

La désinformation à l'assaut des démocraties

I. La désinformation, un risque mondial accru par les plateformes numériques

Érosion de la confiance, divisions accrues : la désinformation figure parmi les principaux risques identifiés par le *World Economic Forum* en 2025, entravant la coopération nécessaire pour affronter les crises mondiales¹. Mais sommes-nous aussi rationnels que nous le croyons ? Une étude de l'OCDE (2024) révèle que nous ne détectons les fausses informations que dans 6 cas sur 10, malgré une forte confiance en nos capacités à les identifier.² En France, deux-tiers des Français adhèrent à au moins une *fake news*³.

Il est important de distinguer trois concepts. La mésinformation, qui est une information erronée diffusée sans intention de causer du tort. La mal-information, qui s'appuie sur des faits réels mais est diffusée pour nuire, tel que le *doxing*. Et enfin, la désinformation, qui consiste en la création et la diffusion délibérée d'informations fausses pour nuire à un individu, un groupe, une organisation ou un État⁴. On les distingue de la propagande et de la satire.

La montée de la désinformation et mésinformation par les réseaux sociaux pose des risques réels pour nos sociétés : polarisation, réduction de la confiance dans les processus et institutions démocratiques⁵, montée de la violence. L'accès à des sources d'information pluralistes et la liberté d'expression restent nécessaires au débat public. Aujourd'hui, les jeunes accordent désormais une confiance similaire aux réseaux sociaux et aux médias traditionnels⁶. La transition d'un modèle de médias *gatekeepers* à la dictature des algorithmes et le partage d'informations instantanée par les plateformes numériques (Meta, X, Youtube, Tiktok) a élargi l'espace démocratique mais crée des risques de désinformation massive à grande échelle⁷. L'épidémie d'infobésité due aux réseaux sociaux nous a conduits à une situation de surcharge informationnelle, générant une situation d'impuissance apprise sous forme d'apathie, de cynisme et de suivi de tendances, ainsi qu'une *selective exposure* par des bulles de filtre et une balkanisation d'internet⁸.

II. Comment répondre à la désinformation ?

A. L'impact des plateformes numériques

À l'ère du *buzz*, les algorithmes des réseaux sociaux favorisent les *fake news*, se diffusant six à vingt fois plus vite que les faits, générant plus de clics et donc de revenus (étude de *Science*, 2018)⁹. De nombreux chercheurs et analystes soutiennent que ce modèle basé sur l'engagement¹⁰ crée une incitation perverse à privilégier les contenus qui captent le plus l'attention, même s'ils sont

¹ [Global Risks Report 2025: Conflict, Environment and Disinformation Top Threats > Press releases | World Economic Forum](#)

² [The OECD Truth Quest Survey | OECD](#)

³ [Européennes 2024 : les Français particulièrement vulnérables à la désinformation | Ipsos](#)

⁴ [Journalism, fake news & disinformation: handbook for journalism education and training: UNESCO series on journalism education; 2018 - 265552eng.pdf](#)

⁵ [Full article: Information, doubt, and democracy: how digitization spurs democratic decay](#)

⁶ [Trust in voting: How misinformation threatens democracy - USC Today](#)

⁷ [Misinformation spread differently than most content on Facebook during the 2020 election. Northeastern research finds](#)

⁸ [Chung-hong Chan & King-wa Fu. "The Relationship Between Cyberbalkanization and Opinion Polarisation - Recherche Google](#)

⁹ [The spread of true and false news online | Science](#)

¹⁰ [The Future of Platform Power: Fixing the Business Model | Journal of Democracy](#)

sensationnalistes, polarisants, émotionnellement chargés, voire faux.¹¹ La désinformation, en particulier celle qui suscite l'indignation ou la peur, génère souvent un fort engagement. Sa propagation pourrait donc être, non pas un effet secondaire malheureux, mais une conséquence attendue du modèle économique lui-même.¹²

Shoshana Zuboff a théorisé ce phénomène sous le nom de *Surveillance Capitalism*¹³. Les plateformes ne vendraient pas seulement de la publicité, mais extraient massivement des données sur le comportement des utilisateurs (le "surplus comportemental") pour créer des produits prédictifs permettant d'anticiper et, potentiellement, d'influencer les comportements futurs des individus à des fins commerciales.¹⁴ Ce modèle, basé sur l'extraction et la manipulation de données à l'insu des utilisateurs, crée un désalignement fondamental entre les intérêts économiques des plateformes et le bien-être des utilisateurs ou la santé démocratique. La désinformation peut même être un outil facilitant cette extraction et cette manipulation.¹⁵

La personnalisation des fils, l'opacité des algorithmes et le partage instantané accélèrent aussi la diffusion à grande échelle, vraie ou fausse. La désinformation se répand aussi lentement en *slow burn* par le partage viral entre individus. Une minorité d'utilisateurs est exposée à la majorité des fausses informations¹⁶, et une infime partie, les *super-spreaders* (0,1% en 2019), est responsable de 80% des partages. Mais comment éviter une modération politiquement biaisée ou empêchant des discours légitimes bien que marginaux ou critiques?

Bien qu'elle semble avoir un effet limité sur les élections¹⁷, la désinformation fragilise la confiance, polarise et influence les perceptions. En 2024, les *fake news* sur l'immigration, la criminalité et l'économie ont façonné le récit de campagne des élections américaines et affecté la candidate démocrate¹⁸. Une étude de 2018 de la Fondation Hewlett révèle un cycle vicieux où les algorithmes amplifient les contenus trompeurs sur les réseaux sociaux, incitant politiciens et médias à produire désinformation et polarisation pour obtenir soutien et gains financiers, ce qui détériore l'information politique. (275). Des études internes à Facebook (les "Facebook Papers") ont montré que les algorithmes peuvent orienter vers des contenus extrêmes et polarisants, contribuant à la radicalisation et aux chambres d'écho. Meta aurait constaté un lien entre ses recommandations et les adhésions à des groupes extrémistes¹⁹. Mais comment y répondre? Parmi l'arsenal on retrouve suppression de contenu, suspension, bannissement, *labelling*, *downranking*, redirection vers des sources crédibles. Pour maintenir un équilibre entre le volume de données à traiter, la précision contextuelle et les conditions de travail, une approche combinée de signalement par les utilisateurs, d'intelligence artificielle et de modérateurs humains reste essentielle. Sur les réseaux sociaux, des algorithmes sont développés pour signaler automatiquement les contenus potentiellement faux ou trompeurs. Facebook, par exemple,

¹¹ [Engagement, user satisfaction, and the amplification of divisive content on social media | PNAS Nexus | Oxford Academic](#)

¹² [How do digital platforms profit from disinformation: Research Summary — Dr. Diaz Ruiz](#)

¹³ [Algorithms, Lies, and Social Media | OpenMind Magazine](#)

¹⁴ ["Surveillance Capitalism" Is Not a Fatality | Institut Montaigne](#)

¹⁵ ["Surveillance capitalism – How to get back control of our data" with Shoshana Zuboff & Max Schrems - Shoshana Zuboff | Harvard Kennedy School](#)

¹⁶ [Major Social Media Platforms Have Weakened Rules Against the Spread of Election Misinformation. New ADL Report Finds | ADL](#)

¹⁷ [Are fears about online misinformation in the US election overblown? The evidence suggests they might be | Reuters Institute for the Study of Journalism](#)

¹⁸ [How disinformation defined the 2024 election narrative](#)

¹⁹ [DIGI-Final-Report_July5_2023.pdf & Op-ed: Social media algorithms & their effects on American politics - Fung Institute for Engineering Leadership](#)

utilise des modèles d'IA pour limiter la diffusion de publications mensongères, tandis que Twitter (aujourd'hui X) a mis en place le système *Community Notes*, permettant aux utilisateurs d'ajouter un contexte aux publications virales²⁰.

Malgré des politiques existantes, leur application est jugée largement inefficace et inconsistante, avec un relâchement noté par l'Anti-Defamation League, notamment sur X avant les élections américaines de 2024²¹. Des tests de Global Witness en 2022 ont montré l'échec de TikTok et Facebook à bloquer des publicités avec de fausses informations électorales, tandis que YouTube a montré une application hétérogène entre les États-Unis et le Brésil, où la désinformation a été approuvée²². Ces défaillances s'expliquent par des exceptions pour les personnalités politiques ou contenu "d'intérêt public"²³, un suivi inégal des signalements des utilisateurs au profit de systèmes automatisés ou de *trusted flaggers*, et la faillibilité de la modération automatisée (contournement facile, interprétation contextuelle et linguistique difficile)²⁴. Ainsi, les *Community Notes* de X ont été critiquées par de nombreuses analyses, par leur lenteur d'apparition, leur faible portée et leur échec de consensus sur des sujets polarisants.²⁵ Ainsi, l'autorégulation montre ses limites. Ses politiques varient selon la pression publique, par exemple lors de l'assaut du Capitole, le climat politique et des intérêts géographiques ou commerciaux divergents. L'allocation des ressources de modération diffère selon les pays et les décisions sont influencées par la volonté d'éviter les controverses. De ce fait, l'absence de responsabilité propre des plateformes face à des systèmes organisationnels complexes où la responsabilité est diluée est manifeste²⁶.

Modifier les algorithmes de curation pourrait atténuer la désinformation soit en réduisant la visibilité des contenus nuisibles par la détection, le *downranking* ou la suppression, soit en entraînant les algorithmes à prioriser des valeurs au-delà de l'engagement lors de la recommandation de contenu^{27 28}. Certaines plateformes expérimentent déjà des modèles favorisant le débat constructif et le consensus en récompensant les comportements vertueux par l'accès à de nouvelles fonctionnalités²⁹. La recherche explore comment ces algorithmes pourraient améliorer la compréhension mutuelle et la confiance³⁰. Donner aux utilisateurs plus de contrôle sur leur flux de contenu est une autre solution proposée. Les plateformes pourraient offrir des flux chronologiques ou permettre aux utilisateurs de choisir d'autres algorithmes de recommandation via un *middleware*, un logiciel servant d'intermédiaire entre l'interface utilisateur et la plateforme d'un réseau social³¹. Bien que l'efficacité du *middleware* contre la désinformation ne soit pas prouvée et que certains craignent que les algorithmes préférés ne favorisent le sensationnalisme³², son objectif principal, selon Francis

²⁰ [Misinformation | Transparency Center.](#)

²¹ [Major Social Media Platforms Have Weakened Rules Against the Spread of Election Misinformation. New ADL Report Finds | ADL](#)

²² [TikTok and Facebook fail to detect election misinformation in the US, while YouTube succeeds | Global Witness](#)

²³ [Major Social Media Platforms Have Weakened Rules Against the Spread of Election Misinformation. New ADL Report Finds | ADL](#)

²⁴ [Le casse-tête de la modération des réseaux sociaux par Ophélie Surcouf](#)

²⁵ [Community Notes on X and Meta: Are they as Visible as Users Would Hope?](#)

²⁶ [Couppable, mais pas responsable – Dan Davies, The Unaccountability Machine, 2024 - Institut Avant-garde](#)

²⁷ [Prévalence | Espace modération](#)

²⁸ [The Web's Recommendation Engines Are Broken. Can We Fix Them? | WIRED](#)

²⁹ [An Illustrated Field Guide to Social Media | Knight First Amendment Institute](#)

³⁰ [Bridging Systems: Open problems for countering destructive divisiveness across ranking, recommenders, and governance | Knight First Amendment Institute](#)

³¹ [Francis Fukuyama: How to Save Democracy From Technology | Foreign Affairs](#)

³² [The Future of Platform Power: Making Middleware Work | Journal of Democracy](#)

Fukuyama, est de réduire le pouvoir des grandes entreprises technologiques dans la sphère publique³³. Au-delà, l'émergence et la démocratisation rapide des IA génératives représente un potentiel accrue de création facile et à faible coût de *deepfakes* audio, vidéos et textuelles réalistes³⁴.

Face à ce manque d'autorégulation, quelles réponses réglementaires?

Le *Digital Services Act* de l'Union Européenne, entré en vigueur début 2024, cherche à responsabiliser les plateformes numériques sur les risques sociétaux de leur utilisation. Il instaure des obligations d'évaluation des risques, d'atténuation, de transparence, de *diligence*, et d'intégrité électorale. Les contrevenants s'exposent à une amende jusqu'à 6% du chiffre d'affaires annuel et d'interdiction temporaire au niveau européen en cas d'infractions répétées. Malgré cela, la société civile et des chercheurs ont pointé le manque d'uniformité méthodologique, l'analyse superficielle du rôle des algorithmes et le manque de détails concernant l'efficacité des mesures d'atténuation³⁵. La Commission a engagé des procédures formelles d'infraction contre X (concernant la modération de contenu illégal, la manipulation de l'information, la transparence) et TikTok (concernant la protection des mineurs et, plus récemment, les risques pour l'intégrité électorale liés aux élections roumaines).³⁶ Des "stress tests" pré-électorales ont également été menés avec les plateformes³⁷. Son analyse a pourtant révélé plusieurs faiblesses et risques potentiels. Le manque de définition précise de la désinformation et des risques systémiques laisse une marge d'interprétation et de manœuvre importante³⁸. La fragilité du Code de Pratique est soulignée par le retrait ou la réduction d'engagement de certains acteurs dans le fact-checking. Le processus pourrait excessivement interdire des contenus légaux mais préjudiciables. Enfin, un risque de contrôle accru pour les régimes autoritaires face aux dissidents demeure³⁹.

Du côté des Etats Unis, la Section 230 du *Communications Decency Act* de 1996 donne une immunité aux plateformes, non responsables du contenu publié par les utilisateurs, tout en protégeant les plateformes de responsabilité civile lorsqu'elle agissent de "bonne foi" en restreignant l'accès à du matériel jugé "obscène, indécent, lascif, obscène, excessivement violent, harcelant ou *otherwise objectionable*". Cette Section 230 fait l'objet de débats et d'appels bipartisans à sa réforme, avec d'un côté un camp pro-modération associé aux Démocrates dénonçant le manque de responsabilité des plateformes, et de l'autre le camp anti-censure associé aux Républicains souhaitant que les plateformes ne puissent pas censurer des contenus, quels qu'ils soient⁴⁰. Les Etats Unis ne disposant pas de loi fédérale complète imposant aux plateformes des obligations, la régulation est fragmentée avec certains Etats comme le Texas et la Floride, essayant d'imposer des restrictions à la modération se heurtant à des contestations juridiques fondées sur le Premier Amendement⁴¹.

³³ [Radical Proposal: Middleware Could Give Consumers Choices Over What They See Online | Stanford HAI](#)

³⁴ [AI-generated disinformation poses threat of misleading voters in 2024 election | PBS News](#)

³⁵ [A Critical Look at the DSA's First Risk Assessments: Civic Discourse and Electoral Processes | liberties.eu](#)

³⁶ [Beyond Disinformation: How DSA Risk Assessments Ignore Democracy's Real Threats | TechPolicy.Press](#)

³⁷ [Civic Discourse and Electoral Processes](#)

³⁸ [The EU's Code of Practice on Disinformation is Now Part of the Digital Services Act. What Does It Mean? | TechPolicy.Press](#)

³⁹ [The regulation of content moderation in the DSA: can we trust the due process? - MedCrave online](#)

⁴⁰ [Summarizing the Section 230 Debate: Pro-Content Moderation vs Anti-Censorship | Bipartisan Policy Center](#)

⁴¹ [The Digital Services Act and the Brussels Effect on Platform Content Moderation | Chicago Journal of International Law](#)

Ainsi, ces deux réglementations entrent en conflit : responsabilité conditionnelle contre immunité presque universelle, approche proactive et systématique contre approche réactive et autorégulation, liberté d'expression en équilibre avec d'autres droits fondamentaux comme la dignité humaine et la protection de l'intérêt public contre liberté d'expression absolue. Ainsi, cette divergence pose des défis majeurs de conformité dans un paysage réglementaire mondial fragmenté. L'Effet Bruxelles, où les normes européennes, plus strictes et assorties de sanctions élevées, influencent les pratiques mondiales des entreprises, conduirait à des normes de protection et d'expérience utilisateur différentes selon les régions géographiques⁴². Bien que le DSA représente une approche plus interventionniste, son efficacité réelle et sa mise en oeuvre restent difficiles face à un manque de définition harmonisée au niveau européen d'un contenu "illégal" et "préjudiciable" dans 27 Etats membres, l'application cohérente et rapide par la Commission et la lutte contre une conformité superficielle des plateformes⁴³. En somme, si le DSA exerce indéniablement une influence mondiale en raison de la puissance du marché européen, forçant les plateformes à adapter au moins partiellement leurs opérations (*effet de facto*), son adoption directe et généralisée par d'autres pays (*effet de jure*) semble peu probable à court terme. Les conflits juridiques fondamentaux (notamment avec les États-Unis)⁴⁴, la capacité des plateformes à segmenter leur conformité, les coûts et la complexité de mise en œuvre⁴⁵, ainsi que la résistance des géants du numérique face à une remise en cause de leur modèle économique⁴⁶ constituent des freins majeurs. Une fragmentation réglementaire mondiale, avec des approches hybrides ou divergentes, apparaît plus probable qu'une convergence rapide autour du modèle européen.

Ainsi, il faudra garantir la mise en place et le renforcement d'organes de surveillance indépendants pour évaluer les risques systémiques, la conformité des plateformes aux réglementations et garantir une application impartiale des règles. Également, le renforcement de la transparence du fonctionnement des algorithmes, de leur modération, pratiques publicitaires, gestion de données est nécessaire pour améliorer la recherche indépendante sur le sujet.

B. La désinformation comme outil d'ingérence

Dans un contexte de rivalités géopolitiques croissantes, les régimes autoritaires tels que la Russie, la Chine ou l'Iran utilisent la désinformation numérique comme un instrument stratégique d'influence et de déstabilisation. Loin d'être un phénomène marginal, ces opérations d'influence s'inscrivent dans des stratégies coordonnées, inscrites dans le temps long, visant à affaiblir les démocraties de l'intérieur⁴⁷.

Comme le souligne un dossier récent publié par le think tank Confrontations Europe⁴⁸, ces États exploitent les vulnérabilités des sociétés ouvertes en s'appuyant sur un large éventail d'intermédiaires

⁴² [US and EU Clash over Regulation of Digital Content Moderation](#)

⁴³ [DSA Disinformation Dilemma: Trump and TikTok Squeeze Europe - CEPA](#)

⁴⁴ [The Digital Services Act and the Brussels Effect on Platform Content Moderation | Chicago Journal of International Law](#)

⁴⁵ [Towards a global approach to digital platform regulation | 03 Regulatory pathways and potential solutions](#)

⁴⁶ [EU Export of Regulatory Overreach: The Case of the Digital Markets Act \(DMA\) |](#)

⁴⁷ Jeangène Vilmer, J.-B. (2023). Les démocraties face aux manipulations de l'information : vulnérabilités et résilience. Dans S. Taillat, A. Cattaruzza et D. Danet *La Cyberdéfense - 2e éd. : Politique de l'espace numérique Les démocraties face aux manipulations de l'information : vulnérabilités et résilience* | Cairn.info

⁴⁸ [Confrontations Europe. Ingérence étrangère et désinformation: Sommes-nous prêts pour les élections européennes ? Mars 2024.](#)

: fermes à trolls, agences de communication privées, ou encore médias relais tels que RT ou Sputnik. L'objectif n'est pas tant de convaincre que de diviser, brouiller les repères, et miner la confiance dans les institutions démocratiques.

La Russie, en particulier, s'est imposée comme un acteur majeur de la guerre informationnelle. Ses campagnes visent à exacerber les fractures identitaires, à délégitimer les processus électoraux (comme aux États-Unis en 2016 ou en France en 2017⁴⁹), et à renforcer une image de chaos inhérente aux systèmes démocratiques. De son côté, la Chine développe une approche plus insidieuse : elle combine la censure interne, la diplomatie publique, et l'influence informationnelle pour diffuser un récit favorable à ses intérêts géostratégiques, notamment sur Taïwan, Hong Kong ou le Xinjiang.

On constate une permanence de ces campagnes, qui ne se limitent plus à des contextes de crise ponctuels. Elles participent d'une logique de conflictualité hybride, où le brouillage de l'information devient une arme de guerre non conventionnelle, cherchant à désorienter les opinions publiques, polariser les débats et faire vaciller les fondements de la démocratie libérale.

Mais la menace désinformationnelle n'est pas uniquement exogène, elle est aussi endogène. Une partie de l'écosystème politique domestique, et en particulier les partis d'extrême droite radicale, a intégré la désinformation comme une composante stratégique de son action politique. Loin d'être le simple produit d'un populisme généralisé ou d'une marginalité idéologique, cette instrumentalisation du faux relève d'un choix délibéré, appuyé par une analyse précise des dynamiques attentionnelles propres au numérique.

Une étude majeure publiée en janvier 2025, menée par Petter Törnberg et Juliana Chueri⁵⁰, fondée sur l'analyse de 32 millions de tweets de parlementaires issus de 26 démocraties occidentales entre 2017 et 2022, met en lumière ce phénomène avec rigueur. En croisant des millions de liens partagés avec des bases d'évaluation de fiabilité des sources (Media Bias/Fact Check, Wikipedia), les chercheurs montrent que le populisme, pris isolément, n'est pas prédictif d'un usage intensif de la désinformation. Ni les partis populistes de gauche, ni ceux de la droite traditionnelle ne se distinguent significativement en la matière. Seuls les partis d'extrême droite populiste présentent une probabilité nettement supérieure de diffuser des contenus à faible factualité.

Pourquoi cette asymétrie ? Parce que la désinformation, pour ces forces politiques, remplit une fonction politique centrale. Elle sert à affaiblir la légitimité des institutions démocratiques, à saper la crédibilité des médias traditionnels, et à mobiliser un électorat traversé par la défiance, convaincu que les canaux d'information officiels sont corrompus ou mensongers. La diffusion du faux devient une manière de signaler sa rupture avec l'« establishment », de polariser l'opinion, de structurer un récit simplifié et émotionnel du monde. Dans ce contexte, le mensonge n'est pas une dérive, mais un outil politique rationalisé.

Cette stratégie prospère dans un environnement façonné par l'économie de l'attention, qui valorise les contenus émotionnels, clivants, spectaculaires, autant de caractéristiques que l'on retrouve dans les récits désinformationnels. La dynamique est donc circulaire, plus les extrêmes droites diffusent du

⁴⁹ [Jean-Baptiste Jeangène Vilmer. 2019. *The "Macron Leaks" Operation : A Post-Mortem*. IRSEM/Atlantic Council.](#)

⁵⁰ [Törnberg, P., & Chueri, J. \(2025\). When Do Parties Lie? Misinformation and Radical-Right Populism Across 26 Countries. The International Journal of Press/Politics. When Do Parties Lie? Misinformation and Radical-Right Populism Across 26 Countries - Petter Törnberg, Juliana Chueri. 2025](#)

faux, plus elles captent l'attention ; plus elles captent l'attention, plus elles gagnent en influence politique. Ce cycle toxique mine les conditions mêmes du débat démocratique.

C. L'éducation à l'esprit critique comme levier de résilience

L'éducation à l'esprit critique, à travers l'éducation aux médias et à l'information (EMI), constitue un pilier essentiel dans la lutte contre la désinformation en ligne. Selon l'UNESCO (2013), les citoyens bénéficiant d'un bon niveau d'EMI sont généralement moins enclins à relayer des informations erronées.⁵¹ Cette compétence est essentielle pour évaluer les sources, déceler les manipulations et renforcer la résilience cognitive face à l'infobésité. Cependant, son efficacité est limitée par les inégalités d'accès à l'éducation et la polarisation sociale.

Des pays comme la Finlande, le Canada et l'Estonie ont démontré de manière concrète les bénéfices des politiques publiques favorisant l'EMI dès le plus jeune âge. La Finlande, reconnue pour sa résilience face à la désinformation, a intégré l'EMI dans le cursus scolaire dès l'école primaire, en mettant l'accent sur la capacité d'analyse, la détection des biais et la compréhension du fonctionnement des médias⁵². Au Canada, des initiatives comme "MediaSmarts" proposent des ressources interactives pour les enseignants et les parents afin de lutter contre la désinformation⁵³. Néanmoins, ces exemples restent marginaux à l'échelle mondiale où la formation à l'esprit critique reste souvent superficielle, ponctuelle ou absente, notamment dans les pays en développement.

Parmi les principales faiblesses de cette approche éducative, on note le manque d'enseignants formés, l'absence de politiques publiques cohérentes et la difficulté d'adapter les contenus pédagogiques aux mutations rapides du numérique⁵⁴. En outre, le développement de l'esprit critique, compétence complexe, requiert du temps, des pédagogies actives et un soutien institutionnel, des éléments souvent insuffisants dans les systèmes éducatifs. Pour remédier à ces limites, il est recommandé d'intégrer l'EMI de manière transversale dans les programmes scolaires, de garantir la formation continue des enseignants et de favoriser les partenariats entre les écoles, les universités et les organisations de la société civile.

Certains estiment que l'éducation à l'esprit critique est trop lente face à la propagation virale des fausses informations. Cependant, des études comme celle de Lewandowsky (2020) montrent que le *pre-bunking* (ou inoculation psychologique) peut réduire de 30% la crédibilité perçue des fausses informations⁵⁵. Cette technique, inspirée des vaccins, consiste à exposer préventivement les individus à des versions affaiblies de contenus manipulateurs, tout en expliquant leurs stratégies. Des initiatives telles que le jeu numérique *Bad News* ont prouvé une amélioration significative de la résistance des utilisateurs à la désinformation après quelques sessions interactives⁵⁶. Ces approches proactives préparent mentalement les individus avant qu'ils ne soient confrontés à des informations trompeuses.

En complément, la vérification des faits, bien que réactive, reste un outil indispensable. Des organisations comme Agência Lupa (Brésil), Chequeado (Argentine) ou Full Fact (Royaume-Uni)

⁵¹ UNESCO. *Media and Information Literacy: Policy and Strategy Guidelines*. Paris: UNESCO, 2013.

⁵² [Digital News Report 2023 | Reuters Institute for the Study of Journalism](#)

⁵³ [Welcome to MediaSmarts | MediaSmarts](#)

⁵⁴ Livingstone, Sonia; Bulger, Monica. "Media Literacy—Past and Present." *Journal of Media Literacy Education*, vol. 10, no. 1, 2018.

⁵⁵ [The Debunking Handbook 2020 - Center for Climate Change Communication](#)

⁵⁶ [The fake news game: actively inoculating against the risk of misinformation: Journal of Risk Research: Vol 22 , No 5 - Get Access](#)

jouent un rôle essentiel dans la déconstruction des fausses informations. Toutefois, leur impact reste limité en raison de la faible portée de leurs actions et de la résistance d'un public déjà émotionnellement engagé dans des récits spécifiques.

Ainsi, la lutte contre la désinformation en ligne nécessite une approche intégrée où l'éducation aux médias et à l'information joue un rôle central. Investir dans l'esprit critique dès l'école, compléter par des stratégies de *pre-bunking* et de *fact-checking*, et utiliser les technologies comme appui, peut contribuer à bâtir une société plus résiliente. Mais sans engagement politique en faveur d'une éducation critique et équitable, tout progrès technique risque de rester superficiel ou temporaire.

III. Conclusion : un impératif démocratique face à la désinformation.

La désinformation reste ainsi une menace aux multiples formes, nourrie par la complexité des plateformes numériques et les ingérences d'acteurs étatiques et non-étatiques. Elle demeure un défi crucial pour la survie de nos démocraties. Elle érode la confiance, intensifie la polarisation, favorise l'ingérence étrangère et exploite nos vulnérabilités cognitives, minant ainsi les bases du débat public et compromettant la légitimité des élections. Face à cette urgence, des solutions individuelles, isolées et dispersées sont inefficaces. Seule une stratégie holistique, globale et coordonnée, engageant divers acteurs, permettra d'établir des sociétés résistantes à la désinformation.

Il convient donc d'inverser la tendance, de lutter contre la désinformation qui affaiblit nos démocraties et de renforcer nos politiques sur le sujet par les recommandations suivantes :

1. **Responsabiliser les plateformes** avec une approche de “sécurité dès la conception” pour prévenir les risques de désinformation en rendant obligatoire la transparence des algorithmes, de leur modération et de l'accès et l'usage de leur données; une modération humaine contextuelle, multilingue et équitable; la suppression des exceptions pour les personnes et contenus “d'intérêt public”; et un système de recommandation basé sur la qualité des échanges et non l'engagement.
2. **Réguler de manière proactive et harmonisée** en améliorant et étendant le DSA, par l'évaluation des risques, des organismes de surveillance indépendants et une coopération internationale sur le sujet pour contrer efficacement les menaces transnationales comme l'ingérence étrangère tout en garantissant le respect de la liberté d'expression.
3. **Renforcer la résilience** individuelle et collective par l'intégration de l'AMI dès le plus jeune âge, en renforçant l'esprit critique et la détection des biais, des activités de *pre-bunking* et le soutien au *fact-checking*.
4. **Renforcer le rôle des chercheurs et de la société civile** en augmentant les financements de la recherche indépendante pour analyser les mécanismes de la désinformation et l'efficacité de contre-mesures par l'accès à des données de qualité, non biaisés et plus représentatives, ainsi que renforcer le rôle essentiel de surveillance et de plaidoyer de la société civile.

L'heure n'est ni à la complaisance, ni à l'inaction. Citoyens, décideurs politiques, plateformes numériques, chercheurs, éducateurs et organisations de la société civile, nous devons collectivement prendre nos responsabilités pour préserver l'intégrité de notre espace informationnel. Investissons dans l'éducation critique, exigeons la transparence des algorithmes, soutenons la recherche indépendante et œuvrons ensemble à l'élaboration de réglementations efficaces. L'avenir de nos démocraties dépend de notre capacité à débattre dans un écosystème informationnel sain et digne de confiance.