avec les graffitis d'étoiles de David à Paris en novembre 2023 [97], orchestrés par un réseau de désinformation russe, en vue de pousser un narratif de montée de l'antisémitisme en France. Cette illusion d'événements réels offre aux désinformateurs la capacité à susciter de plus fortes émotions chez le public cible, qui va être témoin sur le terrain d'une réalisation concrète de ce qu'il peut lire en ligne, le poussant à valider la fausse information.

Avec ces techniques croisées, il y a donc toujours une action qui vient s'ajouter à la diffusion de la désinformation. Nous avons remarqué que cette action pouvait prendre diverses formes, en s'appuyant sur différents domaines et registres. Nous avons identifié trois domaines d'action en particulier, dont les méthodes sont parfois empruntées, puis croisées avec une diffusion plus classique. Ainsi, nous nous focaliserons tout d'abord sur l'utilisation de moyens d'action issus du répertoire de l'action collective ; pour ensuite aborder l'amplification et le détournement d'évènements directement sur les réseaux en ligne ; et enfin analyser l'emploi de méthodes étant initialement associées au lobbying.

[96] Citation de Laurent Esquenet, lors de l'entretien réalisé par notre équipe le 18 octobre 2024
[97] Maxime Tellier. « Derrière les tags d'étoiles de David à Paris, un vaste réseau de désinformation russe ». *Franceinfo*, 26 janvier 2024. lien.

a. L'utilisation des moyens d'action issus du répertoire de l'action collective

Le concept de répertoire de l'action collective, développé par l'historien et sociologue Charles Tilly en 1984, renvoie au « *stock limité de moyens d'action à la disposition des groupes contestataires, à chaque époque et dans chaque lieu* » [98]. Ces moyens d'action sont utilisés par les acteurs contestataires, afin de faire retentir leurs mouvements sociaux et de se faire entendre. L'utilisation de ces méthodes peut constituer un levier particulièrement puissant dans la légitimation de fausses informations. En effet, étant habituellement mobilisés par les différents acteurs de la société civile pour appuyer leurs revendications, de telles actions orchestrées par une puissance qui opère une ingérance peuvent alors passer pour des opérations de groupes militants.

C'est notamment ce qu'il s'est passé à Paris en octobre 2023, avec les graffitis d'Etoiles de David. Le 30 octobre, dans un contexte de tensions faisant suite à l'attaque du Hamas en Israël le 7 octobre et à la réponse du gouvernement israélien à Gaza, une soixantaine d'Etoiles de David ont été taguées au pochoir dans le 14ème arrondissement de Paris. Cette information est immédiatement reprise et relayée par l'ensemble des médias français, de médias israéliens et internationaux. Dans les lignes du journal The Times of Israël, on peut alors lire le témoignage du Président de l'Union des Etudiants Juifs de France, Samuel Lejoyeux : « Cet acte de marquage rappelle les procédés des années 30 et la Seconde Guerre mondiale qui ont conduit à l'extermination de millions de juifs » [99]. Le Parquet de Paris ouvre une instruction dès le 31 octobre, et les responsables politiques commentent les faits. La Première ministre de l'époque, Elisabeth Borne, réagit avec les mots suivants : « *Au nom du gouvernement, je condamne avec une fermeté absolue ces agissements ignobles […] s'en prendre à quelqu'un parce qu'il est juif, […] c'est s'en prendre à l'âme même de la République* » [100].

Il y a donc un très fort retentissement médiatique et institutionnel, avec l'identification initiale de ces graffitis comme des actes antisémites, émanant supposément d'individus ou de groupes contestataires locaux. Cette première analyse n'est pas étonnante, puisque taguer des symboles ou slogans est un moyen d'action régulièrement employé dans les mouvements sociaux contestataires quels qu'ils soient [101]. Le 6 novembre, une semaine après l'événement, VIGINUM annonce qu'il s'agit finalement d'un acte d'ingérence russe. Grâce à son enquête, le service met en lumière le lien entre les graffitis et le dispositif russe RRN (Recent Reliable News).

[98] Cécile Péchu. « Répertoire d'action ». *Dictionnaire des mouvements sociaux*, 2009. lien.
[99] The Times of Israel, « Stars of David Spray-Painted on Buildings in Paris, Heightening Fears among Jews ». 31 octobre 2023. lien.
[100] Le Monde. « Des étoiles de David taguées en Ile-de-France : enquête ouverte, Elisabeth Borne dénonce des « agissements ignobles » ». 31 octobre 2023. lien
[101] Anny Bloch-Raymond. « Tags, graffs et fresques murales : revendications identitaires, expressions communautaires ? (San Francisco Strasbourg) »., *Agora débats/jeunesses*. lien.

En effet, les experts retracent la diffusion de 2589 posts polémiques sur les graffitis, par un réseau de 1095 bots associés à l'opération de désinformation RRN [102]. Un des éléments les plus édifiants du lien entre cette action et l'ingérence russe est la primo-diffusion de certains de ces posts, près de 48h avant la première publication authentique des tags. De son côté, le Tribunal judiciaire de Paris annonce dans son communiqué de presse avoir identifié un couple auteur des faits, ayant déjà quitté la France. L'analyse de leurs conversations téléphoniques, ainsi que celle d'un autre couple de moldave ayant agi de manière similaire quelques jours auparavant, permet de penser que ces deux couples auraient agi sous la commande d'une même tierce personne [103]. La suite des investigations établira la responsabilité d'Anatoli Prizenko, un homme d'affaires moldave connu pour son engagement pro-russe, et qui reconnaît son implication [104].

Un événement de terrain, assimilable à une action collective authentique, peut donc décupler la force d'impact de la désinformation.

Ici, cet événement a profondément touché la population française, bien que le démasquage de l'opération d'ingérence n'ait pris qu'une semaine. Si le cas des Etoiles de David à Paris demeure à ce jour le plus emblématique de cette méthode émergente, les acteurs de lutte contre la désinformation ont pu identifier d'autres cas en Europe.

A ce titre, l'ONG EU DisinfoLab parle de « potentielles opérations hybrides » comme tactiques employées dans la campagne de désinformation russe Doppelgänger, à laquelle se rattache l'opération RRN [105]. EU DisinfoLab renvoie alors vers Meta, qui identifie plusieurs cas assimilables aux méthodes de désinformation croisées. Effectivement, son Rapport sur les menaces adverses du deuxième trimestre 2024 [106] met en lumière l'implication d'un réseau russe lié à la diffusion de posts sur les Etoiles de David dans d'autres opérations. Bien que la plupart d'entre elles sont plutôt à ranger dans la catégorie de l'amplification et du détournement d'événements réels, que nous allons voir ensuite, sont également citées certaines techniques relevant du répertoire de l'action collective, comme l'organisation et l'incitation en ligne à des manifestations physiques contre le soutien à l'Ukraine en Allemagne, France ou Pologne. Lors de ces manifestations sont également distribués des flyers, permettant d'accéder aux boucles Telegram de ces opérations. Le répertoire de l'action collective constitue ainsi une nouvelle ressource pour les désinformateurs, avec un large panel de moyens d'action dans lequel ils peuvent se servir.

[102] Représentation Permanente de la France auprès de l'OSCE. « Russie - Nouvelle ingérence numérique russe contre la France », 9 novembre 2023. lien.
[103] Parquet du Tribunal Judiciaire de Paris. « Communiqué de presse de la procureure de la République », 7 novembre 2023. lien.
[104] Jacques Pezet et Elsa de La Roche Saint-André. « Anatoli Prizenko, commanditaire présumé des étoiles de David taguées dans Paris, prétend que l'action visait à «soutenir» les Juifs ». *Libération*, 8 novembre 2023. lien.
[105] EU DisinfoLab. « What Is the Doppelganger Operation? List of Resources », 30 octobre 2024. lien.
[106] Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, et Mike Dvilyanski. *Adversarial Threat Report*, 2024. lien.

b. L'amplification et le détournement en ligne d'évènements réels

Il s'agissait ici de la forme la plus représentative et la plus palpable de la désinformation croisée, avec la création d'actions de terrain qui vont susciter des émotions et des réactions intenses au sein des sociétés européennes.

Toutefois, l'appui de la désinformation sur un acte tangible n'implique pas forcément que ce dernier ait été orchestré par la puissance qui s'ingère, ni même nécessairement qu'il soit de terrain. Pour revenir à la citation de Laurent Esquenet, il parle d'un nouveau type de désinformation qui s'appuie sur « la création d'évènements qui n'existent pas ». Or, s'il cite les Etoiles de David en exemple, il évoque également l'affaire des punaises de lit à Paris en septembre 2023. On pourrait alors se dire qu'il ne s'agit pas de création ici, puisqu'il y avait effectivement des problèmes de punaises de lit à Paris. Toutefois, on a pu remarquer par la suite que la panique médiatique avait été largement disproportionnée vis-à-vis de la situation réelle. En cause, une polémique « artificiellement amplifiée » par la Russie sur les réseaux sociaux, comme l'expliquait le ministre français délégué à l'Europe du moment, Jean-Noël Barrot [107].

L'amplification et le détournement d'événements existants peut constituer un problème distinct, puisqu'un phénomène authentique va servir de base à la construction d'un édifice mensonger tout autour. Nous pouvons alors considérer qu'il s'agit là aussi, de manière différente, de créer quelque chose qui n'existe pas, en donnant à l'événement initial une ampleur complètement déconnectée de sa réalité. Il s'agit d'une autre manière de croiser la désinformation avec le réel, qui ne nécessite cette fois-ci pas forcément d'engager de moyens d'action sur le terrain, le phénomène étant déjà existant. L'enjeu pour les désinformateurs est alors de l'exploiter à profit.

L'amplification en ligne d'événements réels ou tangibles pour les populations européennes est précisément la forme de désinformation croisée à laquelle on peut assimiler les cas soulignés par Meta dans le Rapport Q2 2024 [108]. Ces rapports trimestriels sur les méthodes adverses ont un but bien précis, identifier des « Coordinated Inauthentic Behavior (CIB) » et les réseaux qui y sont liés. En tant que géant du web et gestionnaire de plateformes en ligne, la multinationale se concentre sur l'aspect numérique de la désinformation. Nous pouvons justement reprendre un exemple qui se passe entièrement en ligne, mais qui simule l'expression d'une partie de la population moldave.

[107] Le Figaro. « France: la psychose des punaises de lit a été «amplifiée» par Moscou, affirme le ministre délégué à l'Europe ». 1 mars 2024. lien
[108] Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, et Mike Dvilyanski. Adversarial Threat Report, 2024. lien.

Meta nous apprend ainsi que le troisième réseau CIB russe identifié dans le rapport Q2 2024 a promu une pétition pour l'abolition du vote par correspondance en Moldavie, dont on ne sait pas vraiment si elle est indépendante ou non. Cette pétition d'apparence authentique et présente sur la plateforme en ligne openPetition est relayée par les comptes de ce réseau, qui diffusent également des posts pro-russes ou des critiques du gouvernement moldave. Bien qu'entièrement numérique, la pétition constitue tout de même un élément concret, qui vient renforcer le narratif pro-russe déjà poussé par les leviers plus classiques de désinformation, tels les posts cités à l'instant. A travers cet exemple assez spécifique, nous nous rendons compte que le phénomène associé n'a pas forcément besoin d'être physique, mais doit toutefois renvoyer à une action tangible et créatrice d'effets dans la société, comme c'est le cas avec la pétition.

Dans ce rapport, Meta fait à plusieurs reprises le lien entre ce qui est publié sur Facebook ou Instagram et des évènements réels. On se retrouve alors dans une configuration plus similaire à celle concernant l'affaire des punaises de lit. Le troisième réseau CIB suscite de nouveau notre intérêt, puisque c'est aussi celui-ci qui se trouve derrière les manifestations contre le soutien à l'Ukraine déjà évoquées. En effet, le réseau est à l'origine d'actions de terrain, puisque certaines pages ou groupes en ligne associés, qui se présentent de façon mensongère comme des soutiens aux ukrainiens, revendiquent l'organisation de certaines manifestations qui visent en réalité à développer une opinion contre l'aide à l'Ukraine. Ce fut notamment le cas du groupe Telegram « Ukrainian European Front », qui avait créé une page Facebook directement repérée et supprimée par les services de Meta. L'implication russe dans les manifestations en physique a également été mise en avant par les services d'investigation du journal Le Monde [109].

Mais au-delà des manifestations dans l'espace public, qui relève plutôt du répertoire de l'action collective, il est intéressant de remarquer que l'amplification des événements réels en ligne est un élément central dans le mode d'action de ce réseau. Le rapport de Meta met l'accent sur ce point, puisque les actes de terrain (manifestations, stickers, graffitis, etc.) sont ensuite repris sur les différents réseaux sociaux avec des photos ou vidéos, ainsi que sur des « pages d'informations », qui tâchent de faire croire à des manifestations authentiques. A noter que la vision amplificatrice constitue une sorte de matrice, dont s'imprègne l'action réelle. Dans l'exemple soulevé par *Le Monde*, à Paris, les auteurs, qui ne sont que trois, se fondent dans une manifestation concernant la réforme des retraites, détournant alors une manifestation réelle afin de créer une illusion de masse et d'augmenter l'impact des images relayées.

[109] Thomas Eydoux et Margaux Farran. « How Russia Is Staging Fake Protests in Europe to Discredit Ukraine ». Le Monde, 7 mai 2023. lien

Ainsi, si l'on peut établir une distinction entre désinformation croisée se référant au répertoire de l'action collective et désinformation croisée via l'amplification d'évènements réels qui ne sont pas nécessairement créés par la puissance qui s'ingère, ce dernier exemple nous montre que ces deux formes de désinformation peuvent être combinées dans le but de maximiser l'impact.

c. La désinformation croisée en déploiement vers d'autres champs d'activités, tels que le lobbying

Suite à cette analyse de la désinformation croisée et des manières dont elle se manifeste la plupart du temps, il apparaît clairement qu'elle repose systématiquement sur la création de quelque chose qui n'existe pas. Si les formes et techniques peuvent différer, un point commun à tous les cas étudiés est la mise en œuvre d'une illusion de réel à travers des évènements tangibles, qu'ils soient orchestrés, amplifiés ou détournés par les désinformateurs. Ce fil directeur semble particulièrement bien fonctionner avec les phénomènes de terrain, qui touchent plus directement les sociétés. Toutefois, bien que les exemples renvoient souvent à des actes issus du répertoire de l'action collective, à l'amplification en ligne de phénomènes réels, ou aux deux en même temps, ce type de désinformation s'étend également à d'autres domaines d'activités.

Nous remarquons ainsi que de récentes techniques de désinformation vont venir piocher dans le répertoire d'action du lobbying. Dans son rapport INGE 2 [110], la Commission spéciale du Parlement européen sur l'ingérence étrangère et la désinformation cite certains risques d'ingérence liés au manque de réglementation des activités de lobbying. En revanche, il n'est pas question dans le rapport de l'appropriation de certaines techniques de lobbying par les désinformateurs de pays tiers. Or, ces croisements se développent. C'est ce que mettent en avant les journalistes d'investigation de Forbidden Stories dans l'enquête « Story Killers » sur la désinformation. A travers l'étude des techniques contemporaines employées par l'officine de désinformation israélienne Team Jorge, ils soulignent la proposition par l'agence de créer des ONG afin de servir de relais aux idées à diffuser. Dans un podcast France Inter [112], Frédéric Métézeau, journaliste Radio France infiltré pendant l'enquête, revient sur cette proposition, nous décrivant une situation que l'on peut sans aucun doute identifier comme de l'astroturfing.

[110] 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.
[111] France Inter, « Story Killers, la dernière enquête de Forbidden Stories ». 16 février 2023. lien.

Cette technique de désinformation et d'influence doit son nom au sénateur Lloyd Bentsen, qui la définit en 1985 par « l'astroturf » (gazon synthétique), en opposition au terme « grass-roots » qui renvoie à des mouvements de base citoyenne. Elle vise à créer de toute pièce quelque chose de réel (une association, un mouvement, etc.), qui va servir à relayer des idées dans le but d'influencer un public [112]. Cela rejoint en tout point le fil directeur des cas de désinformation croisée étudiés jusqu'ici. Cette méthode n'est pas nouvelle, puisqu'elle est définie dès 1985. Pour autant, c'est une technique habituellement associée à l'activité des lobbies industriels. Il est donc intéressant de voir que certaines agences de désinformation aux ressources conséquentes, telles que la Team Jorge, se mettent à reprendre des méthodes de lobbying dans leur catalogue de techniques.

En somme, il apparaît que l'ensemble des méthodes croisées forme dans sa globalité un type de désinformation émergent et récent, qui tend à se développer davantage.

Si les cas les plus emblématiques de désinformation croisée sont caractérisés par une action de terrain assortie d'une amplification en ligne, il ne faut pas mettre de côté le déploiement vers d'autres secteurs actuellement à l'œuvre.

La reprise de l'astroturfing dans des campagnes de désinformation en est un bon exemple, qui invite les acteurs de lutte à rester vigilant quant à la possibilité d'investissement de nouveaux domaines d'activités par les désinformateurs. La désinformation croisée constitue aujourd'hui un élément fondamental des stratégies d'ingérence hybrides des Etats tiers, qui peut même venir se confondre dans des cas extrêmes avec l'action directe d'un gouvernement. C'est ainsi ce que relève la commission spéciale INGE 2 dans son rapport au sujet des migrants déplacés à la frontière polonaise par les autorités biélorusses. Au-delà de l'ingérence physique, le rapport met en avant l'aspect de désinformation, avec un flux migratoire alimenté par la Biélorussie visant entre autres à exploiter le sujet majeur de division qu'est la migration au sein de l'Union européenne [113].

Il convient donc d'accorder une attention toute particulière à ce type de désinformation en plein développement, qui se manifeste sous diverses formes et qui présente un risque considérable de déstabilisation et de renforcement des clivages au sein des sociétés européennes.

[112] France Inter « L'astroturfing, la grande illusion de l'opinion », 25 janvier 2024. lien.
[113] ibid.

CONFRONTATIONS EUROPE

Sciences Po Strasbourg
École
de l'Université de Strasbourg

DOSSIER SPÉCIAL DÉSINFORMATION
& INGÉRENCE ÉTRANGÈRE

LA LUTTE CONTRE LA DÉSINFORMATION

ACTEURS ET TECHNIQUES

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 affutée. 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 XXIème 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'expliciter 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 évènements, 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 terreaux 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 reconnaitre 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 numériques 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 des 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'approprier 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 Télégram.

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.

BIBLIOGRAPHIE

Articles et ouvrages académiques :

Armitage, Rachel, et Cristian Vaccari. « Misinformation and disinformation ». In *The Routledge Companion to Media Disinformation and Populism*, 2021.

Beauvais, Catherine. « Fake news: Why do we believe it? » *Joint Bone Spine*, 1 juillet 2022. https://doi.org/10.1016/j.jbspin.2022.105371

Bloch-Raymond, Anny. « Tags, graffs et fresques murales : revendications identitaires, expressions communautaires ? (San Francisco Strasbourg) ». In *Agora débats/jeunesses*. Vol. 29, 2002. https://www.persee.fr/doc/agora_1268-5666_2002_num_29_1_2021

Boyer, Isabelle, et Luciana Radut-Gaghi. « Des stéréotypes à l'ère des fake news ». *Communication. Information médias théories pratiques*, 11 octobre 2021. https://doi.org/10.4000/communication.14378

Brennen, J. Scott, Felix M. Simon, et Rasmus Kleis Nielsen. « Beyond (Mis)Representation: Visuals in COVID-19 Misinformation ». *The International Journal of Press/Politics*, janvier 2021. https://journals.sagepub.com/doi/10.1177/1940161220964780

Charon, Paul, et Jean-Baptiste Jeangène Vilmer. *Les opérations d'influences chinoises - Un moment machiavélien*. Editions Des Equateurs, 2024.

Dan, Viorela, Britt Paris, Joan Donovan, Michael Hameleers, Jon Roozenbeek, Sander van der Linden, et Christian von Sikorski. « Visual Mis- and Disinformation, Social Media, and Democracy ». *Journalism & Mass Communication Quarterly*, 25 août 2021. https://doi.org/10.1177/10776990211035395

Dowling, Melissa-Ellen. « Democracy under siege: foreign interference in a digital era ». *Australian Journal of International Affairs* Vol 75, 30 mars 2021.

Gaillard, Stefan, Zoril A. Oláh, Stephan Venmans, et Michael Burke. « Countering the Cognitive, Linguistic, and Psychological Underpinnings Behind Susceptibility to Fake News: A Review of Current Literature With Special Focus on the Role of Age and Digital Literacy ». *Frontiers in Communication*, 2021. https://doi.org/10.3389/fcomm.2021.661801

Gregory, Sam. « Deepfakes, Misinformation and Disinformation and Authenticity Infrastructure Responses: Impacts on Frontline Witnessing, Distant Witnessing, and Civic Journalism ». *Journalism 23*, no 3 (1 mars 2022): 708-29. https://doi.org/10.1177/14648849211060644

Hameleers, Michael, Thomas E. Powell, Toni G.L.A. Van Der Meer, et Lieke Bos. « A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media ». *Political Communication*, 3 mars 2020. https://doi.org/10.1080/10584609.2019.1674979

Lemaire, Marine, Mathieu Cassotti, et Grégoire Borst. « Development of fake detection during adolescence ». septembre 2022. https://hal.science/hal-03769028

Limonier, Kévin, et Maxime Audinet. « De l'enquête au terrain numérique : les apports de l'Osint à l'étude des phénomènes géopolitiques ». *Hérodote 186*, no 3 (11 octobre 2022): 5-17. https://doi.org/10.3917/her.186.0005

Liv, Nadine, et Dov Greenbaum. « Deep Fakes and Memory Malleability: False Memories in the Service of Fake News ». *AJOB Neuroscience*, 2 avril 2020. https://doi.org/10.1080/21507740.2020.1740351.

Low, Jwen Fai, Benjamin C. M. Fung, Farkhund Iqbal, et Shih-Chia Huang. « Distinguishing between fake news and satire with transformers ». *Expert Systems with Applications*, 1 janvier 2022. https://doi.org/10.1016/j.eswa.2021.115824.

Messaris, Paul, et Linus Abraham. « The Role of Images in Framing News Stories ». In *Framing public life: Perspectives on media and our understanding of the social world*. Routledge, 2001. https://www.taylorfrancis.com/books/edit/10.4324/9781410605689/framing-public-life-stephen-reese-oscar-gandy-jr-august-grant.

Morgan, Susan. « Fake news, disinformation, manipulation and online tactics to undermine democracy ». *Journal of Cyber Policy* 3, no 1 (2 janvier 2018): 39-43. https://doi.org/10.1080/23738871.2018.1462395.

Péchu, Cécile. « Répertoire d'action ». In *Dictionnaire des mouvements sociaux*, 454-62. Presses de Sciences Po, 2009. https://doi.org/10.3917/scpo.filli.2009.01.0454.

Pennycook, Gordon, et David G. Rand. « The Psychology of Fake News ». *Trends in Cognitive Sciences*, 1 mai 2021. https://doi.org/10.1016/j.tics.2021.02.007.

Rossetti, Michael, et Tauhid Zaman. « Bots, disinformation, and the first impeachment of U.S. President Donald Trump ». *PLOS ONE*, 8 mai 2023. https://doi.org/10.1371/journal.pone.0283971.

Tumber, Howard, et Silvio Waisbord. The Routledge Companion to Media Disinformation and Populism - 1st Edi, 2021. https://www.routledge.com/The-Routledge-Companion-to-Media-Disinformation-and-Populism/Tumber-Waisbord/p/book/9780367704919?srsltid=AfmBOor2ZdQlmiRdxYBAE5vPmLb9kV-NBJS-TY5zo03NNP1ObBV18a2n.

Varol, Onur, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, et Alessandro Flammini. « Online Human-Bot Interactions: Detection, Estimation, and Characterization », 27 mars 2017. https://doi.org/10.48550/arXiv.1703.03107

Wylie, Christopher. *Mindfuck : le complot Cambridge Analytica pour s'emparer de nos cerveaux*, 2020. https://www.librairie-sciencespo.fr/livre/9782246824732-mindfuck-le-complot-cambridge-analytica-pour-s-emparer-de-nos-cerveaux-christopher-wylie/.

Zillmann, Dolf, Silvia Knobloch, et Hong-sik Yu. « Effects of photographs on the selective reading of news reports ». *Media Psychology*, 2001. https://doi.org/10.1207/S1532785XMEP0304_01.

Articles de presse :

Albert, Eric. « Le Royaume-Uni interdit l'acquisition de journaux par des Etats étrangers ». *Le Monde*, 15 mars 2024. https://www.lemonde.fr/economie/article/2024/03/15/le-royaume-uni-interdit-l-acquisition-de-journaux-par-des-etats-etrangers_6222219_3234.html

André, Jérémy. « Désinformation : « La Chine recrute aussi des influenceurs étrangers » ». *Le Point*, 17 février 2024. https://www.lepoint.fr/monde/chine-desinformation-manipulations-et-agents-d-influence-sur-les-reseaux-sociaux-17-02-2024-2552704_24.php

Audureau, William, 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. https://www.lemonde.fr/les-decodeurs/article/2023/10/27/un-an-de-desinformation-et-d-errements-strategiques-d-elon-musk-sur-x-anciennement-twitter-en-quarante-dates-cles_6196856_4355770.html

Condomines, Anaïs. « Ingérences étrangères : que risque Rachid M'Barki, accusé d'avoir menti devant la commission d'enquête parlementaire ? » *Libération*, 20 janvier 2024, sect. CheckNews. https://www.liberation.fr/checknews/ingerences-etrangeres-que-risque-rachid-mbarki-accuse-davoir-menti-devant-la-commission-denquete-parlementaire-20240120_3ZSRI7MQNBHHRLO27QJKILGZME/

Courrier international. « Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée ». 26 mai 2021. https://www.courrierinternational.com/revue-de-presse/vu-de-letranger-des-influenceurs-francais-approches-pour-denigrer-le-vaccin-pfizer

Eydoux, Thomas, et Margaux Farran. « How Russia Is Staging Fake Protests in Europe to Discredit Ukraine ». *Le Monde*, 7 mai 2023. https://www.lemonde.fr/en/international/article/2023/05/07/how-russia-is-staging-fake-protests-in-europe-to-discredit-ukraine_6025808_4.html

Feng, Isabelle. « Derrière TikTok se profile l'ombre du Parti communiste chinois ». *Le Monde*, 14 avril 2023. https://www.lemonde.fr/idees/article/2023/04/14/derriere-tiktok-se-profile-l-ombre-du-parti-communiste-chinois_6169514_3232.html

Franceinfo. « Guerre en Ukraine : ce que l'on sait de l'opération de désinformation russe "Doppelgänger" qui a visé la France ». 14 juin 2023. https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-ce-que-l-on-sait-de-l-operation-de-desinformation-russe-doppelganger-qui-a-vise-la-france_5887325.html

Geoffroy, Romain, et Maxime Vaudano. « Quels sont les liens de Marine Le Pen avec la Russie de Vladimir Poutine ? » *Le Monde*, 20 avril 2022. https://www.lemonde.fr/les-decodeurs/article/2022/04/20/quels-sont-les-liens-de-marine-le-pen-avec-la-russie-de-vladimir-poutine_6122903_4355770.html

Lagodinsky, Serguey. « The State of Media Freedom in Europe, Challenges and Protections ». *Euractiv*, 30 novembre 2024, sect. Politics. https://www.euractiv.com/section/politics/special_report/the-state-of-media-freedom-in-europe-challenges-and-protections/

Le Figaro. « France: la psychose des punaises de lit a été «amplifiée» par Moscou, affirme le ministre délégué à l'Europe ». 1 mars 2024, sect. Société. https://www.lefigaro.fr/actualite-france/france-la-psychose-des-punaises-de-lit-a-ete-amplifiee-par-moscou-affirme-le-ministre-delegue-a-l-europe-20240301

Le Monde. « Des étoiles de David taguées en Ile-de-France : enquête ouverte, Elisabeth Borne dénonce des « agissements ignobles » ». 31 octobre 2023. https://www.lemonde.fr/societe/article/2023/10/31/le-parquet-de-paris-ouvre-une-enquete-apres-la-decouverte-d-etoiles-de-david-taguees-sur-des-immeubles_6197523_3224.html

Le Monde. « Google va cesser de diffuser des publicités politiques dans l'ensemble de l'Union européenne ». 15 novembre 2024. https://www.lemonde.fr/pixels/article/2024/11/15/google-va-cesser-de-diffuser-des-publicites-politiques-dans-l-ensemble-de-l-union-europeenne_6394931_4408996.html

Ledroit, Valentin. « Qatargate : tout comprendre au scandale de corruption qui touche le Parlement européen ». Touteleurope.eu, 3 octobre 2023. https://www.touteleurope.eu/institutions/qatargate-tout-comprendre-au-scandale-de-corruption-qui-touche-le-parlement-europeen/

Leffief, Jean-Philippe. « « Qatargate » : ce que l'on sait des soupçons de corruption au Parlement européen ». *Le Monde*, 15 décembre 2022. https://www.lemonde.fr/international/article/2022/12/15/qatargate-ce-que-l-on-sait-des-soupcons-de-corruption-au-parlement-europeen_6154482_3210.html

Leloup, Damien. « Graffitis d'étoiles de David : des liens établis avec d'autres opérations d'ingérence en Europe ». *Le Monde*, 15 août 2024. https://www.lemonde.fr/pixels/article/2024/08/15/graffitis-d-etoiles-de-david-des-liens-etablis-avec-d-autres-operations-d-ingerence-en-europe_6282321_4408996.html

L'Express. « Désinformation : quelles conséquences après la suppression de CrowdTangle par Meta ? » 2 avril 2024, sect. Tech et transformations. https://www.lexpress.fr/economie/high-tech/desinformation-quelles-consequences-apres-la-suppression-de-crowdtangle-par-meta-N7FLRMMQ3NHCNJGWR4P5E27OWI/

Ouest France. « Soupçons d'ingérence à BFMTV. « J'étais manipulé » : Rachid M'Barki aurait reconnu avoir été payé ». 19 janvier 2024, sect. BFMTV. https://www.ouest-france.fr/medias/bfmtv/soupcons-dingerence-a-bfmtv-jetais-manipule-rachid-mbarki-aurait-reconnu-avoir-ete-paye-908cb26a-b6c4-11ee-95de-219f489f3c47.

Pezet, Jacques, et Elsa de La Roche Saint-André. « Anatoli Prizenko, commanditaire présumé des étoiles de David taguées dans Paris, prétend que l'action visait à «soutenir» les Juifs ». *Libération*, 8 novembre 2023, sect. CheckNews. https://www.liberation.fr/checknews/anatoli-prizenko-commanditaire-presume-des-etoiles-de-david-dans-paris-pretend-que-laction-visait-a-soutenir-les-juifs-20231108_UXKBHMT4WBBFDPSRGBW5BBRSDM/.

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. https://www.lindependant.fr/2024/12/07/presidentielle-annulee-en-roumanie-des-centaines-de-milliers-de-faux-comptes-des-millions-de-faux-abonnes-85000-cyberattaques-usage-intensif-de-lia-12376458.php.

Starcevic, Seb. « Russian bots boosted NATO critic ahead of Croatian election, researchers say ». *POLITICO*, 9 janvier 2025. https://www.politico.eu/article/russia-bots-nato-croatia-election-presidential-candidate-eu-donald-trump-zoran-milanovic-campaign/.

Tellier, Maxime. « Derrière les tags d'étoiles de David à Paris, un vaste réseau de désinformation russe ». *Franceinfo*, 26 janvier 2024. https://www.francetvinfo.fr/enquetes-franceinfo/enquete-franceinfo-derriere-les-tags-d-etoiles-de-david-a-paris-un-vaste-reseau-de-desinformation-russe_6325623.html.

The Times of Israel, « Stars of David Spray-Painted on Buildings in Paris, Heightening Fears among Jews ». 31 octobre 2023. https://www.timesofisrael.com/stars-of-david-spray-painted-on-buildings-in-paris-continuing-antisemitic-spate/.
Wienand, Von L., S Steurenthaler, et S Loelke. « Putins Troll-Armee greift Deutschland an ». t-online, 30 août 2022. https://www.t-online.de/nachrichten/deutschland/gesellschaft/id_100042596/ukraine-krieg-prorussische-kampagne-das-steckt-hinter-den-fake-artikeln.html.

Zachová, Aneta, Laura Miraglia, Pekka Vanttinen, et Sofia Mandilara. « L'ingérence croissante de la Chine au sein des universités européennes ». *Euractiv*, 1 décembre 2022. https://www.euractiv.fr/section/international/news/lingerence-chinoise-croissante-au-sein-des-universites-europeennes/.

Rapports et sites Internet :

Alaphilippe, Alexandre, Gary Machado, Raquel Miguel, et Francesco Poldi. « Doppelganger - Media Clones Serving Russian Propaganda ». EU Disinfo Lab, 27 septembre 2022. https://www.disinfo.eu/doppelganger/

Andrzejewski, Cécile. « "Team Jorge" : Révélations sur les manipulations d'une officine de désinformation ». Forbidden Stories (blog), 15 février 2023. https://forbiddenstories.org/fr/team-jorge-desinformation/

Caline, Guillaume, et Laurence Vardaxoglou. « Regard des Français sur la lutte contre la désinformation ». Fondation Jean Jaurès, 5 novembre 2024. https://www.jean-jaures.org/publication/regard-des-francais-sur-la-lutte-contre-la-desinformation/

Centre for Information Resilience. « Disinformation campaign uncovered by researchers ahead of Croatian presidential run-off », 8 janvier 2025. https://www.info-res.org/cir/articles/disinformation-campaign-uncovered-by-researchers-ahead-of-croatian-presidential-run-off/

CheckFirst. « Are State-Controlled Chinese sources trying to dominate Xinjiang coverage on Google News? », 22 février 2023. https://checkfirst.network/are-state-controlled-chinese-sources-trying-to-dominate-xinjiang-coverage-on-google-news/

« Comprendre les menaces et les défis - Désinformation visuelle et multimodale (DVM) ». Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa. https://labinfo.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20French%20CRIM%20Report%20Final%20(digital).pdf

« Deny, Deceive, Delay (Vol 3): Climate Information Integrity Ahead of COP28 ». Climate Action Against Disinformation, 29 novembre 2023. https://caad.info/analysis/reports/deny-deceive-delay-vol-3-climate-information-integrity-ahead-of-cop28/

D'Hooghe, Ingrid, Annemarie Montulet, Marijn de Wolff, et Frank N. Pieke. « Assessing Europe-China Collaboration in Higher Education and Research ». Leiden Asia Centre, 2018. https://www.chinazentren.de/2018/08/31/assessing-europe-china-collaboration-in-higher-education-and-research/

EU DisinfoLab. « Past Project: CrossOver ». Consulté le 21 janvier 2025. https://www.disinfo.eu/projects/crossover/

EU DisinfoLab. « What Is the Doppelganger Operation? List of Resources », 30 octobre 2024. https://www.disinfo.eu/doppelganger-operation/

Fakt. « Le biais de confirmation, un vecteur non négligeable vers la désinformation », 10 septembre 2024. https://www.fakt-afrique.org/le-biais-de-confirmation-un-vecteur-non-negligeable-vers-la-desinformation/

Fourreau, Valentine. « Réseaux sociaux : où sont-ils les plus utilisés pour s'informer ? » Statista, 11 mars 2024. https://fr.statista.com/infographie/27039/part-des-internautes-utilisant-les-reseaux-sociaux-comme-source-information/

Franklin, Margarita, Lindsay Hundley, Mike Torrey, David Agranovich, et Mike Dvilyanski. Adversarial Threat Report, 2024. http://archive.org/details/adversarial-threat-report-Meta.

Garrett, R. Kelly, Robert Bond, et Shannon Poulsen. « Too Many People Think Satirical News Is Real ». The Ohio State University, 16 août 2019. https://news.osu.edu/too-many-people-think-satirical-news-is-real/

Garritzmann, Julian. « Higher Education Funding across the Globe ». Education International, 15 mai 2024. https://www.ei-ie.org/en/item/28580:higher-education-funding-across-the-globe

Google Search Central. « Bien débuter en référencement naturel (SEO) : principes de base », s. d. https://developers.google.com/search/docs/fundamentals/seo-starter-guide?hl=fr

Google Search Central. « Essentiels de la recherche Google ». https://developers.google.com/search/docs/essentials?hl=fr

Google Search Central. « Règles concernant le spam dans la Recherche sur le Web Google ». https://developers.google.com/search/docs/essentials/spam-policies?hl=fr

Karásková, Ivana, Tamás Matura, Richard Q. Turcsányi, et Matej Šimalčík. « Central Europe for Sale: The Politics of China's Influence ». Association for International Affairs (AMO), 16 avril 2018. https://www.amo.cz/en/mapinfluence-en/central-europe-sale-politics-chinas-influence-2/

Keast, Jacinta. « Shadow Play: A pro-China and Anti-US Influence Operation Thrives on YouTube ». Australian Strategic Policy Institute, 15 décembre 2023. https://www.aspistrategist.org.au/shadow-play-a-pro-china-and-anti-us-influence-operation-thrives-on-youtube/

« La désinformation peut-elle tuer? » Science-Presse, 29 mars 2023. https://www.sciencepresse.qc.ca/vote-pour-science/2023/03/29/desinformation-peut-tuer

Länder-Analysen. « EU vs Disinfo: Doppelgänger », no 456 (11 octobre 2024): 13-18. https://laender-analysen.de/russland-analysen/456/eu-disinfo-doppelgaenger/

McBrien, Tyler. « Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016-2020. » Innovations for Successful Societies, Princeton University, 2020. https://successfulsocieties.princeton.edu/publications/defending-vote-estonia-creates-network-combat-disinformation-2016%E2%80%932020.

Miguel Serrano, Raquel, et Maria Giovanna Sessa. « Beyond Disinformation Countermeasures: Building a Response-Impact Framework ». EU DisinfoLab, 29 novembre 2024. https://www.disinfo.eu/publications/beyond-disinformation-countermeasures-building-a-response-impact-framework/.

Montaclair, Florent. « Du Tic à La Tactique : Les Mécanismes Grammaticaux de l'infox à Travers Les Tweets de Donald Trump ». The Conversation, 1 septembre 2022. http://theconversation.com/du-tic-a-la-tactique-les-mecanismes-grammaticaux-de-linfox-a-travers-les-tweets-de-donald-trump-188404.

Newman, Nic, Richard Fletcher, Robertson Craig T., Amy Ross Arguedas, et Nielsen Rasmus Kleis. « Reuters Institute Digital News Report 2024 ». Reuters Institute, 2024. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf.

NewsGuard, et ComScore. « Advertising on Misinformation », 23 août 2021. https://www.comscore.com/fre/Perspectives/Presentations-and-Whitepapers/2021/Advertising-on-Misinformation.

Östlund, Stefan, Tommy Shih, et Albin Gaunt. « Responsible Internationalisation : Guidelines for Reflection on International Academic Collaboration ». STINT, The Swedish Foundation for International Cooperation in Research and Higher Education, 2020. https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-342009.

Pamment, James, et Elsa Isaksson. « Psychological Defence: Concepts and Principles for the 2020s ». Lund University Psychological Defence Research Institute, juin 2024. https://mpf.se/psychological-defence-agency/publications/archive/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s.

Parton, Charles. « China-UK Relations: Where to Draw the Border Between Influence and Interference? » Royal United Services Institute for Defence and Security Studies, février 2019. https://www.rusi.org/explore-our-research/publications/occasional-papers/china-uk-relations-where-draw-border-between-influence-and-interference.

Renaudie, Amaury. « La stratégie d'influence chinoise dans le monde universitaire français ». Enderi, 28 juillet 2023. https://www.enderi.fr/La-strategie-d-influence-chinoise-dans-le-monde-universitaire-francais_a1162.html.

Simon, Phil. « La liberté d'expression face à la satire politique : un équilibre fragile ». Actualités Juridiques, 15 octobre 2024. https://www.avocats-emergence.fr/la-liberte-dexpression-face-a-la-satire-politique-un-equilibre-fragile/.

Statista. « Les sites internet les plus consultés au monde en 2024 », juin 2024. https://fr.statista.com/statistiques/1387500/nombre-visites-sites-internet-les-plus-visites-monde/.

Sources institutionnelles et législatives :

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. https://digital-strategy.ec.europa.eu/fr/news/commission-makes-eu16-million-funding-available-support-journalism-and-media-literacy-across-europe

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. https://ec.europa.eu/commission/presscorner/detail/fr/ip_24_6487

Commission européenne, « Tackling R&I Foreign Interference: Staff Working Document », 2022. https://data.europa.eu/doi/10.2777/513746

Commission européenne. « The 2022 Code of Practice on Disinformation », 16 juin 2022. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Conseil de l'Union européenne. « Une boussole stratégique pour renforcer la sécurité et la défense de l'UE au cours de la prochaine décennie », mars 2022. https://www.consilium.europa.eu/fr/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

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. https://data.consilium.europa.eu/doc/document/ST-7371-2022-COR-1/fr/pdf

Cour des Comptes européennes. « La désinformation concernant l'UE : un phénomène sous surveillance mais pas sous contrôle », 2021. https://data.europa.eu/doi/10.2865/086773

Gattolin, André. « Rapport d'information (…) sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences ». Direction de l'information légale et administrative, Sénat, 2021. https://documentation.insp.gouv.fr/insp/doc/VIEPUBLIQUE/5E81BCCC12159C8BC0C885657C024258/rapport-d-information-sur-les-influences-etatiques-extra-europeennes-dans-le-monde-universitaire-et-.

« Matriochka : une campagne prorusse ciblant les médias et la communauté des fact-checkers ». VIGINUM, 10 juin 2024. http://www.sgdsn.gouv.fr/publications/matriochka-une-campagne-prorusse-ciblant-les-medias-et-la-communaute-des-fact-checkers.

Organisation Mondiale de la Santé. « Gestion de l'infodémie sur la COVID-19 : Promouvoir des comportements sains et atténuer les effets néfastes de la diffusion d'informations fausses et trompeuses », 20 septembre 2020. https://www.who.int/fr/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation

Parlement européen. Décision du Parlement européen du 18 décembre 2024 sur la constitution, les compétences, la composition numérique et la durée de mandat d'une commission spéciale sur le bouclier européen de la démocratie (2024/2999(RSO)) (2024). https://www.europarl.europa.eu/doceo/document/TA-10-2024-0065_FR.html.

Parlement européen. « L'essentiel de la plénière 26-29 février 2024 - Session plénière Strasbourg », 22 février 2024. https://www.europarl.europa.eu/pdfs/news/expert/2024/2/briefing/20240212BRI17604/20240212BRI17604_fr.pdf.

Parlement Européen. Proposition de résolution sur le Russiagate: allégations d'ingérence russe dans les processus démocratiques de l'Union européenne (2024). https://www.europarl.europa.eu/doceo/document/B-9-2024-0130_FR.html.

Parlement européen. « Rapport sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation », 15 mai 2023. https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_FR.html.

Parlement européen. Résolution du Parlement européen du 8 février 2024 sur le Russiagate: allégations d'ingérence russe dans les processus démocratiques de l'Union européenne (2024/2548(RSP)) (2024). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0079_FR.html.

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. https://www.europarl.europa.eu/doceo/document/A-9-2024-0102_EN.html.

Parquet du Tribunal Judiciaire de Paris. « Communiqué de presse de la procureure de la République », 7 novembre 2023. https://www.tribunal-de-paris.justice.fr/sites/default/files/2023-12/CPETOILESBLEUES.pdf.

Présidence de la République. « Les lumières à l'ère numérique », 11 janvier 2022. https://www.vie-publique.fr/rapport/283201-lumieres-l-ere-numerique-commission-bronner-desinformation.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) (2022). http://data.europa.eu/eli/reg/2022/1925/oj/eng.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng.

Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (Text with EEA relevance) (2024). https://eur-lex.europa.eu/eli/reg/2024/1083/oj/eng.

Représentation permanente de la France auprès de l'OSCE. « Russie - Nouvelle ingérence numérique russe contre la France », 9 novembre 2023. https://osce.delegfrance.org/Russie-Nouvelle-ingerence-numerique-russe-contre-la-France-9-novembre-2023.

SEAE. « Plan d'action Contre La Désinformation », 5 décembre 2018. https://www.eeas.europa.eu/node/54866_en.

SEAE. « Questions and Answers about the East StratCom Task Force », 27 octobre 2021. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en.

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. http://www.sgdsn.gouv.fr/publications/publication-dun-guide-de-sensibilisation-la-menace-informationnelle-destination-de.

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. http://www.sgdsn.gouv.fr/publications/publication-dun-guide-de-sensibilisation-la-menace-informationnelle-destination-des.

Secrétariat général de la défense et de la sécurité nationale. « Portal Kombat : un réseau structuré et coordonné de propagande prorusse », 12 février 2024. http://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse.

Secrétariat général de la défense et de la sécurité nationale. « Publication d'un guide de sensibilisation à la menace informationnelle à destination de l'écosystème des acteurs économiques associés aux JOP24 », 20 juin 2024. http://www.sgdsn.gouv.fr/publications/publication-dun-guide-de-sensibilisation-la-menace-informationnelle-destination-de.

Secrétariat général de la défense et de la sécurité nationale. « RRN : une campagne numérique de manipulation de l'information complexe et persistante », 13 juin 2023. http://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et.

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. http://www.sgdsn.gouv.fr/publications/synthese-de-la-menace-informationnelle-ayant-vise-les-jeux-olympiques-et-paralympiques.

Sénat. « Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide », 23 juillet 2024. https://www.senat.fr/rap/r23-739-1/r23-739-1.html.

Sénat. « Mission d'information "Influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences" », septembre 2021. https://www.senat.fr/travaux-parlementaires/structures-temporaires/missions-dinformation-communes/archives/mission-dinformation-influences-etatiques-extra-europeennes-dans-le-monde-universitaire-et-academique-francais-et-leurs-incidences.html.

Tatham, Steve A. Strategic Communication: A Primer. Defence Academy of the United Kingdom, Advanced Research and Assessment Group, 2008.

UK Legislation. Digital Markets, Competition and Consumers Act 2024 (2024). https://www.legislation.gov.uk/ukpga/2024/13/enacted.

Wardle, Claire, et Hossein Derakhshan. « Information Disorder: Toward an interdisciplinary framework for research and policymaking ». Council of Europe, 2017. INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making Information Disorder Toward an interdisciplinary framework for research and policymaking

Sources audio

France Inter. « L'astroturfing, la grande illusion de l'opinion », 25 janvier 2024. https://www.radiofrance.fr/franceinter/podcasts/zoom-zoom-zen/zoom-zoom-zen-du-jeudi-25-janvier-2024-1862289

France Inter, « Story Killers, la dernière enquête de Forbidden Stories ». 16 février 2023. https://www.radiofrance.fr/franceinter/podcasts/un-jour-dans-le-monde/un-jour-dans-le-monde-du-jeudi-16-fevrier-2023-3485180.

Franceinfo. « Intelligence artificielle, "badbots", fermes à robots... Au cœur de la guerre en ligne contre les campagnes de désinformation et de manipulation de l'opinion », 25 novembre 2024. https://www.francetvinfo.fr/replay-radio/le-choix-franceinfo/reportage-intelligence-artificielle-badbots-fermes-a-robots-au-c-ur-de-la-guerre-en-ligne-contre-les-campagnes-de-desinformation-et-de-manipulation-de-l-opinion_6889778.html

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