Guide sur la manipulation de l'information : Un conseil pratique pour les élections et au-delà

NDI NATIONAL DEMOCRATIC INSTITUTE

IRI INTERNATIONAL REPUBLICAN INSTITUTE Advancing Democracy Worldwide

Stanford | Internet Observatory *Cyber Policy Center*

Guide sur la manipulation de l'information : Un conseil pratique pour les élections et au-delà

Septembre 2021

NDI NATIONAL DEMOCRATIC INSTITUTE

IRI INTERNATIONAL REPUBLICAN INSTITUTE Advancing Democracy Worldwide

Stanford | Internet Observatory Cyber Policy Center

Table des matières

À propos de nous

International Republican Institute

L'International Republican Institute (IRI) est une organisation non gouvernementale sans but lucratif ni affiliation politique qui s'engage promouvoir la démocratie et la liberté dans le monde entier. Depuis 1983, l'IRI a apporté son soutien à des organisations de la société civile, des journalistes, des gouvernements démocratiques et d'autres acteurs de la démocratie dans plus de 100 pays - en Afrique, en Asie, en Eurasie, en Europe, en Amérique latine et aux Caraïbes, au Moyen-Orient et au nord de l'Afrique. L'équipe Technologie et Démocratie de l'IRI œuvre dans toutes les régions du monde pour aider les acteurs de terrain à faire de la numérisation et de la révolution technologique une force pour les avancées démocratiques, notamment à travers une variété de programmes visant à contrer la manipulation de l'information et à renforcer la résilience dans le monde entier.

National Democratic Institute

Le National Democratic Institute for International Affairs (NDI) est une organisation non gouvernementale sans but lucratif ni affiliation politique qui vise à répondre aux aspirations des personnes du monde entier à vivre dans des sociétés démocratiques qui reconnaissent et promeuvent les droits humains fondamentaux. Depuis sa fondation en 1983 comme l'une des quatre principales institutions de la National Endowment for Democracy, le NDI et ses partenaires locaux œuvrent pour soutenir et renforcer les institutions et les pratiques démocratiques en renforçant les partis politiques, les organisations civiques et les parlements, en préservant les élections et en promouvant la participation citoyenne, l'ouverture et la responsabilisation des gouvernements. Le NDI est l'organisation phare qui travaille à la mise en œuvre d'une série de programmes variés incluant des aspects clés des technologies de l'information et de la communication (TIC), cible les institutions démocratiques et soutient les démocrates en général, en particulier à travers ses initiatives INFO/tegrity qui appuient des interventions contre la désinformation, les discours haineux et d'autres formes de contenu nuisible tout en promouvant l'intégrité de l'information dans le monde entier.

Stanford Internet Observatory

Le Stanford Internet Observatory est un programme interdisciplinaire de recherche, d'enseignement et d'engagement politique pour l'étude des abus dans les technologies de l'information actuelles, en mettant l'accent sur les réseaux sociaux. Le Stanford Internet Observatory a été fondé en 2019 pour mener des recherches sur l'utilisation abusive d'Internet à des fins préjudiciables, formuler des réponses techniques et politiques et enseigner à la prochaine génération comment éviter les erreurs du passé.

Remerciements

Auteurs

Ce guide a été rédigé par Daniel Arnaudo, Samantha Bradshaw, Hui Hui Ooi, Kaleigh Schwalbe, Amy Studdart, Vera Zakem and Amanda Zink.

Remerciements

Nous remercions les nombreuses personnes du monde entier qui nous ont soutenus dans l'élaboration de ce guide, notamment pour leurs contributions en tant que personnes interrogées, participants aux tables rondes et réviseurs de ce guide. Nous tenons également à remercier Renée DiResta, Elena Cryst, Josh Goldstein, Shelby Grossman et Moira Whelan pour leurs commentaires et leurs conseils sur ce rapport.

Nous remercions également la National Endowment for Democracy pour son soutien à l'élaboration de ce guide.

Introduction

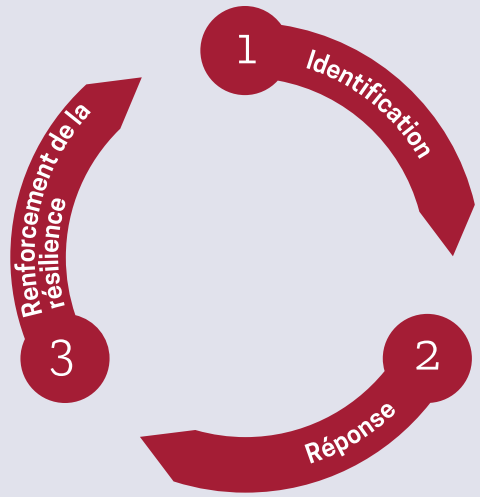
Ces dernières années, l'International Republican Institute (IRI), le National Democratic Institute (NDI) et le Stanford Internet Observatory (SIO) ont observé des efforts visant à compromettre l'intégrité des informations liées aux élections dans tous les coins du monde. Sans des efforts concertés pour identifier les manipulations d'informations liées aux élections, y répondre et développer la résilience à long terme, les attaques contre l'intégrité de l'information risquent de délégitimer les élections dans le monde entier, de réduire la confiance dans les gouvernements élus, de polariser les sociétés et d'affaiblir les démocraties en général.

La manipulation de l'information autour d'une élection est un phénomène nouveau et peu familier pour de nombreux pays. Les acteurs de la société civile, les journalistes, les gouvernements, les organismes chargés de l'organisation des élections et d'autres acteurs de la démocratie se retrouvent souvent à devoir réagir dans la période précédant une élection. Pour relever ce défi, l'IRI, le NDI et le SIO ont uni leurs forces pour créer ce guide, destiné à aider à surmonter les six premiers mois du processus de préparation électorale. Le guide présente les bases du problème et les éléments essentiels des réponses possibles et indique des ressources fiables pour ceux qui souhaitent approfondir un type particulier d'intervention ou de menace.

Nous espérons que ce guide vous permettra, ainsi qu'à tous ceux qui se consacrent à la défense de la démocratie, de repousser les tentatives de déstabilisation d'une concurrence libre et égale entre tous les partis politiques. La manipulation de l'information étant un défi permanent, ce guide vous sera également utile en dehors des cycles électoraux.

L'approche du guide

L'approche du guide consiste à savoir comment (1) **identifier** les campagnes de manipulation de l'information en cours, (2) élaborer des **réponses** en temps réel et à court terme et (3) **développer la résilience à long terme** face à la manipulation de l'information. Bien que nous décrivions trois étapes distinctes dans ce guide, le processus de lutte contre la manipulation de l'information est circulaire et chaque étape se chevauche et se renforce les unes les autres. Les délais de planification varieront en fonction du contexte, mais, dans la mesure du possible, nous encourageons une planification proactive plutôt que réactive pour contrer efficacement la manipulation des informations électorales. La stratégie en trois parties de ce guide peut vous aider à développer des réponses rapides et en temps réel, ainsi qu'à établir des approches à long terme et durables pour développer la résilience afin de maintenir l'intégrité des élections et de renforcer les processus démocratiques.



Contexte : Comprendre la manipulation de l'information

Comment utiliser cette section

Cette section présente les composantes de la manipulation de l'information et définit les termes couramment utilisés.

Qu'est-ce que la manipulation de l'information

La manipulation de l'information est ***un ensemble de tactiques impliquant la collecte et la diffusion d'informations afin d'influencer ou de perturber la prise de décision démocratique***. Bien que la manipulation de l'information puisse utiliser les canaux d'information traditionnels - tels que la télévision, la presse écrite ou la radio - nous nous concentrons ici sur les aspects numériques de la manipulation de l'information. Nous examinons dans ce guide comment les campagnes de manipulation de l'information choisissent plusieurs ***vecteurs*** numériques, sont dirigées par des ***acteurs*** variés et utilisent un ensemble de ***tactiques*** pour diffuser différents types de ***contenu***.

Acteurs de la menace

Dans la plupart des environnements électoraux, un certain nombre d'acteurs différents sont susceptibles de créer de la manipulation de l'information. Pour compliquer davantage les choses, si certains de ces acteurs agissent de manière indépendante, d'autres agissent en coordination, vont à contre-courant ou profitent du chaos général et du manque de confiance dans l'environnement informationnel. Les différents acteurs ont des raisons diverses de perpétrer de la manipulation de l'information. Une campagne politique vise à remporter une élection ; le secteur de l'influence et les sociétés de relations publiques commerciales veulent gagner de l'argent ; un adversaire étranger peut tenter d'influencer le résultat d'une élection, de favoriser des intérêts nationaux ou de semer le chaos ; enfin, un groupe extrémiste peut chercher à promouvoir sa cause politique. Nous avons présenté ici les principaux acteurs de la menace impliqués dans les campagnes de manipulation de l'information. Bien que cette liste ne soit pas exhaustive, elle constitue un point de départ pour réfléchir aux acteurs pertinents dans le contexte de votre propre pays.

- Les **partis et les campagnes politiques** utilisent la manipulation de l'information pour discréditer l'opposition, amplifier faussement des contenus pour atteindre un public plus large ou suggérer qu'ils ont plus de soutien public qu'en réalité, ou manipuler le discours politique d'une manière qui profite au programme de leur campagne. Il est important de noter que les campagnes politiques peuvent avoir recours à la manipulation de l'information en dehors et pendant les cycles électoraux.

- Les **groupes haineux et autres groupes extrémistes** utilisent la manipulation de l'information pour promouvoir leur programme social ou politique, souvent en fomentant la haine et la polarisation politique, en réduisant au silence, en intimidant ou en privant de leurs droits des groupes cibles et en incitant à la violence. Leurs objectifs peuvent être de retourner l'électorat majoritaire contre un groupe particulier, d'accroître le soutien aux politiques extrémistes et/ou de supprimer la participation politique.

- Les **gouvernements étrangers** utilisent la manipulation de l'information comme un instrument de maitrise politique et géopolitique. La manipulation de l'information peut servir à influencer le résultat d'une élection dans un pays stratégiquement important, à promouvoir les intérêts du gouvernement ou à façonner la perception de l'État à l'étranger. La manipulation de l'information peut être déguisée (par exemple, par l'utilisation de faux comptes) ou ouverte (par exemple, par des médias soutenus par l'État).

- Les **gouvernements nationaux** utilisent la manipulation de l'information pour influencer l'attitude du public et supprimer la participation ou l'expression politique de certaines personnes, tels que les activistes, les journalistes ou les opposants politiques. À l'instar des États étrangers, les gouvernements peuvent avoir recours à la manipulation de l'information ouverte et déguisée pour atteindre des objectifs politiques, notamment la répression des droits de l'homme. Les gouvernements nationaux peuvent également adopter plus facilement la censure comme forme de manipulation de l'information.

- Les **acteurs commerciaux**, parmi lesquels les plateformes de réseaux sociaux, les sociétés de relations publiques ou entreprises de communication stratégique, utilisent la manipulation de l'information dans le cadre d'un modèle économique, en collaborant avec d'autres acteurs pour diffuser la désinformation à des fins lucratives. Le secteur de l'influence collabore souvent avec des campagnes politiques, des gouvernements ou des États étrangers pour soutenir leurs objectifs particuliers.

- Les **médias non indépendants** qui ont un agenda politique ou un intérêt économique spécifique, ou qui sont soutenus par un gouvernement ou un autre acteur politique, peuvent utiliser la manipulation de l'information pour influencer l'attitude du public conformément aux objectifs de leurs bailleurs de fonds.

Il peut être difficile de déterminer qui est à l'origine de la manipulation de l'information, surtout lorsque les objectifs des

différents acteurs se chevauchent. Par exemple, un acteur étatique étranger pourrait amplifier le contenu produit par des groupes haineux nationaux ou des théories du complots. D'autre part, les utilisateurs qui créent un contenu attrayant et mettent des publicités sur leurs pages sont exposés à des incitations commerciales à produire de la més/désinformations dont la viralité pourrait générer des revenus.

Il existe de nombreuses façons de catégoriser les types d'acteurs de la menace impliqués dans les campagnes de manipulation de l'information. Les dichotomies de la désinformation[1] de DFRLab peuvent vous aider à réfléchir plus en détail aux types d'acteurs et aux motivations qui se cachent derrière la manipulation de l'information

Contenu

La manipulation de l'information fait usage d'une variété de contenus pour influencer, perturber ou déformer l'écosystème de l'information. Ce contenu peut être utilisé pour influencer les attitudes ou les croyances du public, persuader les individus d'agir ou de se comporter d'une certaine manière - comme empêcher le vote d'un groupe particulier de personnes - ou inciter à la haine et à la violence. La manipulation de l'information peut apparaitre dans de nombreux types de contenus. Nous présentons ici quelques termes clés utilisés dans ce rapport et par d'autres chercheurs, activistes et praticiens qui étudient et combattent la manipulation de l'information.

- La **mésinformation** est une information fausse, inexacte ou trompeuse, indépendamment de l'intention de tromper.
- La **désinformation** est la création, la diffusion et/ou l'amplification délibérée d'informations fausses, inexactes ou trompeuses avec l'intention de tromper.
- La **malinformation** utilise des informations véridiques ou factuelles et les utilise à des fins de persuasion. Il peut s'agir, par exemple, de contenus publiés dans le cadre d'une opération de piratage et fuitage (*hack-and-leak*), où des messages privés sont partagés publiquement dans le but de nuire à un adversaire.
- La **propagande** est une information destinée à promouvoir un objectif, une action ou un résultat politique. La propagande implique souvent la désinformation, mais elle peut aussi utiliser des faits, des informations volées ou des demi-vérités pour influencer les individus. Elle fait souvent appel aux émotions, plutôt que de se concentrer sur des pensées ou des arguments rationnels. La propagande peut être utilisée par différents acteurs, mais dans ce rapport, nous nous concentrons spécifiquement sur la propagande orchestrée par l'État.
- Le **discours haineux** est l'utilisation d'un langage discriminatoire à l'égard d'une personne ou d'un groupe sur la base de son identité, notamment sa religion, son ethnicité, sa nationalité, son handicap, son sexe ou son orientation sexuelle. Les discours haineux font souvent partie d'efforts plus larges de manipulation de l'information. Ils sont particulièrement présents dans les contextes électoraux où l'objectif de la manipulation de l'information est de polariser le discours politique et/ou d'empêcher la participation politique d'un groupe particulier.

Il existe de nombreuses autres façons de catégoriser les types de contenu impliqués dans la manipulation de l'information. Pour des ressources supplémentaires, veuillez vous référer au rapport intitulé Information Disorder : Toward an Interdisciplinary Framework for Research and Policy Making, commandé par le Conseil de l'Europe et produit en coopération avec First Draft et le Shorenstein Center on Media, Politics and Public Policy de l'Université de Harvard.[2]

Tactiques

La manipulation de l'information fait appel à une variété de tactiques pour diffuser, amplifier ou cibler des messages à différents publics sur les réseaux sociaux. Nombre de ces tactiques exploitent les caractéristiques des technologies numériques et des réseaux sociaux pour diffuser différents types de contenus. Si la manipulation des médias n'est pas nouvelle, les tactiques numériques peuvent modifier la portée, l'échelle et la précision de la manipulation de l'information de diverses manières. Nous définissons ici certaines des tactiques clés identifiées par les chercheurs, les journalistes, les activistes et les entreprises de plateformes.

[1] Emerson T. Brooking, *Dichotomies of Disinformation*, (Laboratoire d'analyses scientifiques Digital Forensic Research Lab de Atlantic Council, février 2020), https://github.com/DFRLab/Dichotomies-of-Disinformation.

[2] Claire Wardle et Hossein Derakhshan, Information Disorder : Toward an Interdisciplinary Framework for Research and Policymaking (Conseil de l'Europe, 31 octobre 2017), https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/.

- La **technologie générée par l'IA** est utilisée dans la manipulation de l'information pour créer de faux profils ou contenus. Les technologies d'IA, comme les réseaux antagonistes génératifs (GAN), utilisent des « réseaux neuronaux » de machine learning pour créer des images ou des vidéos qui ressemblent à des personnes réelles mais qui sont totalement fausses. Cela inclut les vidéos hypertruquées « deepfake », qui ont recours aux technologies d'IA pour créer des vidéos d'apparence réaliste qui sont entièrement fausses.

- Le **contenu visuel manipulé** consiste à manipuler de l'information en photoshopant des images ou en éditant des vidéos. Il peut s'agir de simples trucages ou « cheap fakes », qui n'utilisent pas de technologies générées par l'IA, mais modifient plutôt des vidéos avec un niveau de sophistication technique inférieur.

- La **manipulation des moteurs de recherche** consiste à utiliser des outils de publicité numérique, comme le placement de mots clés, pour exploiter les lacunes des résultats de recherche. Ces stratégies tentent de placer la désinformation en tête des requêtes des moteurs de recherche, de sorte que les personnes recherchant des informations exactes sont plus susceptibles de tomber sur de la désinformation.

- Les **faux sites web** sont utilisés pour créer la substance derrière une campagne de manipulation d'influence au moyen de sites web de « fake news » ou de fermes de contenu qui publient de grandes quantités d'histoires fausses, trompeuses ou inexactes, parfois en contrefaisant de véritables organismes de presse.

- Le **trolling** est le fait d'intimider ou de harceler des personnes pour provoquer une réaction émotionnelle chez la cible. Si tout le monde peut être victime de trolling en ligne, certaines communautés le vivent différemment et souvent plus durement. Cela inclut les femmes, les personnes ayant des identités de genre diverses, les minorités raciales ou ethniques ou les personnes racisées.

- La **propagande informatique** implique l'utilisation de robots logiciels ou « bots » et d'autres formes de technologies automatisées pour amplifier la propagande et d'autres contenus nuisibles en ligne. Les bots sont des morceaux de code conçus pour imiter le comportement humain en aimant, partageant, retweetant ou même en commentant des messages. Ils peuvent être utilisés pour amplifier faussement certains types de contenus ou de comptes en ligne.

- Les **faux comptes ou « faux-nez »** sont des comptes gérés par de vraies personnes, qui génèrent un engagement inorganique. Comme les bots, les faux comptes ou les faux-nez peuvent aimer, partager, retweeter ou commenter des messages pour amplifier faussement certains types de contenus ou de comptes en ligne. Mais plutôt que d'être automatisés, les faux comptes ou les « faux-nez » sont gérés par de vraies personnes.

- Les **opérations de piratage et de fuitage (hack-and-leak)** consistent à pirater des sources d'information privées ou sensibles et à divulguer stratégiquement des informations au public afin de saper la confiance ou l'intégrité d'une personne ou d'une idée.

- La **prise de contrôle de comptes** consiste à pirater les comptes de personnes réelles afin d'usurper leur identité ou de diffuser de la més/désinformation à un large public.

- La **publicité et le microciblage** consistent à utiliser des plateformes publicitaires en ligne pour collecter des données sur les utilisateurs et les cibler avec des messages persuasifs.

- La **censure** consiste à bloquer, rediriger ou limiter l'accès à certains types d'informations en ligne.

De nombreux types de tactiques peuvent être utilisés pour manipuler l'écosystème de l'information numérique. Ces tactiques dépendront de la plateforme utilisée, des compétences des personnes impliquées et du contexte national unique dans lequel se déroule la manipulation des informations. Pour plus d'informations sur les types de tactiques utilisées dans les campagnes de manipulation de l'information, voir le document Disinformation Primer de l'USAID. [3]

Vecteurs

L'écosystème de l'information a radicalement changé au cours des trois dernières décennies. Internet et les réseaux sociaux en particulier ont créé un environnement dans lequel la manipulation de l'information est extrêmement extensible, très bon marché et très malléable.

[3] USAID et National Democratic Institute, *Countering Disinformation : A Guide to Promoting Information Integrity*, (Consortium for Elections and Political Process Strengthening, 2021), https://pdf.usaid.gov/pdf_docs/PA00XFKF.pdf.

Comportement trompeur organisé et campagnes d'information

Les entreprises de réseaux sociaux tentent de prendre davantage de mesures pour lutter contre la manipulation des informations sur leurs plateformes. Lorsqu'ils font référence à la manipulation de l'information, ils utilisent des termes comme « comportement trompeur organisé » sur Facebook ou « campagnes d'information » sur Twitter. Bien que les termes désignant la manipulation de l'information et leurs tactiques diffèrent selon les plateformes, les plateformes de réseaux sociaux prennent de plus en plus de mesures contre les réseaux de faux comptes qui diffusent de la désinformation, incitent à la violence ou portent atteinte à l'intégrité des élections. L'un des éléments essentiels des définitions des plateformes concernant la manipulation de l'information est l'utilisation de faux comptes ou de faux-nez qui se font passer pour quelqu'un d'autre, comme un acteur d'un État étranger se faisant passer pour un citoyen d'un autre pays.

Depuis 2018, Twitter et Facebook ont publié davantage de données sur la manipulation d'informations sur leurs plateformes dans leurs blogs ou dans le Centre de transparence sur les campagnes d'information de Twitter.[4] Vous trouverez également des liens vers des ressources qui peuvent vous aider à identifier les campagnes coordonnées de manipulation de l'information à la section Étape 1 : Identification. Cependant, il est important de noter que les définitions utilisées par les plateformes pour supprimer la manipulation d'informations ont des limites. Par exemple, lorsque des réseaux d'utilisateurs réels partagent des informations trompeuses sur une élection, il peut s'avérer beaucoup plus difficile pour les plateformes de prendre des mesures contre des utilisateurs authentiques plutôt que contre des faux comptes. C'est pourquoi il est important à la fois de réagir et de renforcer la résilience face à la manipulation de l'information grâce au fact-checking, à l'éducation aux médias et à la mise en place de réseaux de collaboration, afin que les utilisateurs réels soient moins susceptibles de partager des informations nuisibles, inexactes ou trompeuses. Vous pouvez en savoir plus sur ces stratégies aux sections Étape 2 : Réponse et Étape 3 : Renforcement de la résilience.

Si les **plateformes de réseaux sociaux populaires** - telles que Facebook, Twitter et YouTube - sont souvent mises en avant comme vecteurs de manipulation de l'information, ce type d'activité se produit également sur **d'autres plateformes de réseaux sociaux** comme Reddit, Pinterest, Instagram, TikTok, Tumblr et WeChat. On les retrouve également sur des **plateformes de messagerie cryptées et non cryptées** comme LINE, Telegram, WhatsApp, Facebook Messenger, Signal ou Viber. (Pour plus d'informations sur la conduite d'enquêtes éthiques en milieu fermé, rendez-vous à la section Étape 2 : Réponse.) Certaines manipulations d'informations peuvent viser les **moteurs de recherche sur Internet**, comme Google, Yahoo ou Bing. D'autres **ciblent des communautés particulières** d'utilisateurs, comme les joueurs, par le biais de plateformes telles que Twitch, Xbox Live ou PlayStation Online. Alors que les principales plateformes de réseaux sociaux ont redoublé d'efforts pour fixer des limites à la diffusion de contenus préjudiciables, de nouvelles plateformes ont été créées. Certaines de ces plateformes s'attachent à créer des environnements non modérés et d'autres ont mis en place des politiques de modération qui favorisent explicitement le discours d'une idéologie par rapport à une autre, souvent en mettant l'accent sur des opinions politiques particulières ou extrémistes.

La manipulation de l'information se produit presque toujours à la fois en ligne et hors ligne : la télévision, la radio, la presse écrite, le milieu académique et d'autres domaines de l'écosystème de l'information peuvent être impliqués. Par exemple, les journalistes ou les médias peuvent amplifier un contenu créé dans le cadre d'une campagne de manipulation de l'information si ce contenu a été partagé par une personnalité politique importante, ou s'il est particulièrement sensationnel et susceptible d'attirer l'audience. Un acteur sophistiqué qui commet de la manipulation de l'information peut s'emparer d'organes d'information de premier plan ou accorder des subventions à des organismes de recherche pour qu'ils produisent des analyses qui soutiennent ses objectifs.

[4] Centre de Transparence de Twitter, « Campagnes d'information », (Twitter, s.d.), https://transparency.twitter.com/en/reports/information-operations.html.

Nouveaux défis pour la manipulation de l'information

La manipulation de l'information s'adapte constamment aux changements de l'écosystème médiatique. Les entreprises de réseaux sociaux s'améliorent pour détecter et supprimer la manipulation de l'information sur leurs plateformes, mais néanmoins les acteurs de la menace ont également appris à modifier leurs stratégies, leurs outils et leurs tactiques. Initialement, les chercheurs s'inquiétaient de l'utilisation de bots politiques pour amplifier la més/désinformation sur les plateformes de réseaux sociaux, mais aujourd'hui la distinction entre les comptes de bots automatisés et les contenus créés par des humains est de moins en moins claire. La montée en puissance de divers acteurs commerciaux proposant la désinformation en tant que service rend également plus difficile pour les entreprises de réseaux sociaux de détecter les manipulations de l'information et de prendre des mesures à leur encontre, car les trolls à louer sont payés pour polluer la sphère de l'information. Par ailleurs, la distinction entre les campagnes d'information étrangères et l'extrémisme ou le terrorisme national est de moins en moins claire, car l'ingérence étrangère sélectionne de plus en plus les récits nationaux pour amplifier les divisions raciales, de genre ou politiques préexistantes.

Alors que les plateformes disposent de politiques pour l'authenticité visant à supprimer les comportements *trompeurs* organisés, en août 2021, il n'existe pas de directives claires pour gérer les comportements *authentiques* organisés. Lorsque des plateformes grand public et omniprésentes dans le monde entier, comme Facebook, Twitter, TikTok ou YouTube, prennent des mesures à l'encontre de contenus et de comptes, ces voix réapparaissent parfois sur d'autres plateformes ou sur des chaînes privées qui ne disposent pas des mêmes normes pour supprimer les contenus ou les comptes qui diffusent de la més/désinformation, des discours haineux ou qui incitent à la violence. Et certaines plateformes, comme WhatsApp ou Signal, cryptent les messages personnels et des groupes, ce qui rend beaucoup plus difficile la détection des campagnes d'information et la lutte contre la diffusion de més/désinformations et d'autres formes d'informations nuisibles. Si le cryptage peut protéger la vie privée et la sécurité des activistes et des défenseurs des droits de l'homme en ligne, des acteurs malveillants ont tiré parti de la sécurité de ces plateformes pour renforcer la diffusion d'informations nuisibles ou trompeuses en ligne.

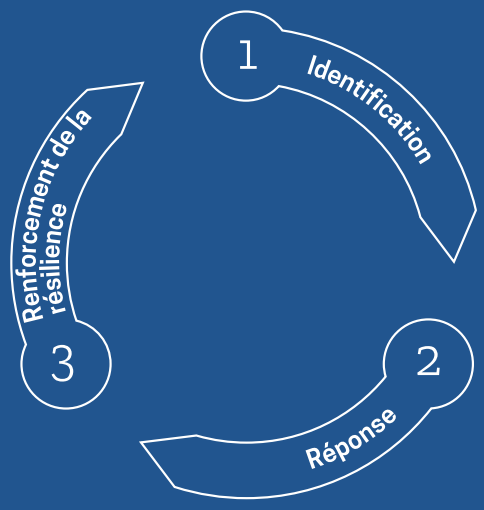
En même temps, tout le monde ne vit pas la manipulation de l'information de la même manière. Les journalistes, les activistes politiques et les membres de l'opposition politique sont fréquemment la cible de campagnes de diffamation et de harcèlement visant à saper leur crédibilité et leur légitimité professionnelle. Ces campagnes sont souvent plus graves pour les femmes, les minorités ou les personnes racisées, qui sont confrontées à des niveaux plus élevés de harcèlement, de menaces en ligne et de sexualisation. Les populations minoritaires ou marginalisées sont également souvent la cible d'une violence en ligne qui peut avoir des répercussions concrètes sur leur sécurité et leur sûreté, car les discours en ligne peuvent avoir une incidence sur la violence politique hors ligne.

Enfin, la technologie elle-même est en constante évolution et les nouvelles innovations créent de nouvelles possibilités de manipulation de l'information. L'intelligence artificielle (IA) a ouvert la voie à de nombreuses possibilités de tromperie en ligne : les comptes bots automatisés peuvent utiliser des algorithmes de machine learning (comme GPT-3) pour paraître plus humains ; les réseaux antagonistes génératifs (GAN) peuvent être utilisés pour créer de fausses photos de profil qui ressemblent à de vraies personnes ou d'autres formes de médias synthétiques comme les vidéos « deepfake ». Par exemple, les vidéos « deepfake » sont utilisées pour représenter trompeusement des femmes dans de la pornographie, ce qui peut avoir des effets dommageables et durables sur leur santé mentale et leurs perspectives de carrière. Les innovations en matière de surveillance des données posent également de nouveaux défis en matière de manipulation des informations, car il devient beaucoup plus facile de cibler des communautés ou des individus spécifiques avec des messages persuasifs. Les données relatives aux préférences et aux intérêts des utilisateurs peuvent être utilisées pour prédire les valeurs et les comportements d'individus ou de groupes et les acteurs commerciaux élaborent déjà des modèles pour cibler des communautés de personnes avec des messages de (dé)mobilisation. Les données pouvant être utilisées dans la manipulation de l'information ne feront que croître à mesure que l'Internet des objets introduit davantage de points de données sur les utilisateurs par le biais de dispositifs portables, voitures, appareils et capteurs intelligents. Nous devons faire évoluer nos réponses pour suivre le rythme de ces innovations et renforcer notre capacité de résilience face aux futures manipulations de l'information.

Identifier, répondre et renforcer la résilience face à la manipulation de l'information

Comment utiliser cette section

Une fois que vous avez compris les aspects fondamentaux de la manipulation de l'information, l'étape critique suivante consiste à acquérir une compréhension et un ensemble de compétences pour identifier les risques futurs et les campagnes en cours dans le contexte de votre propre pays. L'identification des campagnes en cours, ainsi que des risques futurs, est l'une des étapes les plus difficiles, car les acteurs malveillants masquent souvent leur identité et créent des obstacles à l'attribution technique d'une campagne. Pour vous aider dans ce processus, cette section présente quelques stratégies clés. Nous avons également dressé une liste de ressources utiles et accessibles pour vous aider tout au long du processus d'identification.



Étape 1 Identification

Cartographie de l'environnement de l'information

La première étape pour identifier la manipulation de l'information consiste à cartographier l'environnement de l'information afin d'identifier les vulnérabilités propres à votre élection. Vous devez procéder à une évaluation des risques qui identifie les différents acteurs de la menace susceptibles de lancer une campagne de manipulation de l'information et les canaux - y compris numériques, de diffusion, de radio ou de presse écrite - qui pourraient être utilisés dans le cadre de leurs efforts. Vous devrez également identifier les différents partenaires avec lesquels vous travaillerez pour lutter contre les menaces qui se présentent, tels que les représentants politiques des entreprises de réseaux sociaux, les représentants du gouvernement, les organismes chargés de l'application de la loi ou d'autres organisations de la société civile (OSC). Cette section donne un aperçu des questions clés auxquelles il faut répondre pour cartographier l'environnement de l'information.

- **Quel est le paysage médiatique et de l'information ?**
  La première étape de la *cartographie de l'environnement de l'information* consiste à comprendre votre paysage médiatique actuel. Où les gens obtiennent-ils les informations politiques ? Où la manipulation de l'information est-elle susceptible de survenir ? A cette étape, vous devez vous pencher sur les entités médiatiques traditionnelles comme les chaînes de télévision, les journaux et les stations de radio et évaluer la transparence de la propriété des médias, la correction politique et les normes professionnelles appliquées par les médias. Vous devez également prendre en compte les médias numériques, tels que les plateformes de réseaux sociaux, les applications de chat cryptées ou les forums web. Familiarisez-vous avec les politiques des plateformes sur lesquelles vous soupçonnez que des campagnes d'information pourraient avoir lieu, examinez leurs conditions d'utilisation et leur réglementation communautaire, ainsi que d'autres mesures spécifiques au pays qui pourraient avoir été annoncées dans les blogs des plateformes. Vous devez également vous familiariser avec les initiatives de vérification des informations existantes et le rôle d'autres influenceurs en ligne dans l'élaboration du discours politique pour certaines communautés d'utilisateurs.

- **Où se trouvent les audiences en ligne et quelles communautés d'utilisateurs sont plus vulnérables à la manipulation de l'information ou aux implications négatives de ces campagnes ?**
  La manipulation de l'information affecte les utilisateurs différemment et les femmes, les personnes racisées et les personnes ayant des identités de genre et des orientations sexuelles différentes en font l'expérience plus sévèrement que les autres.[5] La deuxième étape de la cartographie de l'environnement de l'information consiste à comprendre vos publics et les groupes de personnes qui pourraient être marginalisés, privés de participation ou profondément affectés par les efforts de manipulation de l'information en cours. Cela implique d'examiner de près les petites communautés et les communautés locales dans le contexte de votre pays.

- **Qui sont les acteurs probables de la menace ?**
  La troisième étape de la *cartographie de l'environnement de l'information* consiste à identifier les différents acteurs de la menace et à comprendre leurs motivations à manipuler l'information. Comprendre qui est, ou pourrait être, à l'origine de la manipulation des informations vous aidera à réagir et à renforcer la résilience face aux futures campagnes. Demandez-vous : Qui sont les principaux acteurs de la menace - s'agit-il d'acteurs nationaux, d'États étrangers ou des deux ? Quelles pourraient être les motivations derrière ces campagnes - s'agit-il de perturbations politiques ou de gains économiques ? Voir la section Contexte pour plus d'informations sur les acteurs de la menace et leurs motivations à manipuler l'information.

- **Qui sont les partenaires avec lesquels vous pouvez travailler pour lutter contre la manipulation de l'information ?**
  La quatrième étape de la *cartographie de l'environnement de l'information* consiste à identifier les partenaires qui peuvent vous aider à lutter contre la manipulation de l'information. Dans ce cas, vous devriez envisager d'identifier les partenaires gouvernementaux et non gouvernementaux pertinents, tels que les organismes de gestion des élections, qui pourraient être en mesure d'aider à répondre aux campagnes de manipulation de l'information en cours. Les

[5] National Democratic Institute, *Tweets that Chill : Analyzing Online Violence Against Women in Politics* (NDI, 14 juin 2019), https://www.ndi.org/tweets-that-chill.

journalistes et autres OSC de votre pays peuvent travailler avec vous pour vérifier les informations ou fournir un contre-message en cas de manipulation de l'information. Vous devez également identifier des contacts sur les plateformes de réseaux sociaux avec lesquels vous pouvez travailler pour supprimer du contenu ou des comptes des réseaux sociaux. Il est important de noter que tous les partenaires ne seront pas pertinents pour tous les contextes. L'important est d'identifier qui apportera des compétences, des ressources ou des capacités pour vous aider à réagir et à renforcer la résilience face à la manipulation de l'information. Pour vous aider à identifier les partenaires pertinents, vous pouvez explorer la base de données du guide Countering Disinformation.[6]

- **Quelles sont les réglementations pertinentes à connaître dans le cadre de vos recherches et pour la rédaction de vos rapports ?**
  Chaque pays aura des lois ou des règlements différents concernant les élections, les campagnes et les discours en ligne. La cinquième étape de la cartographie de l'environnement de l'information consiste à comprendre le paysage juridique et réglementaire de votre pays en ce qui concerne les questions liées à l'environnement de l'information électorale. La connaissance de ces règles vous préparera à mieux travailler avec les agences gouvernementales pour répondre ou renforcer la résilience face à la manipulation de l'information, ou pour vous protéger, ainsi que vos collègues et votre organisation, lorsque vous déciderez de la meilleure façon de réagir. Par exemple, certains gouvernements peuvent avoir des règlements qui interdisent de faire campagne trois jours avant une élection. Il peut également exister des règles ou des réglementations concernant l'achat de publicités étrangères. La connaissance des réglementations pertinentes peut vous aider à signaler les contenus illicites aux régulateurs et aux organismes de gestion des élections, ainsi qu'aux plateformes de réseaux sociaux pour qu'ils les suppriment.

Conseil : N'oubliez pas les plateformes régionales et locales

Dans ce guide, nous citons les principales plateformes de réseaux sociaux mondiales, mais sachez qu'il existe également de nombreuses autres plateformes régionales et locales. Le partage de contenu manipulé entre plateformes est courant, et vous observerez que des informations partagées sur une plateforme le sont aussi sur d'autres. Nous vous conseillons de faire une plongée en profondeur dans votre écosystème d'information local et d'observer quelles plateformes de réseaux sociaux sont largement utilisées et comment elles sont liées les unes aux autres. En plus de vos propres observations, les rapports We Are Social[7] sur l'utilisation des réseaux sociaux par pays s'avère une ressource utile pour vous aider à cartographier le paysage de l'information. L'inventaire Global Cyber Troops[8] donne également un aperçu de la manipulation de l'information par pays et des différents vecteurs utilisés dans les campagnes de manipulation de l'information.

Identifier les récits de manipulation de l'information courants

Après avoir compris l'environnement informationnel dans lequel vous allez travailler, vous pouvez commencer à réfléchir aux types de récits ou de thèmes que les différents acteurs pourraient utiliser dans leurs campagnes de manipulation de l'information. Pour vous aider à les identifier, nous avons décrit les récits courants utilisés dans les campagnes d'information pendant les élections.

- Les **contenus polarisant et séparatistes** sont parfois utilisés dans les campagnes de manipulation de l'information pour attiser les divisions politiques, raciales, religieuses,

[6] International Foundation for Electoral Systems, International Republican Institute, National Democratic Institute, « Database of Informational Interventions » (Consortium for Elections and Political Process Strengthening, 2021), https://counteringdisinformation.org/index.php/interventions.

[7] We Are Social, « Digital in 2020 » (2020), https://wearesocial.com/digital-2020.

[8] Samantha Bradshaw, Hannah Bailey et Philip Howard, « Industrialized Disinformation : 2020 Global Inventory of Organized Social Media Manipulation », Computational Propaganda Research Project (Oxford Internet Institute, 13 janvier 2021), https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/.

culturelles ou entre les genres. Ces récits se concentrent souvent sur les divisions préexistantes au sein de la société et utilisent des récits identitaires pour semer la discorde et le mécontentement au sein de l'électorat.

- Les **récits de délégitimation** diffusent des contenus qui sapent l'intégrité du processus électoral. Il peut s'agir de fausses déclarations concernant la sécurité des machines à voter, d'erreurs dans le processus de vote ou le dépouillement des bulletins, ou d'autres irrégularités présumées. Ces récits sont conçus pour semer la méfiance dans les processus qui soutiennent les élections. Les récits de délégitimation peuvent également avoir pour objectif de discréditer certains politiciens ou candidats, agents électoraux ou entités civiques.

- Les récits de **suppression politique** sont utilisés pour décourager certains groupes de personnes de participer à la politique. Ces stratégies de suppression visent les processus démocratiques ; il peut s'agir de diffuser des informations erronées sur la manière de voter et sur le lieu du vote, de suggérer que certaines communautés d'individus ne sont pas autorisées à voter ou qu'il y a de la violence dans les bureaux de vote. Ils peuvent également inclure des récits incitant les électeurs à assister ou non à des rassemblements ou à des événements politiques, ou qui encouragent la fraude électorale.

- La **haine, le harcèlement et la violence** sont une autre forme de suppression qui utilise le harcèlement, la diffamation ou les menaces de violence pour décourager certains utilisateurs ou communautés d'exprimer leurs pensées ou opinions en ligne ou de participer aux débats nécessaires au bon fonctionnement de la démocratie. La haine, le harcèlement et la violence créent une culture de la peur et peuvent étouffer l'expression politique en ligne.

- Des **résultats électoraux prématurés ou des proclamations de victoire** sont parfois diffusés sur les réseaux sociaux afin de saper la confiance dans le résultat de l'élection. Cela se produit souvent avant la fin du dépouillement des bulletins de vote et tout particulièrement si une course politique est serrée et controversée.

De nombreux types de récits peuvent émerger pendant une élection et bon nombre d'entre eux seront spécifiques au contexte de votre pays. Il est important de réfléchir aux types de récits susceptibles d'être utilisés dans le cadre de campagnes de manipulation de l'information, afin d'être mieux préparé à répondre avec des contre-messages ou à renforcer la résilience face aux récits avant qu'ils ne se propagent. L'inventaire Global Cyber Troops[9] du Computational Propaganda Project décrit d'autres types de récits ou de « stratégies de communication » qui ont été observés dans les campagnes de manipulation de l'information à travers le monde.

Identifier les efforts de manipulation de l'information existants

Une fois que vous avez cartographié l'environnement de l'information et compris les différents types de récits que les acteurs peuvent utiliser pour porter atteinte à l'intégrité des élections, vous devez commencer à surveiller l'écosystème des campagnes en cours. Les acteurs de la menace tentent souvent de dissimuler leur identité ou leurs campagnes afin d'éviter d'être détectés. Cependant, il existe un certain nombre de ressources et de bonnes pratiques pour identifier les campagnes en cours, que nous avons compilées pour vous. Vous devez également tenir compte de ces cinq principes clés lorsque vous menez des enquêtes sur la manipulation d'informations.

Cinq principes clés

1. **Le contexte est important.** Chaque pays et chaque élection se déroule dans un environnement médiatique, culturel, social et économique différent. Il est important de cartographier votre écosystème d'information et les menaces probables afin de se concentrer sur les technologies et les plateformes pertinentes qui sont prédominantes dans votre pays.

2. **Connaitre ses limites**. Toute recherche sur la manipulation de l'information a ses limites et les données recueillies sur ce type de campagnes sont toujours imparfaites. Il est important de comprendre ce que vous savez et ne savez pas sur la manipulation des informations en fonction des données avec lesquelles vous travaillez et de ne pas tirer de conclusions hâtives sur l'authenticité des informations en ligne. Il peut être tout aussi préjudiciable pour la légitimité d'une élection d'attribuer de la manipulation d'informations de manière erronée.

[9] Bradshaw, Bailey et Howard, « Industrialized Disinformation : 2020 Global Inventory of Organized Social Media Manipulation ».

3. **Le comportement prime sur le contenu.** Pour identifier les manipulations d'informations, il est important d'examiner les schémas de comportement des comptes, plutôt que de s'intéresser à un seul élément de contenu. Les plateformes sont mieux à même de réagir aux comportements trompeurs organisés et l'identification de vastes réseaux de comptes coordonnés pour manipuler l'environnement d'information en ligne fournira une base plus solide pour supprimer des contenus et des comptes.

4. **Ne pas causer de dommage.** La collecte, le stockage et l'utilisation de données en ligne peuvent avoir des répercussions sur la vie privée et la sécurité des personnes et il est important que toute collecte d'informations visant à surveiller la manipulation des informations soit effectuée de manière éthique. Les données en ligne peuvent s'accompagner d'attentes en matière de respect de la vie privée et les réflexions sur le consentement, la sécurité et la confidentialité est une partie importante de votre travail d'enquêteur. Mal stocker ou anonymiser les données peut avoir des conséquences négatives sur la vie privée ou la sécurité des utilisateurs qui participent à la vie politique en ligne. Il est donc important de prendre les mesures nécessaires pour ne pas causer de dommage et pour protéger et sécuriser les données avec lesquelles vous travaillez.

5. **Tolérance zéro pour la haine, la répression et la violence.** La haine ou l'incitation à la violence en ligne peuvent avoir des conséquences concrètes non seulement sur l'intégrité des élections, mais aussi sur la sécurité des citoyens. Ces récits ne proviennent pas toujours de comptes trompeurs organisés ou de campagnes d'information formalisées, mais peuvent être partagés par des utilisateurs authentiques ou réels. Cependant, toute information qui propage la haine, tente d'empêcher la participation ou le discours politique, ou incite à la violence doit être immédiatement signalée aux plateformes et aux autres parties concernées, quelle que soit la source. Vous trouverez de plus amples informations sur la manière de signaler du contenu dans la section « Signalement » à l'Étape 2 : Réponse.

Conseil : Identifier la manipulation de l'information

Gardez à l'esprit que les campagnes de manipulation de l'information peuvent se dérouler aussi bien hors ligne que sur des plateformes en ligne ; les médias grand public (tels que la télévision, la radio et les journaux) sont des vecteurs courants de diffusion de fausses informations et vous devez garder les principes ci-dessus à l'esprit lorsque vous consommez des informations provenant de sources hors ligne également. Veillez à vérifier les informations que vous entendez ou voyez avant de les partager avec vos réseaux de confiance et les membres de votre organisation. Étant donné que les médias grand public ont souvent des partis pris intentionnels, ils peuvent parfois présenter de fausses informations ou des « demi-vérités » (voir la section Éducation à la culture numérique à l'Étape 3 : Renforcement de la résilience).

Outils Open Source Intelligence (OSINT) pour identifier la manipulation de l'information

L'OSINT est une technique de collecte et d'analyse d'informations provenant de sources publiques (ouvertes). Ces ressources peuvent être utilisées pour suivre et identifier la désinformation.

La boîte à outils d'investigation en ligne de Bellingcat : *(Liste de ressources)* Cette feuille de calcul Google Doc facile à parcourir comporte différents onglets pour différents outils de vérification des informations, tels que la vérification des images et des vidéos; les contenus et comptes des réseaux sociaux; les numéros de téléphone et services de messagerie fermés; les cartes et services de localisation ; les trackers de transpor ; l'analyse des adresses IP et des sites web; les entreprises internationales; l'environnement; les outils d'amélioration de la sécurité en ligne, de la confidentialité et de la visualisation des données ; les ressources universitaires ; et des guides supplémentaires.[10]

Le manuel de Data Journalism pour la désinformation et la manipulation des médias : *(Guide)* Ce manuel vous aide à mener des recherches OSINT sur les comptes de réseaux sociaux, la détection des bots et la manipulation des images. Il fournit également des ressources pour mener des enquêtes sur le web et entre les plateformes, ainsi que des conseils et des outils pour l'attribution d'une campagne.[11]

Le manuel de surveillance des médias de Beacon Project : *(Guide)* Ce manuel vous aide à effectuer des analyses fondées sur des données des récits de désinformation et de leurs sources. Le manuel est un bon point de départ pour les chercheurs intéressés par l'observation des médias, mais qui ne savent pas par où commencer, ainsi que pour ceux qui cherchent à s'assurer que les meilleures pratiques méthodologiques sont appliquées.[12]

CrowdTangle : *(Outil)* Facebook a créé CrowdTangle comme outil d'identification et de suivi des tendances sur les réseaux sociaux. L'outil peut suivre les comptes vérifiés, les pages et les groupes publics. L'outil peut également être utilisé pour surveiller les comptes publics sur Instagram et les fils de discussion subreddit sur la plateforme Reddit.[13]

Vous devriez examiner ces ressources, ainsi que les outils supplémentaires figurant à l'annexe C, page 64, afin de déterminer quels outils vous seront les plus utiles, à vous et à votre organisation, pour identifier la manipulation des informations. Chaque campagne, organisation et contexte national sera différent et nécessitera une combinaison d'outils, de compétences et de partenaires. Ainsi, le fait de comprendre les outils qui peuvent vous aider à identifier et à suivre les campagnes en cours vous permettra de réagir et de renforcer la résilience.

[10] « Bellingcat's Online Investigation Toolkit », https://docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit#gid=930747607

[11] Craig Silverman, éd., *Verification Handbook for Disinformation and Media Manipulation* (European Journalism Centre s.d.), https://datajournalism.com/read/handbook/verification-3/.

[12] The Beacon Project, « Media Monitoring Handbook » (International Republican Institute, août 2021), https://www.data-iribeaconproject.org/handbook/.

[13] CrowdTangle (Facebook, s.d.), https://www.crowdtangle.com.

Élaborer un flux de travail

Lorsque vous suivez la manipulation des informations, vous devez élaborer des stratégies de surveillance à court et à long terme. Lors de l'élaboration d'un flux de travail, vous devez tenir compte des éléments suivants :

- **Quels sont vos buts ou objectifs principaux ?** Essayez-vous de réduire l'impact de la désinformation en vérifiant les récits ? Ou bien essayez-vous de responsabiliser les acteurs malveillants qui se livrent à la désinformation ? Vos objectifs détermineront directement la portée de votre surveillance, ainsi que les types d'outils et de partenaires avec lesquels vous travaillerez.

- **Quelle portée** a votre surveillance ? Déterminer la portée implique de poser des questions telles que :

  - Quelle est la pénétration d'Internet dans votre pays et les réseaux sociaux serviront-ils de source d'information pendant les élections ?
  - Quelles sont les plateformes qui feront l'objet d'une surveillance ?
  - Quelles sont les plus grandes menaces pour l'intégrité électorale en matière de désinformation ?
  - Qui sont les acteurs potentiels impliqués dans la manipulation de l'information ?
  - Quels sont les thèmes liés aux élections qui sont considérés comme faisant partie du champ d'application de votre surveillance, dans quelles langues travaillerez-vous et quelles questions laisserez-vous en dehors du champ de vos enquêtes ?

- **Quels outils allez-vous utiliser** pour vous aider dans l'identification et la surveillance ?

- Lors de la collecte de données sur la manipulation de l'influence dans les médias numériques, imprimés ou télévisés, **comment les données seront-elles collectées**, étiquetées et stockées pour rendre l'analyse et le triage plus accessibles pour vous et votre organisation ? Le processus de suivi et de surveillance des campagnes d'influence peut prendre des semaines, voire des mois, et la mise en place d'un système permettant de recueillir des informations au fil du temps sera déterminante pour votre réussite.

- **Qui sera chargé de surveiller** l'écosystème de l'information ? Comment fonctionnera cette équipe et **comment les membres seront-ils formés** afin d'avoir une approche cohérente dans l'identification des manipulations d'influence en ligne ?

- Certaines périodes vous obligeront-elles, vous et votre organisation à **intensifier les activités de surveillance**, par exemple avant une élection ou un référendum politique important ?

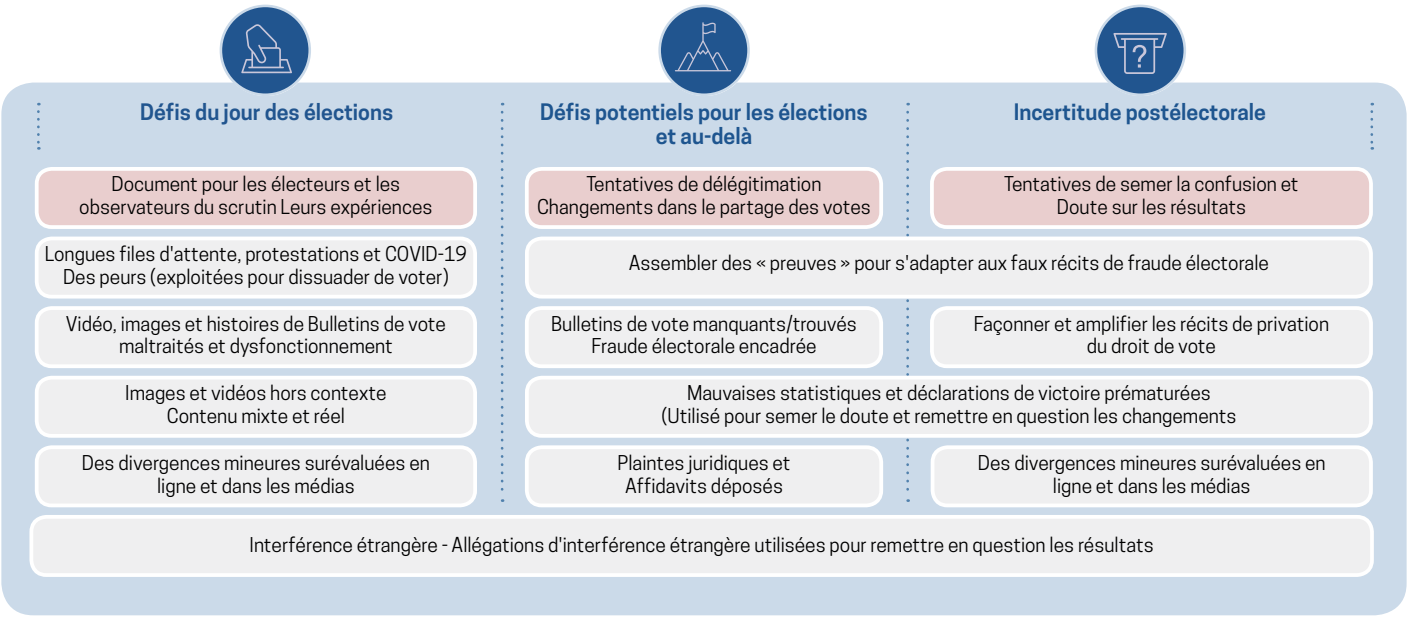
Pour plus de ressources sur l'élaboration de votre flux de travail et la réflexion sur la portée de vos processus d'identification, voir le Guide d'observation des médias sociaux pour observateurs citoyens de l'Union européenne.[14]

[14] *Guide d'observation des médias sociaux pour observateurs citoyens* (Union européenne, août 2019), https://www.ndi.org/sites/default/files/social-media-DEF.pdf.

Étape 2 Réponse

Dans ce guide, *répondre* signifie *réagir rapidement à une activité en ligne nuisible liée aux élections*. Quelles que soient la force de vos défenses et l'importance que vous accordez à la prévention, en réalité ceux qui défendent l'intégrité de l'information auront toujours un train de retard. Il est donc essentiel de se concentrer davantage sur l'identification et la réponse afin d'agir rapidement et efficacement contre la manipulation des informations liées aux élections lorsqu'elle ne se produise. Ce chapitre couvrira les réponses, notamment les signalements aux organes de gestion des élections (OGE), aux agences gouvernementales, aux forces de l'ordre et aux plateformes de réseaux sociaux ; les communications stratégiques ; la vérification des informations ; et le silence stratégique.

Figure 1. A quoi s'attendre : Défis pour le jour du scrutin et par après



Source : Modèle adapté du document « What to expect on election night and days after » de Election Integrity Partnership. Le graphique initial portait sur une étude de cas américaine, que nous avons adaptée pour l'appliquer à un contexte mondial.[15]

Signalement

La manipulation de l'information peut être signalée aux organes de gestion des élections (OGE), aux agences gouvernementales, aux forces de l'ordre, aux plateformes de réseaux sociaux, aux organisations non gouvernementales internationales (ONGI), aux organisations de vérification des informations ou aux organisations qui représentent le domaine concerné ou la communauté ciblée.

Chaque entité endosse des rôles différents, qui se chevauchent parfois, dans sa réponse à la manipulation de l'information. Les plateformes de réseaux sociaux peuvent enquêter et prendre des mesures pour réduire la propagation de la désinformation et des discours incitant à la haine ; les gouvernements et les commissions électorales peuvent créer des cadres juridiques qui limitent la capacité des acteurs malveillants à perpétrer de la manipulation de l'information, ainsi que lancer des campagnes d'information pour partager des informations exactes ou démystifier les informations inexactes ; les organisations de vérification des informations peuvent enquêter sur la véracité d'une allégation et démystifier publiquement la manipulation de l'information ; les ONGI peuvent travailler avec des partenaires locaux pour s'assurer que les préoccupations sont prises au sérieux et qu'il existe une capacité à faire face à la situation ; et les organisations qui travaillent dans des domaines spécifiques ou avec des communautés ciblées peuvent prendre des mesures pour protéger leurs communautés et/ou contribuer aux efforts de démystification. Les efforts les plus efficaces en matière de signalement consistent probablement à s'engager avec un certain nombre de partenaires différents selon le contexte local et les

[15] Kate Starbird et al., « Uncertainty and Misinformation : What to Expect on Election Night and Days After », (Election Integrity Partnership, 26 octobre 2020), https://www.eipartnership.net/news/what-to-expect.

spécificités de la manipulation de l'information qui a été observée. Il convient de noter qu'il est difficile pour les OSC, les OGE ou les activistes de s'attaquer seuls à la manipulation de l'information; les gouvernements et les entreprises technologiques doivent également s'engager pour relever ces défis.

Cette section vous aidera à comprendre qui joue quel rôle, comment signaler le plus efficacement possible la manipulation de l'information et ce à quoi vous pouvez vous attendre une fois que vous avez fait votre signalement. Il est important de comprendre que les conseils que nous fournissons peuvent ne pas fonctionner pour chaque type d'acteur ou d'environnement de l'information. Pour choisir les meilleures tactiques à suivre, vous devez prendre en compte le contexte de votre pays, les types de relations ou de partenaires que vous avez déjà, ainsi que la mission, les compétences techniques et l'expertise de votre groupe. Par exemple, tous les groupes n'auront pas les compétences nécessaires pour vérifier les informations ou être en mesure de signaler la manipulation d'informations à un gouvernement qui est lui-même à l'origine de cette manipulation.

Après avoir examiné les suggestions de **l'Étape 1 : Identification**, vous devez maintenant réfléchir aux objectifs que vous souhaitez atteindre en signalant la manipulation de l'information.

- Le contenu a-t-il été retiré ?
- Des utilisateurs ou des pages ont-ils été bannis ?
- Lancer une enquête sur un comportement trompeur organisé ou d'autres violations des conditions de service de la plateforme ?
- Accroître l'attention et la sensibilisation à un événement, une tendance ou un acteur menaçant spécifique ?
- Plaider pour que le gouvernement et les plateformes de réseaux sociaux prennent des mesures préventives ?

Une fois que vous aurez examiné les questions ci-dessus, vous serez mieux à même de choisir les entités les plus appropriées pour signaler la manipulation des informations qui a été observée. Vous pouvez signaler un même problème ou violation à plusieurs entités à la fois. Nous avons regroupé les entités potentielles en trois catégories générales :

Gouvernement

Vérifiez si votre gouvernement, votre commission électorale ou d'autres agences de lutte contre la cybercriminalité ou organismes d'information disposent d'un système de signalement de la més/désinformation. Si oui, vous devez envisager de leur signaler le contenu en infraction en tenant compte d'un certain nombre de facteurs (voir page 18).

Plateformes de réseaux sociaux

Si le contenu ou le comportement est en violation des politiques et conditions de la plateforme de réseaux sociaux où il se trouve, vous pouvez signaler le contenu à la plateforme concernée (voir page 22).

Vérificateurs d'informations

Envisagez de communiquer la més/désinformation à des groupes de vérification des informations de votre pays ou votre région (voir page 35).

Signalement aux organes de gestion des élections, aux agences gouvernementales et aux forces de l'ordre

La plupart des pays démocratiques disposent d'un organe de gestion des élections (OGE), d'une commission, d'un conseil ou d'un comité électoral[16] qui supervise la mise en œuvre du processus électoral, ainsi que d'agences gouvernementales et d'organismes d'application de la loi qui contribuent à faire respecter les réglementations électorales du pays.

[16] Les noms officiels varient selon les pays et les modèles électoraux peuvent être indépendants, mixtes, judiciaires ou exécutifs, mais nous utiliserons le terme d'organe de gestion des élections (OGE) dans ce guide.

De nombreux OGE ne disposent pas des ressources, des structures ou des mécanismes nécessaires pour faire face à la manipulation des informations liées aux élections ou pour se protéger, et protéger les élections, des récits de manipulation des informations autour des élections. Pour ceux qui le font, très peu ont créé des mécanismes de signalement permettant aux citoyens de signaler les manipulations d'informations liées aux élections observées en ligne.[17] En outre, les OGE n'ont généralement pas le mandat pour élaborer des réglementations rigoureuses concernant les campagnes en ligne, ni la capacité de faire appliquer les réglementations existantes. Cependant, certains OGE ont créé des mesures dissuasives pour empêcher les acteurs malveillants de prendre part à la manipulation de l'information électorale en établissant des codes de conduite pour les campagnes et en collaborant avec les plateformes de réseaux sociaux pour réglementer les comportements des partis politiques et des candidats aux élections.

Si vous souhaitez que votre OGE explore des solutions pour décourager la manipulation des informations électorales ou créer des codes de conduite, vous devez plaider directement auprès de votre OGE. Toutefois, gardez à l'esprit que certains OGE ne sont pas des organes indépendants et qu'ils peuvent donc ne pas être impartiaux dans les structures et les politiques qu'ils adoptent ou dans les mesures qu'ils prennent à l'encontre des contrevenants.

En outre, certains gouvernements ont créé des agences chargées de lutter contre les cyberattaques et autres menaces numériques, dont certaines ont également pour fonction de protéger l'infrastructure électorale, par exemple l'Agence de cybersécurité et de sécurité des infrastructures (CISA) aux États-Unis et l'Agence nationale de cybercryptage (BSSN) en Indonésie. Vérifiez si ces types d'agences existent dans votre pays et si elles ont mis en place des mécanismes de signalement par les citoyens de la manipulation des informations liées aux élections.

Ressources disponibles pour les OGE

La Fondation internationale pour les systèmes électoraux (IFES) dispose d'un certain nombre de ressources et de programmes conçus pour aider les commissions électorales ou les organes de gestion à prévenir et à réagir efficacement à la manipulation de l'information. Si vous travaillez pour un OGE ou si vous souhaitez en savoir plus sur le rôle que les OGE peuvent jouer dans la réponse à la manipulation de l'information liée aux élections, consultez la section sur les approches des OGE pour contrer la désinformation du Guide de lutte contre la désinformation du Consortium pour le renforcement des élections et des processus politiques (CEPPS).[18] [19]

Si ce n'est pas le cas, pensez à plaider auprès de vos élus pour qu'ils les mettent en place. Examinez la section[20] Plaidoyer auprès des gouvernements du Guide de lutte contre la désinformation du CEPPS pour obtenir des conseils et des exemples sur la manière dont une OSC peut plaider pour que son gouvernement prenne des mesures. Il est important de savoir que les régimes autoritaires ont fréquemment eu recours à des agences et à de nouvelles législations de cybersécurité, pour réprimer la liberté d'expression, par le biais de lois qui identifient les contenus de l'opposition comme des « fake news ou de la mésinformation » nuisibles.

Si vous ou votre organisation travaillez sur des campagnes électorales, vous devez examiner attentivement les cadres

[17] Par exemple, le site web de la Commission centrale électorale d'Israël fournit les numéros de contact des lignes d'assistance de la police et du Centre national des cyberincidents et de la sécurité de l'information pour que les citoyens puissent signaler les tentatives de manipulation des électeurs par le biais de faux profils et autres, au lieu de traiter et d'enquêter sur les violations elles-mêmes.

[18] Créé en 1995, le CEPPS met en commun l'expertise de trois organisations internationales dédiées au développement démocratique : la Fondation internationale pour les systèmes électoraux (IFES), l'International Republican Institute (IRI) et le National Democratic Institute (NDI). Le CEPPS a 25 ans d'expérience en matière de collaboration et de leadership dans le domaine du soutien à la démocratie, aux droits de l'homme et à la gouvernance. Fort de ses expériences, le Consortium adopte de nouvelles approches et de nouveaux outils en fonction du paysage technologique en constante évolution. Les organisations fonctionnent comme un consortium afin de fournir à l'USAID et à d'autres bailleurs de fonds la capacité de mettre en œuvre des programmes complexes axés sur la démocratie, les droits et la gouvernance (DDG) à l'échelle de l'ensemble des contextes politiques et des régions géographiques.

[19] USAID et National Democratic Institute, « Election Management Body Approaches to Countering Disinformation » dans Countering Disinformation : A Guide to Promoting Information Integrity ,(Consortium for Elections and Political Process Strengthening, 2021), https://counteringdisinformation.org/topics/embs/0-overview-emb-approaches.

[20] USAID et National Democratic Institute, « Building Civil Society Capacity To Mitigate And Counter Disinformation » dans *Countering Disinformation : A Guide to Promoting Information Integrity*, (Consortium for Elections and Political Process Strengthening, 2021), https://counteringdisinformation.org/topics/csos/5-advocacy-toward-governments.

juridiques, l'application de la loi, les organes de surveillance indépendants et les autres organismes de réglementation qui sont ou pourraient être impliqués dans les réseaux sociaux et l'espace d'information élargi. Dans certains cas, les services de police locaux ou fédéraux disposent d'équipes spécifiquement dédiées à l'application des lois sur le numérique. Lorsqu'ils sont honnêtes et dignes de confiance, ces organismes d'application de la loi constituent des moyens viables de signaler et de surveiller les campagnes nuisibles. Le système judiciaire peut également jouer un rôle dans la gouvernance de l'espace en ligne et peut ordonner des mesures pour mettre fin à la diffusion de la manipulation d'informations en ligne.

Une agence anti-corruption, un organe de contrôle du financement politique ou un organe de contrôle des médias peuvent servir d'organes de contrôle indépendants. Dans la section juridique et réglementaire[21] du Guide de lutte contre la désinformation du CEPPS, quatre types d'approche réglementaire sont décrits plus en détail et s'adressent à la fois aux plateformes et aux acteurs nationaux. Elle comprend notamment des mesures visant à restreindre le contenu et les comportements en ligne et à promouvoir la transparence, l'équité et l'information démocratique pendant les campagnes et les élections. Ce sont toutes des voies potentielles pouvant présenter des points pertinents pour le plaidoyer politique, qui sont explorées plus en détail dans le Guide du CEPPS, mais qui doivent être soigneusement examinées pour chaque contexte national donné. Dans d'autres circonstances, notamment lorsque le gouvernement ne respecte pas les normes démocratiques ou est autrement compromis, les organes chargés de l'application de la loi ou de la réglementation peuvent souvent jouer un rôle activement nuisible, en élaborant et en appliquant des lois qui limitent les discours politiques légitimes au nom de la lutte contre la manipulation de l'information. Il est plus problématique et souvent contre-productif de rendre compte à ces acteurs.

Les pays qui sont généralement libres (voir l'encadré « Outils d'évaluation de l'ouverture d'un gouvernement ») peuvent créer des cadres juridiques pour signaler et répondre à la manipulation de l'information de manière à protéger et à ouvrir l'espace du discours démocratique, tout en se prémunissant contre la manipulation de l'information. Si un pays n'est pas libre ou partiellement libre, vous devez faire preuve de prudence lorsque vous vous adressez à des organismes réglementaires, judiciaires

Outils d'évaluation de l'ouverture d'un gouvernement

L'une des mesures de la position politique d'un gouvernement est l'indice global de liberté de Freedom House.[22] Il indique si un pays est libre, partiellement libre ou pas libre, sur la base de facteurs tels que les droits politiques et les libertés civiles. L'indice de liberté d'Internet[23] de Freedom House étudie les réglementations gouvernementales relatives à Internet, ainsi que divers autres facteurs, en évaluant le degré d'ouverture ou de fermeture de l'Internet national d'un pays, ainsi que la structure des agences gouvernementales qui le réglementent et toute loi pertinente. Il attribue à chaque pays un score qui permet de classer les pays en fonction d'un certain nombre de facteurs, de références et de détails supplémentaires qui devraient être examinés dans le cadre d'une évaluation de l'espace d'information et du cadre juridique. Ces classements sont mis à jour chaque année, mais ils doivent être pondérés en fonction de la situation actuelle dans votre pays, car celle-ci peut changer rapidement. Une autre mesure a été mise au point par l'Institut V-Dem,[24] qui a créé un ensemble de données multidimensionnelles solides tenant compte des systèmes complexes de la démocratie et permettant aux utilisateurs d'évaluer l'évolution d'une démocratie particulière dans le temps. Il ne s'agit là que de trois méthodes permettant d'évaluer l'ouverture d'un pays et le respect de l'État de droit, mais la compréhension de cette composante est une première étape essentielle.

[21] USAID et National Democratic Institute, « Legal and Regulatory Responses to Disinformation » dans Countering Disinformation : A Guide to Promoting Information Integrity, (Consortium for Elections and Political Process Strengthening, 2021), https://counteringdisinformation.org/node/2704/.

[22] « Indice global de liberté » (Freedom House, 2021), https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege/countries-and-regions.

[23] « Indice de liberté d'Internet » (Freedom House, 2021), https://freedomhouse.org/countries/freedom-net/scores.

[24] « V-Dem : Global Standards, Local Knowledge » (Varieties of Democracy, s.d.), https://www.v-dem.net/en/.

ou autres organismes gouvernementaux. À tous les niveaux de liberté, les organes de contrôle d'un pays peuvent être faibles ou inefficaces dans ce domaine, même dans les démocraties fortes. Vous devez évaluer soigneusement ces organismes et la réglementation en matière de suivi, et éventuellement faire appel à des experts et à des ressources pour examiner leur efficacité, leur fiabilité et leur ambition.

Si l'état de droit ou la transparence de ces organes est faible, d'autres options (détaillées ci-dessous) doivent être envisagées. Pour des conseils supplémentaires sur le signalement aux organismes chargés de l'application de la loi, veuillez vous référer à la section sur les cadres juridiques et l'application de la loi du Guide de lutte contre la désinformation du CEPPS.[25]

Lorsque vous cherchez à signaler la manipulation d'informations liées aux élections aux agences gouvernementales, aux commissions électorales et à d'autres organismes chargés de faire respecter la loi, voici quelques facteurs essentiels à prendre en compte :

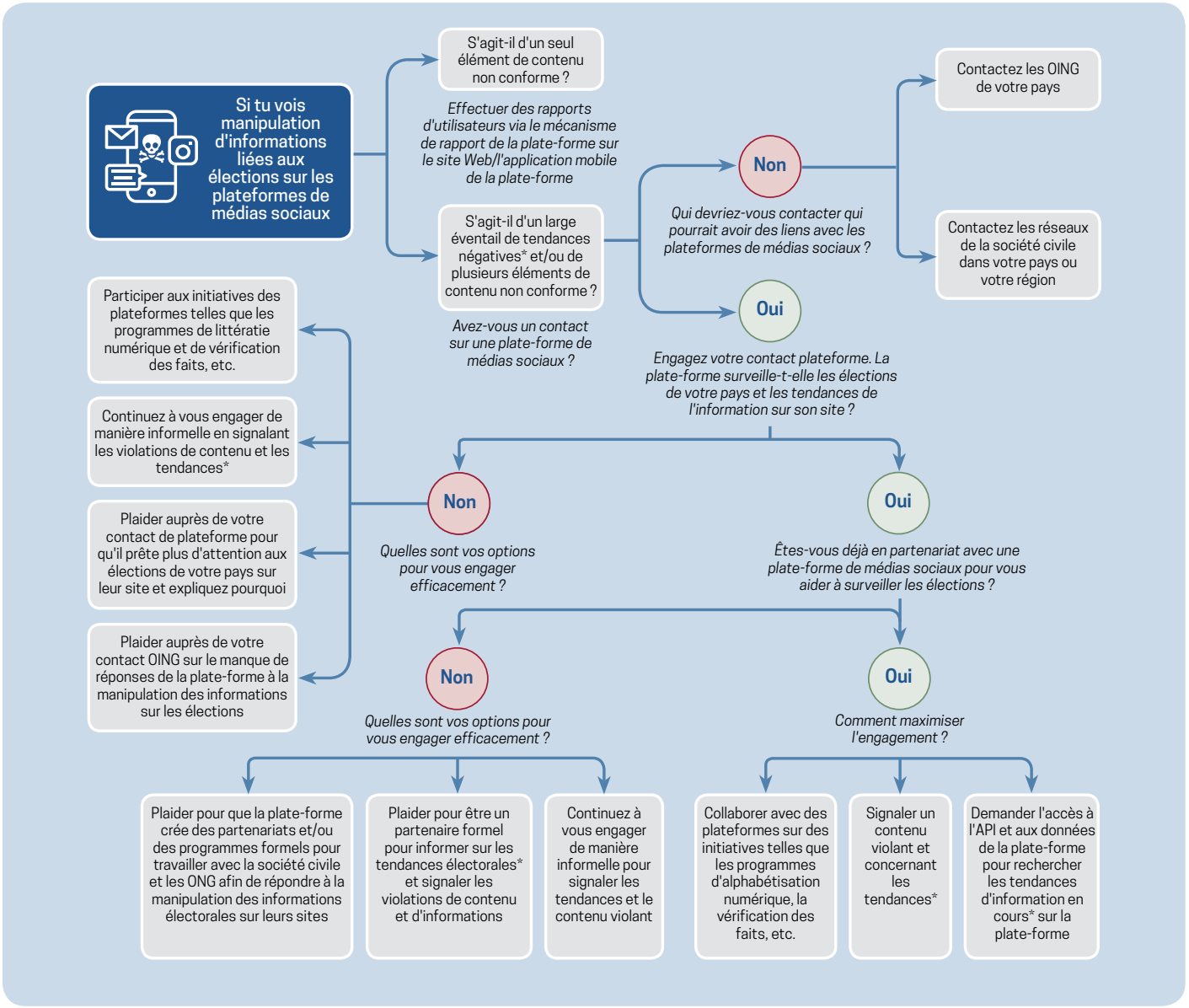
- Pensez-vous que ces agences agissent de manière **impartiale** ?
- Votre gouvernement a-t-il la **capacité et la possibilité** de prendre des mesures concernant le contenu signalé ?
- Votre agence gouvernementale a-t-elle **pris des mesures** après avoir reçu des signalements sur des contenus en ligne préjudiciables ayant conduit au retrait de ces messages ?
- Votre gouvernement **réglemente-t-il les discours en ligne** ou dispose-t-il de lois contre les campagnes de diffamation préélectorales, le sapage de réputation et les campagnes de manipulation de l'information ? Ces lois sont-elles utilisées contre les voix de l'opposition et les partis politiques qui se présentent aux élections ?
- Quelle est la **position politique** générale du gouvernement ? Est-il généralement ouvert et démocratique, ou tend-il à devenir autoritaire ?
- Votre gouvernement a-t-il l'**habitude de réduire au silence les voix de l'opposition** et les critiques, en particulier avant les élections ?
- Certaines agences gouvernementales sont-elles elles-mêmes des **agents de manipulation de l'information** (tant à l'étranger qu'au niveau national)

Pour obtenir une liste complète d'exemples d'actions prises par les gouvernements du monde entier pour se défendre contre la mésinformation, notamment les efforts allant des tentatives légitimes des gouvernements démocratiques pour assurer l'intégrité de l'information, aux initiatives des régimes autoritaires pour censurer les discours qu'ils n'aiment pas, visitez le guide de Poynter pour lutter contre la mésinformation dans le monde.[26]

[25] USAID et National Democratic Institute, « Legal and Regulatory Responses to Disinformation » dans *Countering Disinformation : A Guide to Promoting Information Integrity*. https://counteringdisinformation.org/topics/legal/6-enforcement#EnforcementMandate.

[26] Daniel Funke et Daniela Flamini, « A Guide to Anti-Misinformation Actions Around the World », (Poynter, 13 avril 2021), https://www.poynter.org/ifcn/anti-misinformation-actions/.

Signalement sur les plateformes de réseaux sociaux



***** Si vous êtes une personne ou un groupe effectuant une surveillance des réseaux sociaux pour identifier et signaler les tendances en matière de manipulation de l'information, consultez la page 16 pour obtenir des instructions détaillées sur les stratégies de surveillance à court et à long terme. Pour des conseils plus spécifiques sur l'utilisation des données CrowdTangle de Facebook pour identifier les tendances, consultez la ressource de First Draft ici.[27]

Les plateformes de réseaux sociaux et les hébergeurs de sites web en ligne suivent et réagissent à la manipulation de l'information par le biais de divers mécanismes : signalement par les utilisateurs, partenariats avec la société civile pour identifier les tendances et les risques locaux, recours à des experts, renseignements internes et externes sur les menaces et criminalistique numérique, coordination intersectorielle et engagement avec les organisations gouvernementales. Selon le type d'organisation que vous êtes et ce que vous souhaitez communiquer aux plateformes, certaines de ces options seront plus pertinentes pour vous et d'autres moins.

[27] Carlotta Dotto, « How to Analyze Facebook Data for Misinformation Trends and Narratives » (First Draft, 7 mai 2020), https://firstdraftnews.org/articles/how-to-analyze-facebook-data-for-misinformation-trends-and-narratives/.

Les méthodes utilisées par les plateformes pour traiter les signalements sur la manipulation de l'information, lutter contre la més/désinformation, modérer le contenu et collaborer en interne et en externe varient considérablement et dépendent de l'endroit où l'entreprise a été fondée, de son ancienneté, de ses finances et de ses relations avec les parties prenantes externes et les gouvernements, entre autres considérations.

Conseil : N'ayez pas pour seule approche le signalement sur les plateformes de réseaux sociaux.

Notez que le signalement des contenus en violation aux plateformes de réseaux sociaux est une étape nécessaire mais insuffisante. Il est peu probable que les plateformes réagissent en temps utile aux signalements des utilisateurs et il faut parfois des jours ou des semaines pour recevoir une réponse. Le contenu qui, selon vous, menace l'intégrité électorale peut ne pas être contraire à la politique ou aux normes communautaires d'une plateforme et être laissé en ligne. Souvent, les plateformes ne sont pas non plus préparées à gérer l'environnement de l'information électorale d'un pays sur leurs sites ou ne comprennent pas l'espace d'information et les menaces locales. Par conséquent, le signalement aux plateformes ne doit pas être votre seule démarche et doit être effectué conjointement avec les autres actions recommandées. Les plateformes de réseaux sociaux évoluent rapidement et obligent tous ceux qui travaillent à l'amélioration de l'intégrité de l'information électorale à surveiller constamment et, dans certains cas, à préconiser des changements de produits et de politiques et à adapter leurs stratégies d'interaction avec les plateformes.

Signalement des utilisateurs

Le signalement par les utilisateurs est le moyen le plus accessible de soulever des préoccupations concernant des éléments de contenu spécifiques qui violent les politiques de la plateforme de réseaux sociaux sur laquelle le contenu est partagé. Le signalement par les utilisateurs est généralement aussi simple que de signaler un contenu spécifique sur la plateforme et d'expliquer pourquoi il est nuisible. Notez que les rapports des utilisateurs sont généralement examinés par des systèmes automatisés, des modérateurs de contenu humains et, dans de rares cas, par d'autres services de l'entreprise, en fonction de la violation éventuelle des normes ou des politiques de l'entreprise. Ces processus manquent souvent de contexte sociétal ou politique et de connaissance des langues locales. Le signalement par les utilisateurs n'est pas un moyen efficace d'attirer l'attention sur des tendances inquiétantes ou sur une campagne de manipulation de l'information à grande échelle. Cependant, il est efficace pour supprimer des éléments de contenu ou des comptes de réseaux sociaux qui violent clairement les politiques de la plateforme. Pour plus de détails sur les politiques communautaires et les lignes directrices de chaque plateforme concernant la définition du contenu à signaler et d'autres interventions de la plateforme spécifiques aux élections, reportez-vous à l'annexe B à la page 59.

Le tableau ci-dessous fournit des indications sur les processus de signalement des principales plateformes. Nous avons répertorié ici les principales plateformes de réseaux sociaux en raison de leur grand nombre d'utilisateurs et de leur portée mondiale.

Plateforme	Comment faire un signalement
Facebook	Si vous identifiez des contenus et/ou des comptes sur Facebook que vous soupçonnez de diffuser des contenus préjudiciables avant les élections, suivez les liens ci-dessous. • Signaler une publication Facebook comme étant une fausse information[28] • Comment signaler un contenu[29] Les appels peuvent être référés au Conseil de surveillance. Voir l'encadré sur le Conseil de surveillance de Facebook à la page 25.

[28] Pages d'aide de Facebook, « Comment signaler une fausse information dans une publication Facebook ? » (Facebook, s.d.), https://www.facebook.com/help/572838089565953.

[29] Pages d'aide de Facebook, « Comment signaler des irrégularités » (Facebook, s.d.), https://www.facebook.com/help/1380418588640631.

Plateforme	Comment faire un signalement
Instagram	Pour soumettre des rapports de més/désinformation préjudiciable autour des élections, rendez-vous sur la page Réduire la diffusion de fausses informations sur Instagram.[30]
Google	Les différents produits de Google sont régis par des conditions d'utilisation respectives qui présentent des restrictions sur les comportements et les contenus haineux et trompeurs. Les procédures de Google pour signaler la més/désinformation et autres contenus nuisibles sur sa plateforme sont également spécifiques à chaque produit. Toutefois, c'est Recherche Google Search qui est le plus pertinent dans le cadre de ce guide. L'outil permettant de demander la suppression d'informations dans Recherche Google se trouve sur cette page.[31]
Snapchat	Pour signaler tout soupçon de més/désinformation liée aux élections ou tout autre contenu préjudiciable, utilisez la fonction de signalement de Snapchat dans l'application[32] ou remplissez ce formulaire[33] sur son site web.
TikTok	Pour signaler une vidéo, un commentaire, un utilisateur, un hashtag, etc. suspectés de més/désinformation et d'autres contenus préjudiciables, consultez les instructions détaillées sur la page Signaler un problème de TikTok.[34]
Twitter	Pour signaler les Tweets, Listes et Messages Privés que vous soupçonnez de diffuser des contenus préjudiciables aux élections dans votre pays, suivez les instructions suivantes ici.[35] Twitter définit les contenus préjudiciables dans les Règles de Twitter[36] pour vous aider à comprendre où sont les limites et à déterminer ce qui constitue du contenu à signaler selon ses définitions.
YouTube	Pour signaler de la més/désinformation et d'autres contenus préjudiciables apparaissant sur YouTube par le biais des vidéos, d'une playlist, d'une miniature, d'un commentaire, d'une chaîne, etc., utilisez son mécanisme interne qui se trouve sur la page Signaler un contenu inapproprié.[37]
WhatsApp	Pour signaler un contenu préjudiciable à WhatsApp, suivez les instructions ici.[38] Notez que WhatsApp est une application de messagerie fermée et cryptée. La surveillance du contenu sur cette application est donc différente de celle des autres plateformes de réseaux sociaux énumérées ci-dessus.

[30] Pages d'aide d'Instagram, « Réduire la diffusion de fausses informations sur Instagram » (Instagram, s.d.), https://help.instagram.com/1735798276553028.

[31] Aide de Google, « Suppression de contenu de Google » (Google, s.d.), https://support.google.com/legal/troubleshooter/1114905.

[32] Assistance Snapchat, « Signaler un abus ou un problème de sécurité sur Snapchat » (Snapchat, s.d.), https://support.snapchat.com/en-US/a/report-abuse-in-app.

[33] Snapchat Support, « Contactez-nous » (Snapchat, s.d.), https://support.snapchat.com/en-US/i-need-help.

[34] Aide TikTok, « Signaler un problème » (TikTok, s.d.), https://support.tiktok.com/en/safety-hc/report-a-problem.

[35] Centre d'assistance de Twitter, « Signaler un Tweet, une liste ou un Message Privé » (Twitter, s.d.), https://help.twitter.com/en/safety-and-security/report-a-tweet.

[36] Centre d'assistance de Twitter, « Les Règles de Twitter » (Twitter, s.d.), https://help.twitter.com/en/rules-and-policies/twitter-rules.

[37] Aide YouTube, « Signaler un contenu inapproprié » (YouTube, s.d.), https://support.google.com/youtube/answer/2802027.

[38] Centre d'aide WhatsApp, « Comment utiliser WhatsApp en toute sécurité » (WhatsApp, s.d.), https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp.

Outre les informations présentées dans le tableau ci-dessus, vous pouvez également trouver les instructions détaillées[39] de Mozilla Foundation sur le signalement sur les apps. Sachez que le temps de réponse et les processus d'enquête diffèrent selon les plateformes. En général, après qu'un utilisateur de la plateforme a signalé un contenu en violation par le biais du système en ligne de la plateforme, **le processus d'examination se déroule comme suit :**

Le système automatisé de la plateforme vérifie les violations évidentes dans le contenu signalé - pédopornographie, insultes connues, etc. - et supprime les publications en infraction.

Si le système automatisé n'est pas en mesure de fournir des réponses définitives, la violation signalée est examinée par des modérateurs de contenu, qui peuvent ou non connaître la langue et le contexte locaux.

Si les modérateurs de contenu estiment que les messages ne respectent pas les politiques et les normes communautaires de la plateforme, le message est supprimé. En cas de doute, la publication est transmise à d'autres équipes de l'entreprise, par exemple l'équipe chargée des politiques, l'équipe chargée de la confiance et de la sécurité, etc.

En fonction de la gravité et de l'impact politique de la question, une publication spécifique peut être partagée avec la direction de l'entreprise pour des considérations et un examen plus détaillés avant qu'une décision ne soit prise.

Le Conseil de surveillance de Facebook.

Facebook a créé le Conseil de surveillance pour l'aider à répondre à certaines des questions les plus difficiles concernant la liberté d'expression en ligne, ce qu'il faut retirer, ce qu'il faut laisser et pourquoi.[40] Le Conseil de surveillance prévoit également une procédure d'appel permettant aux personnes de contester les décisions relatives au contenu sur Facebook ou Instagram. Si vous avez déjà demandé à Facebook ou Instagram de revoir l'une de ses décisions en matière de contenu et que vous n'êtes pas d'accord avec la décision finale, vous pouvez faire appel auprès du Conseil. Le processus est détaillé ici.[41] Tous les cas soumis ne seront pas sélectionnés pour faire l'objet d'une procédure d'appel et le délai de la procédure est assez long.

[39] Audrey Hingle, « Misinfo Monday : How to Report Election Misinformation » (Mozilla, 12 octobre 2020, https://foundation.mozilla.org/en/blog/misinfo-monday-how-report-election-misinformation/.

[40] Conseil de surveillance, « Garantir la liberté d'expression au moyen d'un jugement indépendant » (Conseil de surveillance de Facebook, s.d.), https://oversightboard.com.

[41] Conseil de surveillance, « Faire appel des décisions relatives au contenu sur Facebook et Instagram » (Conseil de surveillance de Facebook, s.d.), https://oversightboard.com/appeals-process/.

Une tendance croissante : Manipulation de l'information dans les groupes fermés et les applications de messagerie chiffrée

Alors que les plateformes mettent à jour leurs politiques en matière de manipulation de l'information et intensifient et améliorent leurs efforts en matière de modération et de suppression du contenu, les acteurs malveillants déplacent de plus en plus leurs efforts de manipulation de l'information vers des sites plus difficiles à surveiller, notamment les groupes fermés et les applications de messagerie chiffrée comme les groupes Facebook, WhatsApp, Telegram, Signal, LINE et WeChat. Beaucoup de ces applications sont cryptées et il n'existe aucun moyen efficace de surveiller ou de supprimer de manière proactive la diffusion d'informations malveillantes. Pour contrer les formes de contenu nuisibles comme la désinformation, certaines applications ont mis à jour leurs produits et leurs politiques. Par exemple, WhatsApp a mis en place des limites de transfert de messages pour aider à « ralentir la propagation des rumeurs, des messages viraux et des fake news ».[42] Les journalistes et les chercheurs ont tenté de faire des signalements à partir d'applications de messagerie cryptées en rejoignant des groupes fermés et en mettant en place des lignes d'information pour encourager le public à envoyer du contenu. Cependant, ces méthodes posent également de nombreux défis à ceux qui tentent de signaler des contenus illicites provenant d'applications de messagerie cryptées, notamment des défis éthiques.[43] D'autres, issus de la société civile, ont lancé des campagnes de sensibilisation publiques en partageant des informations précises sur WhatsApp. L'effet de ces types de campagnes reste à voir et les résultats sont difficiles à mesurer. Toutefois, des efforts fructueux ont été déployés pour lutter contre la manipulation de l'information sur les plateformes de messagerie fermées. À Taïwan, une collaboration entre LINE et Cofacts permet de faire vérifier les informations par des volontaires et de démystifier les messages viraux dans les discussions en ligne sans porter atteinte à la vie privée. En Espagne, l'organisation de fact-checking Maldita.es a ajouté en juillet 2020 un chatbot automatisé à sa ligne d'assistance WhatsApp existante afin d'améliorer le temps de réponse et de constituer une base de données pour suivre les tendances en matière de désinformation.[44]

Si vous souhaitez obtenir plus d'informations sur la manière de surveiller et de signaler les groupes fermés et les applications de messagerie, reportez-vous au Manuel de vérification[45] de European Journalism Centre (en particulier le chapitre 7), le Guide essentiel sur les applications de messageries fermées[46] de First Draft et le document de politique générale de Brookings Institution intitulé Countering Disinformation and Protecting Democratic Communication on Encrypted Messaging Applications.[47]

Autres moyens de collaborer avec les plateformes

Collaborer avec les équipes de la plateforme

La plupart des plateformes disposent de diverses équipes qui peuvent servir de points de contact avant, pendant et après les élections. Ces équipes ont des structures d'incitation, des rôles et des intérêts différents et ne connaissent parfois pas l'existence des unes et des autres. Certaines sont basées

[42] Centre d'aide WhatsApp, « À propos de la limite de transfert » (WhatsApp, s.d.), https://faq.whatsapp.com/general/chats/about-forwarding-limits/.

[43] Connie Moon Sehat, Tarunima Prabhakar et Aleksei Kaminski, *Ethical Approaches to Closed Messaging Research : Considerations in Democratic Contexts* (MisinfoCon et The Carter Center, 15 mars 2021), https://www.dropbox.com/s/rkchyrtdkn5buw9/FINAL-Ethical-Approaches-to%20Closed-Messaging-Research.pdf?dl=0.

[44] Harrison Mantas, « WhatsApp Can Be a Black Box of Misinformation, but Maldita May Have Opened a Window » (Poynter, 9 juin 2021), https://www.poynter.org/fact-checking/2021/whatsapp-can-be-a-black-box-of-misinformation-but-maldita-may-have-opened-a-window/.

[45] Silverman, *Verification Handbook for Disinformation and Media Manipulation*.

[46] Carlotta Dotto, Rory Smith et Claire Wardle, « Closed Groups, Messaging Apps & Online Ads » (première version, novembre 2019), https://firstdraftnews.org/wp-content/uploads/2019/11/Messaging_Apps_Digital_AW-1.pdf?x11129.

[47] Jacob Gursky et Samuel Woolley, C*ountering Disinformation and Protecting Democratic Communication on Encrypted Messaging Applications* (Brookings Institution, juin 2021), https://www.brookings.edu/wp-content/uploads/2021/06/FP_20210611_encryption_gursky_woolley.pdf.

localement, tandis que d'autres sont basées dans des centres régionaux ou au siège de l'entreprise. Le tableau ci-dessous donne un large aperçu des rôles liés aux élections et à la manipulation de l'information qui peuvent exister dans une entreprise donnée. Notez qu'identifier le bon personnel peut être difficile. Certains de ces rôles peuvent être remplis par la même équipe ou la même personne et les plateformes les plus récentes - même celles qui ont une large base d'utilisateurs ou un impact sur la sphère d'information - peuvent avoir une présence sur le terrain, des représentants nationaux ou du personnel dans ces fonctions assez limités.

Équipes de la plateforme	Rôles
Politique publique et relations avec le gouvernement	Les équipes chargées de la politique publique et des relations avec les pouvoirs publics sont généralement chargées de nouer le dialogue avec les agences de réglementation et autres organismes gouvernementaux. Leur rôle prédominant est d'assurer un environnement réglementaire favorable à la plateforme. Les entreprises ont tendance à placer les représentants des politiques publiques dans les capitales des pays qui sont des marchés importants. Les équipes chargées de la politique publique peuvent être de bons points d'entrée pour ceux qui tentent de s'attaquer à la manipulation de l'information, mais vous devez savoir qu'elles ont de multiples priorités et motivations concurrentes - en particulier dans les cas où un gouvernement national est un mauvais acteur dans l'espace d'information - et qu'elles ne considèrent donc pas toujours la manipulation de l'information comme faisant partie de leur rôle. Certaines entreprises disposent d'équipes chargées des partenariats et de la communication avec les communautés qui s'engagent spécifiquement auprès de la société civile, des groupes de plaidoyer et des universités.
Politique de contenu / Droits humains	Les plateformes de réseaux sociaux établies qui ont été confrontées à des problèmes importants liés aux préjudices en ligne disposent généralement de plusieurs équipes chargées d'atténuer ces préjudices. Ces équipes supervisent la création de politiques qui déterminent ce qui est autorisé ou non sur la plateforme, développent et surveillent l'application des politiques spécifiques liées aux droits humains et, souvent, développent des partenariats avec la société civile pour aider à orienter l'approche de l'entreprise en matière de contenu et de comportement des utilisateurs. Certaines plateformes ont des équipes dédiées explicitement chargées de garantir l'intégrité des élections. Dans certains cas, ces équipes sont en place de manière permanente, mais dans d'autres cas, elles peuvent être établies ponctuellement pour réagir lors d'une élection spécifique importante pour la plateforme.
Modérateurs de contenu	Les modérateurs de contenu - souvent des consultants et non des employés de l'entreprise - examinent le contenu signalé par les utilisateurs et décident s'il est conforme aux politiques et aux normes communautaires des plateformes. Ces consultants n'ont pas la possibilité de modifier les normes des plateformes.
Produit	Les équipes chargées des produits sont responsables du lancement des produits et de l'amélioration ou de la modification des produits afin d'empêcher les abus sur la plateforme et de limiter la diffusion de més/désinformation (par exemple, limiter le transfert de messages sur WhatsApp, etc.)

Équipes de la plateforme	Rôles
Renseignements sur les menaces	Les chercheurs qui mènent des enquêtes approfondies sur les menaces potentielles sur une plateforme s'intéressent généralement aux comportements trompeurs organisés ou à d'autres types de comportements.

Si vous n'êtes pas encore en contact avec les plateformes pertinentes pour votre sphère d'information, la plupart des entreprises mondiales de réseaux sociaux ont établi des partenariats avec de grandes ONGI ou coalitions, telles que Design 4 Democracy Coalition[48] et d'autres réseaux locaux ou régionaux de la société civile, qui peuvent travailler avec vous pour vous assurer que vous communiquez avec le meilleur point focal au sein de chaque entreprise.

Conseil : Introduction à Design 4 Democracy Coalition

Design 4 Democracy Coalition (D4D), dirigée par NDI, IRI, IFES et International IDEA, est un groupe international d'organisations de défense de la démocratie et des droits humains, venant de régions, d'idéologies politiques et d'horizons divers, qui s'est engagé à faire en sorte que l'industrie de la technologie adopte la démocratie comme principe de conception fondamental. D4D travaille au renforcement de la démocratie à l'ère numérique en établissant un forum de coordination et de soutien au sein de la communauté de la démocratie sur les questions technologiques et en créant un canal institutionnel de communication entre la communauté de la démocratie, les organisations de la société civile et l'industrie de la technologie. La coalition pourrait vous servir de ressource utile. Leurs coordonnées de contact sont disponibles sur le site web de D4D. La coalition D4D a également développé l'outil TRACE Tool, un formulaire qui vous permet de demander l'accès à des formations ou à des outils fournis par les partenaires technologiques de D4D, ou de signaler des problèmes de contenu ou de profil qui doivent être traités rapidement.[49]

Participer à des efforts de collaboration intersectorielle

La plupart des grandes plateformes en ligne ont établi des processus et des programmes de partenariat avec la société civile, les médias indépendants et le monde universitaire autour des questions liées à la manipulation de l'information. Il s'agit notamment de mécanismes permettant de mieux comprendre le contexte local et les questions linguistiques, de partenariats formels avec des vérificateurs d'information, des journalistes et la société civile et de canaux d'assistance rapide pour certains groupes en situation de crise. Les partenaires peuvent fournir de manière préventive des connaissances contextuelles et signaler les domaines problématiques et les événements potentiels qui pourraient faire l'objet d'une manipulation de l'information et entrainer une violence réelle. Cette contextualisation permet aux plateformes de prendre des mesures immédiates, soit en supprimant du contenu, soit en prenant des mesures proactives en modifiant leurs produits, leurs politiques et leurs ressources pour éviter que la plateforme ne facilite la violence ou les comportements antidémocratiques. Cette tactique est particulièrement efficace pour les OSC, les journalistes ou les activistes qui sont victimes de désinformation et de harcèlement de la part de l'État.

[48] Coalition Design for Democracy, https://d4dcoalition.org.

[49] Design for Democracy Coalition, https://d4dcoalition.org; Design for Democracy Coalition, « Contact Us » (D4D, s.d.), https://d4dcoalition.org/index.php/contact-us; Design for Democracy Coalition, "D4D Trace Tool" (D4D, n.d.).

Ces mécanismes sont adaptés en permanence et peuvent être actifs ou non dans votre pays. Les ONGI énumérées dans la section précédente à la page 40 peuvent vous aider à déterminer quels programmes sont actifs dans votre pays et comment vous pouvez y participer. Vous trouverez des exemples d'initiatives réussies à **l'Étape 3 : Renforcement de la résilience**, à la page 40.

Comment les entreprises de réseaux sociaux abordent la manipulation de l'information

Les plateformes de réseaux sociaux préfèrent généralement ne pas se fier uniquement aux utilisateurs qui signalent la diffusion de més/désinformation liées aux élections sur leurs plateformes. Selon le guide de lutte contre la désinformation du CEPPS,[50] les plateformes ont mis en place des politiques, des interventions sur les produits et des mesures d'application pour limiter la diffusion de més/désinformation. La plupart des plateformes ont également mis en place des outils de modération de contenu sous une forme ou une autre. Vous pouvez trouver un inventaire de ces outils dans le guide de modération de contenu Toolkit for Civil Society and Moderation Inventory[51] développé par Meedan.[52]

Les plateformes limitent également la diffusion de més/désinformation liée aux élections en concevant et en mettant en place des **fonctionnalités de produits et des interventions techniques ou humaines**. Cela dépend fortement de la nature et de la fonction d'une plateforme spécifique - service de réseaux sociaux traditionnels, plateforme de partage d'images et de vidéos, application de messagerie et moteur de recherche. Twitter et Facebook utilisent tous deux l'automatisation[53] pour détecter certains types de més/désinformation et faire appliquer les politiques de contenu. De la même manière, les entreprises utilisent des outils techniques pour faciliter la détection des activités trompeuses sur leurs plateformes et rendent publiques leurs conclusions dans des rapports de transparence périodiques qui comprennent des données sur les suppressions de comptes. Vous pouvez trouver plus de détails sur les initiatives des différents types de plateformes pour limiter la diffusion de més/désinformation par le biais des fonctionnalités du produit et de l'intervention technique/humaine à l'annexe B à la page 59 ou dans la section thématique sur les plateformes du Guide de lutte contre la désinformation du CEPPS.[54]

Communications stratégiques

Les communications en réponse ou en préparation à la manipulation d'informations liées aux élections se divisent généralement en deux approches : proactive et réactive.

- **Communication proactive :** Cette approche vise à fournir des informations précises, fiables, cohérentes et concises sur une élection *avant* que les faux récits n'apparaissent, dans le but de créer un espace d'information fiable pour les citoyens.

- **Communication réactive :** Cette approche vise à contrer les faux récits une fois qu'ils ont déjà gagné du terrain, ce qui implique souvent d'identifier directement un faux récit et ses objectifs et de répondre à ces inexactitudes par la vérité (*voir la section Vérification des informations à la page 35*).

[50] USAID et National Democratic Institute, *Countering Disinformation : A Guide to Promoting Information Integrity*.

[51] Kat Lo, *Toolkit for Civil Society and Moderation Inventory* (Meedan, 18 novembre 2020), https://meedan.com/reports/toolkit-for-civil-society-and-moderation-inventory/.

[52] Meedan, https://meedan.com.

[53] @Vijaya and Matt Derella, "An Update on Our Continuity Strategy during COVID-19," *Twitter Company* (blog) (Twitter, 1er avril 2020), https://blog.twitter.com/en_us/topics/company/2020/An-update-on-our-continuity-strategy-during-COVID-19.

[54] USAID et National Democratic Institute, « Platform Specific Engagement for Information Integrity » dans *Countering Disinformation : A Guide to Promoting Information Integrity*, (Consortium for Elections and Political Process Strengthening, 2021), https://counteringdisinformation.org/node/2722/.

Avant d'élaborer une campagne de communication stratégique et avant l'élection elle-même, prenez le temps de réfléchir à la més/désinformation et aux récits erronés qui apparaissent inévitablement avant, pendant et après les élections, afin d'être prêt à communiquer de manière positive et stratégique bien à l'avance. Les campagnes courantes de manipulation de l'information comprennent des contenus qui sèment la confusion sur les procédures de vote ou les processus techniques, tels que des heures de vote erronées ; des contenus qui peuvent entraîner une privation directe de participation des électeurs, tels que des faux rapports sur un environnement de vote dangereux ou des lieux de vote inefficaces ou fermés ; et des contenus qui peuvent délégitimer l'élection, tels que des récits de fraude électorale généralisée, d'infrastructure de vote défaillante ou de théories du complot à grande échelle.[55]

Pendant que vous abordez les faux récits potentiels, commencez à planifier et à convenir de récits et de messages prêts à l'emploi et bien conçus, qui peuvent être déployés rapidement et durablement tout au long de l'élection. Gardez à l'esprit les meilleures pratiques énumérées ci-dessous lorsque vous planifiez votre campagne de communication stratégique afin de vous assurer que le message est clair dès le départ et qu'il reste cohérent et facile à comprendre tout au long de l'élection.

- **Étudiez** soigneusement **votre public** et planifiez votre campagne.
  - Qui est votre (vos) public(s) ?
  - Quel est le but de votre message ?
  - Qu'est-ce qui trouvera un écho auprès de votre public ? Comment construire un message inclusif ?

- Définissez clairement vos **objectifs de communication** et restez en droite ligne avec ces derniers.

- **Créez le contenu.** Concentrez-vous sur des messages qui proposent des actions à votre public. Que leur demandez-vous de faire ?

- **Choisissez les plateformes et les tactiques** pour partager votre contre-récit. Tenez compte de l'accessibilité et de l'inclusion dans le choix de votre plateforme ; diversifiez les voies de communication pour inclure les canaux accessibles dans les zones à faible bande passante ; et utilisez des graphiques, des chansons, des sketchs ou d'autres méthodes de communication innovantes pour les personnes qui ne savent pas lire.

- **Évaluez l'impact.** Continuez à mener des recherches et à observer le dialogue tout en gardant à l'esprit vos objectifs de communication initiaux. Si les conditions changent, envisagez d'adapter votre message pour vous assurer d'atteindre vos objectifs de communication initiaux.

Bien que toute manipulation de l'information ne nécessite pas qu'on y réponde (*voir la section sur le silence stratégique à la page 41*), de très nombreux faux récits nécessiteront une attention particulière lorsqu'ils seront connus du public gagneront en popularité. Toute communication publique concernant la manipulation de l'information, qu'elle soit proactive ou réactive, doit faire preuve de **vérité, ouverture, équité et exactitude**.[56] Pour communiquer efficacement sur la désinformation, vous devez vous pencher sur les points suivants :

- **Rapidité d'exécution.** La rapidité est essentielle pour contrer efficacement la manipulation de l'information. Cela signifie qu'il faut élaborer des protocoles de communication stratégique qui concilient rapidité et précision, avec des directives claires sur les approbations nécessaires et les étapes de communication. Plus la désinformation reste sans réponse, plus elle a de chances d'être efficace.

- **Messages.** Toutes les communications doivent être exactes, fondées sur des valeurs et suffisamment convaincantes pour être prises en compte (voir Pourquoi la désinformation devient-elle virale ?). Votre message doit faire preuve d'empathie face aux préoccupations et suivre les protocoles de facilitation de lecture « Easy Read » décrits ici.[57] Vous trouverez des conseils supplémentaires sur l'élaboration d'une

[55] Election Integrity Partnership, « Election Official Handbook : Preparing for Election Day Misinformation » (20 octobre 2020), https://www.eipartnership.net/news/how-to-prepare-for-election-day-misinformation#Common%20Narratives.

[56] James Pamment et al., RESIST : *Counter-Disinformation Toolkit* (Government Communication Service, 2019), https://3x7ip91ron4ju9ehf2un-qrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf.

[57] People First, « A Guide to Making Easy Read Information » (Nouvelle-Zélande : Office for Disability Resources, Ministère du développement social, s.d.), https://www.odi.govt.nz/guidance-and-resources/a-guide-to-making-easy-read-information/.

campagne de communication convaincante dans la boîte à outils Co/Act.[58]

- **Évitez l'amplification accidentelle.** Si les communications s'opposent directement à une inexactitude, le message doit être formulé de manière à garantir l'amplification de la vérité plutôt que d'attirer accidentellement plus d'attention sur l'inexactitude. Encadrer une affirmation non prouvée entre deux vérités permet de mieux mettre l'accent sur l'exactitude de l'information plutôt que de simplement l'énoncer.

Pourquoi la désinformation devient-elle virale ?

Pour lutter efficacement contre les « fake news », il est important de comprendre comment et pourquoi elles se propagent si rapidement. À l'ère des réseaux sociaux, l'ampleur de la propagation de la désinformation est souvent liée à la réaction émotionnelle que le récit sous-jacent est capable de susciter. Le fait de susciter des émotions telles que le dégoût, la surprise, la colère, la peur et le mépris peut jouer un rôle essentiel dans la rapidité avec laquelle les nouvelles sont partagées. La désinformation est souvent conçue de manière à jouer sur ces émotions, en tirant parti des vulnérabilités dans la façon dont nous formons nos opinions et en exacerbant les divisions et les préjugés existants pour encourager les émotions à prendre le pas sur la raison ou la logique. L'utilisation de l'humour, de l'empathie, de la créativité et d'images ou de graphiques intéressants dans vos communications peut aider les messages véridiques à concurrencer la désinformation.

- **Partenariat / Réseaux.** Souvent, d'autres groupes ou réseaux partagent les mêmes intérêts et le fait de travailler ensemble augmente l'efficacité et renforce la crédibilité des informations lorsqu'elles sont partagées par plusieurs sources. Envisagez de vous associer à des réseaux existants ou à des influenceurs - qui ont un grand nombre d'abonnés et qui sont capables de toucher de larges groupes de la population - pour amplifier vos messages et établir des ponts avec des publics sceptiques (voir ici[59] pour un exemple de recours aux influenceurs par la Finlande pour diffuser des informations vraies sur les élections).

De nombreuses études ont montré que le meilleur moyen de prédire si les gens vont croire une rumeur est le nombre de fois où ils y sont exposés.[60] Les campagnes de communication devraient appliquer ce même principe à la promotion d'informations exactes et mettre l'accent sur la répétition d'un message clair et ciblé afin de diffuser plus efficacement la vérité.[61] Concentrez les communications sur ce que le gouvernement fait pour organiser et préparer les élections, en réfutant la més/désinformation, en mettant en avant la vérité et en cherchant à développer des relations avec les publics et les circonscriptions clés.

Étant donné le volume généralement élevé de récits de désinformation entourant les élections et la capacité souvent limitée des acteurs de la démocratie - notamment les OGE, les OSC et même les sites de médias de masse - à consacrer des ressources pour relever ce défi, il faut se concentrer sur la lutte contre les objectifs des campagnes de manipulation de l'information, qui visent souvent à exploiter les divisions existantes ou à changer l'opinion publique sur un candidat ou un parti politique, plutôt que de contrer les récits individuels. Les OGE, les OSC et les autres acteurs de la démocratie doivent se concentrer sur des stratégies de communication proactives, en consacrant des ressources à la promotion de la vérité plutôt qu'à la lutte contre les inexactitudes.

[58] Co/Act, Human Centered Design for Activists (Co/Act, National Democratic Institute, n.d.), https://www.ndi.org/sites/default/files/Co_Act%20Toolkit.pdf.

[59] Jon Henley, « Finland Enlists Social Influencers in Fight Against Covid-19 », *The Guardian*, 1er avril 2020, https://www.theguardian.com/world/2020/apr/01/finland-enlists-social-influencers-in-fight-against-covid-19.

[60] Lisa Fazio, David Rand et Gordon Pennycook, « Repetition Increases Perceived Truth Equally for Plausible and Implausible Statements », *Psychonomic Bulletin & Review* 26, n°5 (octobre 2019) : 1705-1710, https://doi.org/10.3758/s13423-019-01651-4.

[61] Norbert Schwarz et Madeline Jalbert, « When (Fake) News Feels True : Intuitions of Truth and the Acceptance and Correction of Misinformation », *The Psychology of Fake News : Accepting, Sharing, and Correcting Misinformation*, éd. Rainer Greifeneder, Mariela E. Jaffé, Eryn Newman et Norbert Schwarz (Routledge : 14 août 2020)), https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/46921/9781000179033.pdf?sequence=1&isAllowed=y.

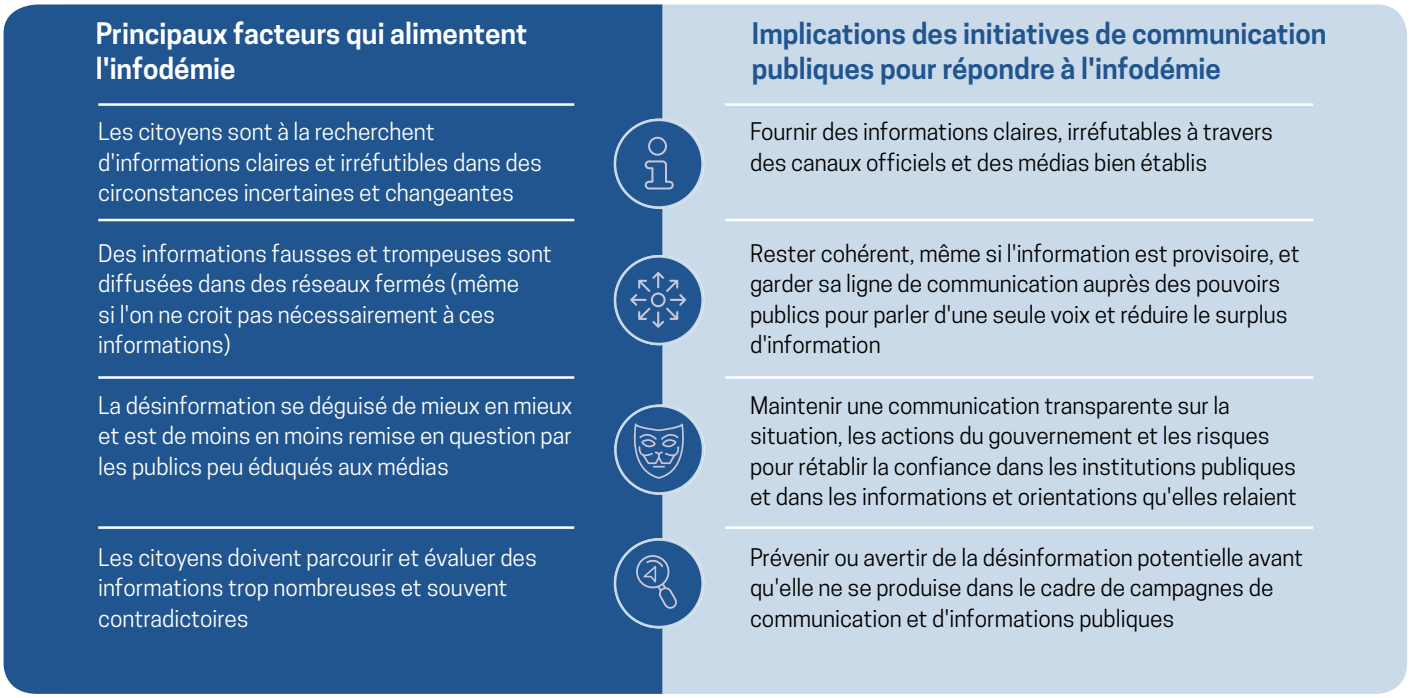
En général, tenez compte des étapes suivantes lorsque vous planifiez vos communications :

1. Identifiez les **faits clés** liés à l'élection qui sont les plus critiques pour réaffirmer continuellement leur véracité - tenez compte du qui, du quoi, du où, du quand et du comment des élections - et utilisez votre message pour établir les faits de base autant que possible.

2. Décidez des **canaux d'information** et des partenaires **les plus fiables** pour aider à transmettre le message; fournissez-leur des messages clairs ainsi que des conseils pour communiquer le message.

3. Tout en partageant régulièrement votre message, continuez à **surveiller la couverture médiatique**, notamment les réseaux sociaux, et établissez une boucle d'information en retour pour savoir comment vos messages sont repris et comment on y répond.

4. **Modifiez votre message** si les conditions changent (revirement le jour des élections ou flambées de violence) afin de démontrer votre réactivité, mais veillez à maintenir des objectifs de communication clairs et la cohérence du message.



Source : Image adaptée du rapport de l'Organisation de coopération et de développement économiques (OCDE) Transparency, communication and trust : The role of public communication in responding to the wave of disinformation about the new Coronavirus.[62]

[62] « Transparency, Communication and trust : the role of public communication in responding to the wave of disinformation about the new Coronavirus », (OCDE, 3 juillet 2020)), https://www.oecd.org/coronavirus/policy-responses/transparency-communication-and-trust-the-role-of-public-communication-in-responding-to-the-wave-of-disinformation-about-the-new-coronavirus-bef7ad6e/.

Pour des conseils plus approfondis sur les communications visant à contrer la manipulation de l'information, consultez les ressources ci-dessous.

La boîte à outils RESIST pour la lutte contre la désinformation Annex E : Strategic Communication ***(Outil)*** est un guide étape par étape pour déployer les modèles FACT et OASIS pour une communication stratégique efficace.[63]

Countering Information Influence Activities : A Handbook for Communicators, ***(Guide)*** publié par l'Agence suédoise de services de secours (Swedish Civil Contingencies Agency), comprend des conseils détaillés sur la manière de choisir la meilleure réponse en matière de communication en fonction de la manipulation de l'information.[64]

Les manipulations de l'information : Un défi pour nos démocraties ***(Guide)*** propose des études de cas et des suggestions utiles basées sur de précédentes campagnes de communication stratégique.[65]

Communications inclusives

Il est important d'adapter vos messages aux différents contextes et de s'efforcer délibérément d'atteindre des publics divers. Les groupes sociaux et thématiques qui sont marginalisés - dont les femmes, les immigrants et les minorités, entre autres - sont souvent les principales cibles des attaques de més/désinformation. Les campagnes de manipulation de l'information s'efforcent souvent d'exploiter les divisions socio-économiques existantes : les électeurs qu'on tente d'empêcher de participer sont souvent des communautés spécifiques et vulnérables et les partis pris et les préjugés sont souvent amplifiés pour semer la discorde, la confusion et la privation du droit de vote. Vous pouvez trouver plus d'informations sur la façon de comprendre les dimensions de genre de la désinformation en particulier dans le chapitre « Gender and Disinformation » du guide de lutte contre la désinformation du CEPPS.[66]

Compte tenu de l'objectif souvent explicitement clivant des campagnes de manipulation de l'information, il est absolument essentiel que les campagnes de communication s'attachent en priorité à atteindre les groupes marginalisés et ciblés et à fournir des informations précises qui autonomisent ces groupes en vue d'atténuer les impacts potentiels. À ce titre, nous recommandons aux acteurs de la démocratie de mettre en œuvre un large éventail de stratégies de communication avant, pendant et après l'élection. Envisagez de diversifier votre approche en vous associant à des réseaux de confiance et à des dirigeants communautaires et adaptez votre message pour qu'il s'adresse à des publics particuliers. Ce faisant, vous toucherez une plus grande partie de la population et des groupes plus vulnérables, ce qui augmentera les chances de supplanter les informations inexactes dans les espaces où elles sont le plus largement diffusées.

Quels que soient les divers canaux ou messages que vous utilisez, l'inclusion, l'accessibilité et la transparence doivent être au premier plan de votre stratégie. Les messages SMS, la radio et les médias traditionnels peuvent toucher une plus grande partie de la population dans les endroits où l'accès à Internet est coûteux ou faible. Les principes de facilitation de lecture Easy Read pour atteindre les populations peu alphabétisées et la création de contenus en plusieurs langues, notamment dans les langues autochtones, sont des éléments essentiels d'une communication accessible et de grande portée.[67] En diversifiant les communications sur des plateformes telles que Facebook, Twitter, Instagram et WhatsApp, entre autres, vous augmenterez les segments de la population que vous pourrez toucher. Enfin, efforcez-vous de produire un contenu facilement partageable pour une communication aussi efficace que possible, par exemple en utilisant des graphiques faciles à comprendre, lorsque c'est possible.

[63] James Pamment et al., « Annex E : Strategic Communication » dans *RESIST : Counter-Disinformation Toolkit* (Government Communication Service, 2019), https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/#Annex-E-Strategic-communication.

[64] *Countering Information Influence Activities : A Handbook for Communicators* (Swedish Civil Contingencies Agency, mars 2019), https://www.msb.se/RibData/Filer/pdf/28698.pdf.

[65] Jean-Baptiste Jeangène Vilmer et al., *Les manipulations de l'information : Un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées), août 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

[66] USAID et National Democratic Institute, « Understanding the Gender Dimensions of Disinformation » dans *Countering Disinformation : A Guide to Promoting Information Integrity* (Consortium for Elections and Political Process Strengthening, 2021), https://counteringdisinformation.org/topics/gender/0-overview-gender-disinformation.

[67] People First, « A Guide to Making Easy Read Information ». (Office for Disability Issues). https://www.odi.govt.nz/guidance-and-resources/a-guide-to-making-easy-read-information/.

Étude de cas : Soutenir l'accès aux médias indépendants pour les populations à faibles revenus en Amérique latine

Au cours de la dernière décennie, l'IRI a mené des programmes dans toute l'Amérique latine pour venir en soutien aux médias indépendants qui produisent et diffusent des informations indépendantes et fiables dans des contextes sociopolitiques en évolution rapide et constante, en ciblant souvent les secteurs à faible revenu qui ont moins de chances de recevoir ces informations ailleurs. Dans le cadre de son travail, l'IRI a constaté que les approches de terrain et la création d'alliances entre la société civile et les médias, ainsi que la prise en compte attentive des questions de sécurité, ont été essentiels pour collaborer de manière fructueuse avec un large éventail de parties prenantes afin d'améliorer la diffusion d'informations véridiques. Si votre organisation cherche à partager des informations véridiques de manière accessible aux secteurs à faibles revenus, envisagez de soutenir un large éventail de médias indépendants par le biais d'un réseau de contenus en ligne, imprimés, radiophoniques, télévisés et de réseaux sociaux, et établissez un réseau de diffusion en utilisant des outils tels que des émissions de radio, des messages de masse et des publicités numériques ciblées, ou des méthodes alternatives telles que des projections publiques, du théâtre de rue ou des spectacles d'humour.

Conseil : Évitez d'amplifier les fausses informations

La répétition d'une fausse information dans le but de la corriger peut parfois entraîner une croyance accrue dans cette fausse information. Ainsi, vos campagnes de communication doivent s'attacher à répéter des informations exactes sans faire référence aux informations que vous tentez de démystifier. Par exemple, une campagne efficace doit dire « Le jour du scrutin est le XXX. Ne vous fiez qu'aux informations provenant de sources officielles », et non « Le jour du scrutin n'est pas le XXX. Ne vous fiez pas aux informations de XXX ».

Études de cas des tactiques de communication

Étude de cas : Communications de la Commission électorale nationale indépendante du Nigeria (INEC)

En période électorale, l'INEC du Nigeria organise des briefings télévisés quotidiens, participe à des interviews télévisées en direct et publie régulièrement des communiqués de presse pour expliquer les politiques et les actions de la commission.[68] Cette communication régulière et proactive permet non seulement d'informer le grand public des activités de la Commission, mais aussi de créer la transparence et la confiance autour du processus électoral. Les activités de l'INEC se poursuivent également au-delà des périodes électorales, avec la création de ressources accessibles d'éducation des électeurs qui expliquent en détail comment et où voter, comment s'inscrire, ainsi que les droits et responsabilités des électeurs. L'INEC produit également régulièrement un bulletin d'information et des communiqués de presse qui contiennent de manière transparente des mises à jour sur les processus électoraux. Ces efforts ont permis d'amplifier activement les informations concernant les processus électoraux au Nigeria, contribuant ainsi à contrecarrer de manière proactive toute manipulation de l'information autour des élections nigérianes.

[68] Independent National Electoral Commision Nigeria, https://www.inecnigeria.org.

Étude de cas : La campagne « Fast Fair Fun » de Taïwan

La clé du succès de la gestion de la pandémie à Taïwan a été d'adopter une stratégie de communication unique, et finalement extrêmement efficace, qui pourrait être imitée dans des contextes liés aux élections. Plutôt que de contrer ou de vérifier les informations erronées sur le virus, le gouvernement taïwanais a lancé une campagne de communication basée sur trois adjectifs : équitable, rapide et amusant (*fair, fast, fun*).

- **Rapide :** Dès que les citoyens ont commencé à signaler des foyers et des inquiétudes, le gouvernement taïwanais a immédiatement adopté des politiques visant à suspendre les voyages à destination et en provenance de la Chine, ce qui témoigne de la confiance et de la transparence entre l'État et ses citoyens. En outre, les informations, souvent partagées par le biais de mèmes, ont été rapidement communiquées pour promouvoir la vérité avant que la désinformation ne se propage.
- **Équitable :** Afin de maximiser la transparence et l'exhaustivité de l'information, l'État a pris des mesures pour rendre publiques les données relatives à la santé, notamment celles concernant l'approvisionnement en masques. Cela a permis à tous les citoyens d'accéder à des informations essentielles et a garanti un accès équitable pour tous.
- **Amusant :** L'État a favorisé l'humour plutôt que les rumeurs et a créé des campagnes de communication humoristiques pour dissiper les rumeurs sur l'approvisionnement en masques, la façon dont le COVID-19 se propage, etc., notamment en désignant un « chien porte-parole » pour transmettre les gestes barrière au public de manière accessible et divertissante. Cette campagne a démontré que l'humour factuel se répand plus vite que la rumeur.

Vérification des informations

La vérification des informations ou *fact-checking* est un processus qui vise à vérifier les informations et à fournir une analyse précise et impartiale d'une allégation. Bien que la vérification des informations puisse à elle seule être inefficace pour protéger l'intégrité de l'environnement de l'information entourant une élection - l'impact direct des corrections est souvent très limité - elle peut s'avérer utile pour corriger des éléments clés de la manipulation de l'information liée aux élections.

Si votre organisation cherche à développer des compétences qui vont au-delà du signalement de préoccupations à des vérificateurs d'informations et souhaite développer sa capacité à effectuer régulièrement et durablement des vérifications d'informations elle-même, prenez en compte les conseils ci-dessous. Comme le souligne le guide complet élaboré par Poynter, la vérification des informations relatives aux élections est guidée par une question principale : **« Comment le savons-nous ? »**[69]

[69] Alexios Mantzarlis, « Module 5 : Vérification des faits (fact-checking) 101 », dans *Journalisme, « Fake News » et Désinformation* (UNESCO, 2018), https://en.unesco.org/sites/default/files/module_5.pdf.

De manière générale, la vérification des informations repose sur trois étapes :[70]

1 Trouvez des allégations vérifiables en surveillant les réseaux sociaux, les médias grand public et les déclarations politiques discutant d'informations liées aux élections afin d'identifier une allégation douteuse ou incorrecte qui peut être vérifiée objectivement. Lorsque vous choisissez une allégation, tenez compte des éléments suivants :

a) Quel est le degré de viralité de l'allégation (quelle est son étendue, sa portée et sa propagation) ?
b) Quelle est la source de l'allégation ? (Qui l'a partagée ?)
c) De quelle nature est l'allégation ? (Peut-elle conduire à la violence ? Est-ce une provocation ?)

2 Une fois que vous avez choisi une allégation, **trouvez les faits** en rassemblant les meilleures preuves disponibles concernant cette allégation, tout en veillant à évaluer la fiabilité de vos sources. Parmi les outils disponibles pour cette étape vous disposez de :

a) Recherche Google Images pour déterminer l'origine des photos ou des vidéos.[71]
b) TinEye Reverse Image Search pour déterminer depuis combien de temps et à quelle fréquence une image est disponible et comment elle a été modifiée.[72]
c) Google Fact Check Explorer pour trouver des résultats de vérification d'informations existants concernant une personne, un sujet ou une question.[73]
d) Amnesty International YouTube DataViewer pour déterminer si une vidéo ou des parties de vidéo ont été précédemment mises en ligne.[74]
e) The Global Disinformation Index qui permet de déterminer la probabilité de désinformation d'un média spécifique.[75]

Vous pouvez trouver une liste solide de ressources supplémentaires ici.[76]

3 Rectifiez les données en évaluant l'allégation à la lumière des meilleures preuves disponibles, généralement sur une échelle de véracité : vrai, principalement vrai, à moitié vrai, principalement faux, faux et mensonge évident.

[70] « How to Fact-Check Like a Pro » (bibliothèque publique d'Albuquerque et du comté de Bernalillo, s.d.), https://abqlibrary.org/FakeNews/FactCheck.

[71] Google Images (Google, s.d.), https://images.google.com.

[72] TinEye Reverse Image Search (TinEye, s.d), https://tineye.com.

[73] Google Fact Check Explorer (Google, s.d), https://toolbox.google.com/factcheck/explorer.

[74] YouTube DataViewer (Amnesty International, s.d.), https://citizenevidence.amnestyusa.org.

[75] Global Disinformation Index (GDI, s.d.), https://disinformationindex.org.

[76] "Tools That Fight Disinformation Online" (RAND Corporation, n.d.), https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html.

Pour obtenir plus de conseils et des modules de formation solides afin de développer les compétences nécessaires pour identifier, évaluer et vérifier efficacement les allégations, et pour former d'autres personnes à la vérification d'informations également, pensez à consulter les ressources suivantes :

- La bibliothèque gratuite de formations First Draft, comprenant des cours en ligne, des boîtes à outils et des ressources.[77]
- Le programme et jeu en ligne Learn to Discern (L2D) pour renforcer les compétences en matière de médias et d'information.[78]
- Trust and Verification, un cours en ligne gratuit, qui montre comment établir la confiance en tant que journaliste ou créateur de contenu à une époque où la manipulation de l'information est répandue.[79]

La vérification des informations en soi est une stratégie imparfaite. Lorsque votre organisation envisage d'évaluer la véracité des faits dans l'espoir de contrer ou de démystifier de fausses informations, gardez à l'esprit les préjugés, non seulement de votre public mais aussi de vous-même, qui pourraient influencer la perception de la vérité. En outre, si vous soupçonnez que de faux vérificateurs d'informations pourraient obscurcir la sphère d'information, référez-vous au code de principes des vérificateurs d'informations de International Fact-Checking Network pour déterminer si leur comportement est digne de confiance.[80]

À mettre en évidence : Partenariat avec les médias

Il est important, dans le cadre des efforts de protection des élections, de travailler avec les médias locaux afin de fournir un contenu faisant autorité avant et pendant les élections et de s'assurer qu'ils font partie de votre équipe de partenariat pour contrer, anticiper et démystifier les faux récits et contenus. En tant que tel, le fait de veiller à ce que les médias indépendants soient équipés des meilleures pratiques pour identifier, répondre et dénoncer les faux récits et soient en mesure de fournir rapidement un contenu faisant autorité soutiendra la mission globale de lutte contre la manipulation de l'information pendant les élections. Il existe un certain nombre de ressources pour les médias, notamment des cours de formation gratuits disponibles sur le site web de First Draft'.[81]

[77] First Draft Training (First Draft, s.d.), https://firstdraftnews.org/training/.

[78] Learn to Discern, "Media Literacy Training" (IREX, s.d.), https://www.irex.org/project/learn-discern-l2d-media-literacy-training.

[79] Craig Silverman, instructeur, « Trust and Verification in an Age of Misinformation », cours en ligne (Centre Knight pour le journalisme aux Amériques) https://journalismcourses.org/es/course/trustandverification/.

[80] International Fact-Checking Network, « Fact-Checkers' Code of Principles » (Poynter, 15 septembre 2016), https://www.poynter.org/ifcn-fact-checkers-code-of-principles/.

[81] First Draft, « Training Resources », https://firstdraftnews.org/training/.

Efforts collaboratifs de vérification des informations

Si les journalistes sont souvent les principaux acteurs des efforts de vérification des informations, bon nombre d'initiatives de vérification des informations les plus réussies sont le résultat d'une collaboration entre des groupes de parties prenantes. Les OSC, les ONG et même les OGE peuvent compléter les efforts des journalistes en agissant comme des sources d'information fiables et en offrant une expertise supplémentaire. Vous trouverez ci-dessous des exemples de collaborations en matière de vérification des informations qui impliquent plusieurs acteurs de la démocratie.

- **StopFake** est une organisation de fact-checking fondée par des professeurs et des étudiants ukrainiens pour identifier et enquêter sur les fausses informations concernant les événements en Ukraine.[82]
- **Africa Check** est la première organisation africaine indépendante à but non lucratif qui couvre le Kenya, le Nigeria, le Sénégal et l'Afrique du Sud. Elle analyse les déclarations publiques importantes et publie des rapports de vérification des informations pour orienter le débat public.[83]
- **Chequeado** est une organisation sans but lucratif ni affiliation politique qui se consacre à la vérification du discours public et à la lutte contre la més/désinformation. Chequeado réunit tous les groupes de parties prenantes dans leurs efforts pour combattre la més/désinformation.[84]
- **The International Fact-Checking Network (IFCN)** est une unité du Poynter Institute qui réunit des vérificateurs d'informations du monde entier et qui promeut activement les meilleures pratiques et les échanges dans ce domaine, en plus de proposer des formations et des bourses.[85]
- **Verificado** est une plateforme collaborative de vérification des informations qui vise à combattre la désinformation et les fake news entourant les élections mexicaines, ainsi qu'à vérifier les rapports sur le processus électoral (*voir l'étude de cas du Mexique à l'annexe A, page 53, pour plus de détails*).[86]
- **Des vérificateurs d'informations tiers** se sont associés à Facebook pour examiner et évaluer l'exactitude des articles et des publications Facebook. Dans des pays tels que la Colombie, l' Indonésie et l'Ukraine, ainsi que dans plusieurs États membres de l'UE, Facebook a chargé des groupes - par le biais de ce qui est décrit comme « un processus de candidature complet et rigoureux » établi par l'IFCN - de devenir des vérificateurs d'informations de confiance qui valident le contenu, apportent leur contribution aux algorithmes qui définissent le fil d'actualité et déclassent et signalent le contenu identifié comme faux.[87]

Des ressources mondiales de vérification des informations peuvent également s'avérer utiles, comme Claim Buster et AP Fact Check,[88] entre autres.

[82] StopFake (Media Reforms Center, s.d.), https://www.stopfake.org/en/main/.

[83] Africa Check, (Africa Check, s.d.), https://africacheck.org.

[84] Chequeado, (La Voz Pública Foundation, s.d.), https://chequeado.com.

[85] The International Fact-Checking Network (Poynter, s.d.), https://www.poynter.org/ifcn/.

[86] Verificado, (Verificado, s.d.), https://verificado.com.mx/tag/fact-checking/.

[87] Page d'aide pour les entreprises de Facebook, « Vérification des informations sur Facebook » (Facebook, s.d.), https://www.facebook.com/business/help/2593586717571940; Tessa Lyons, « Hard Questions : How is Facebook's Fact-Checking Program Working? » Hard Questions (blog), Facebook, 14 juin 2018, https://about.fb.com/news/2018/06/hard-questions-fact-checking/; The International Fact-Checking Network (Poynter, s.d.), https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles.

[88] ClaimBuster (IDIR Lab, Université du Texas à Austin, s.d.), https://idir.uta.edu/claimbuster/; AP Fact Check (AP, n.d.), https://apnews.com/hub/ap-fact-check.

Lorsque votre organisation surveille la sphère des informations à la recherche d'allégations préoccupantes autour des élections, gardez un œil sur les faits clés, décrits ci-dessous, qui pourraient être manipulés pour tromper ou dissuader les électeurs.

Faits clés pendant un processus électoral:	
Qui ?	Les entités et personnes qui organisent les élections.
Quoi ?	Les machines, systèmes et manières de voter.
Quand ?	Les jour(s), heures et échéances de l'enrôlement et du calendrier électoral.
Où ?	Les lieux où voter.
Comment ?	Comment se déroule le vote.

Si votre organisation détecte des informations trompeuses concernant le qui, le quoi, le quand, le où et le comment d'une élection, prenez le temps de signaler l'allégation

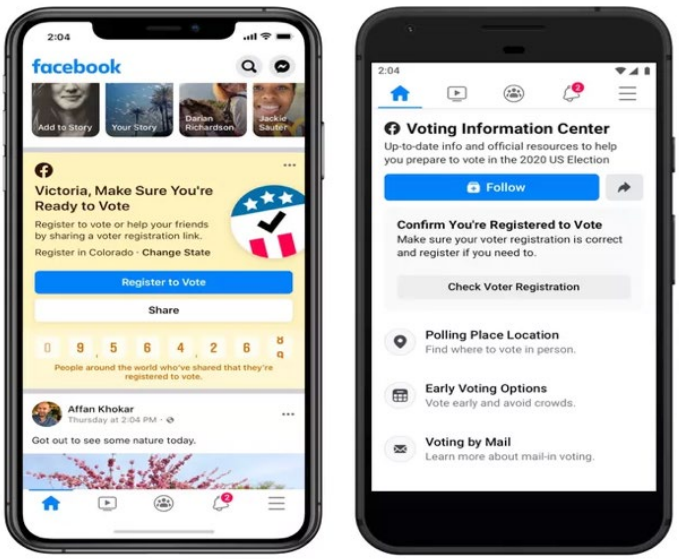
Initiatives des plateformes de réseaux sociaux pour accroître l'accès à des informations crédibles

Un élément clé de la vérification des informations est l'accès à des informations crédibles, fiables et sans restriction, en ligne et hors ligne. En réponse aux efforts de plaidoyer et aux plaintes concernant la complicité des plateformes de réseaux sociaux, certaines plateformes ont lancé des initiatives pour accroître l'accès à des informations crédibles, allant de la redirection des utilisateurs vers des sources fiables d'informations liées aux élections, à l'élargissement de l'accès des API pour permettre la recherche, en passant par l'amélioration des fonctionnalités des produits pour décourager le partage de fausses informations. Lorsque votre organisation cherche à vérifier les informations relatives à une élection, gardez ces actions à l'esprit pour capitaliser sur les initiatives existantes ou pour plaider en faveur d'initiatives similaires si elles n'existent pas encore dans votre pays.

Facebook

Facebook a mis en œuvre un certain nombre d'initiatives visant à améliorer l'accès aux données et aux informations faisant autorité, tant pour les vérificateurs d'informations que pour les chercheurs. L'une des fonctionnalités consiste à apposer des étiquettes ou des boutons d'information sur les messages faisant référence à certains sujets sensibles à la manipulation de l'information, tels que le COVD-19, les vaccins et les élections. Par exemple, l'entreprise étiquette le contenu faisant référence aux « bulletins de vote » ou à « vote » (indépendamment de la véracité du contenu) pendant une élection, en dirigeant les utilisateurs de Facebook vers les informations officielles sur le vote. Ces étiquettes ont été largement utilisées lors de l'élection présidentielle américaine de 2020 et ont également été utilisées lors d'élections dans d'autres pays, notamment en Colombie, au Royaume-Uni et en Allemagne, entre autres.[89]

Par exemple, en préparation des élections locales de 2019 en Colombie, Facebook s'est associé au Conseil national électoral (CNE) de Colombie pour fournir aux citoyens des informations crédibles sur le vote en créant des rappels du jour du scrutin et un bouton « Électeur informé », qui redirigeait l'utilisateur vers l'autorité électorale locale pour obtenir des informations sur le lieu et la date du vote. Ces fonctionnalités ont été utilisées dans d'autres élections dans le monde. D'autres exemples de fonctionnalités d'information des électeurs sur Facebook sont présentés ci-dessous :



Facebook a également commencé à étiqueter certains médias contrôlés par l'État afin d'offrir une plus grande transparence sur les sources d'information de la plateforme. Ces étiquettes apparaissent actuellement sur les pages et sur les bibliothèques d'annonces de la plateforme; elles seront ultimement étendues pour être plus largement visibles. Les étiquettes s'appuient

[89] Hannes Grasegger, « Facebook Says its 'Voter Button' is Good for Turnout. But Should the Tech Giant be Nudging Us At All? » *The Guardian*, 15 avril 2018, https://www.theguardian.com/technology/2018/apr/15/facebook-says-it-voter-button-is-good-for-turn-but-should-the-tech-giant-be-nudging-us-at-all.

sur les fonctionnalités de transparence déjà en place sur les pages Facebook, qui comprennent des panneaux fournissant un contexte sur la manière dont la page est administrée (y compris des informations sur les utilisateurs qui gèrent la page et les pays à partir desquels ils opèrent), ainsi que des informations indiquant si la page est contrôlée par un État.[90]

Twitter

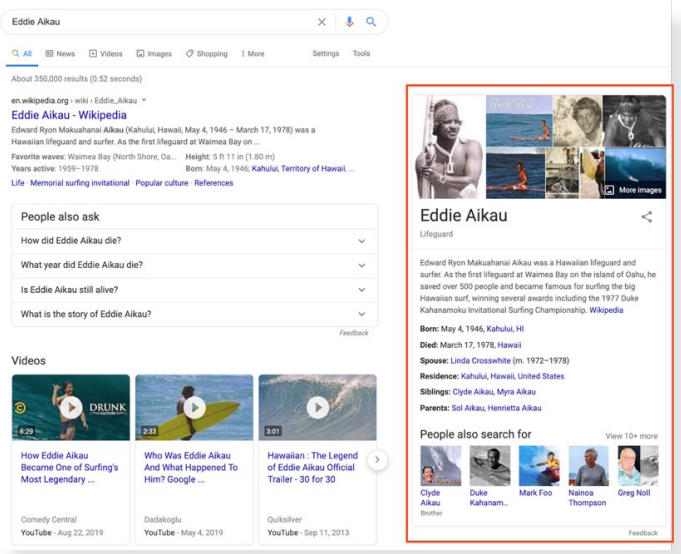
Twitter a mis au point un certain nombre de politiques, de campagnes et de fonctionnalités de ses produits pour permettre aux utilisateurs d'accéder à des informations crédibles et faisant autorité. En 2019, avant l'élection en Inde, Twitter a entrepris des efforts substantiels pour permettre aux utilisateurs d'accéder à des informations crédibles sur l'élection, tout en faisant évoluer son produit, en mettant à jour les règles et en s'attaquant à la manipulation de l'information sur son service affectant l'Inde dans son ensemble.[91] Ces efforts ont également porté sur l'ajout de fonctionnalités supplémentaires et des améliorations du produit afin d'empêcher les utilisateurs de partager des informations trompeuses sur le vote. Plus récemment, Twitter a annoncé un partenariat avec Associated Press (AP) et Reuters afin d'étendre ses efforts pour mieux mettre en évidence les informations fiables ainsi que pour ajouter plus de contexte aux nouvelles et aux tendances qui circulent sur sa plateforme.[92]

WhatsApp

En tant que plateforme de messagerie cryptée, WhatsApp met à la disposition des utilisateurs et des chercheurs des informations limitées sur les activités menées sur ses services. Cependant, WhatsApp a donné accès à son API afin de soutenir certaines initiatives de recherche. La société a élargi l'accès à l'API par le biais du système Zendesk, en particulier pour les groupes liés à la coalition First Draft, tels que Comprova au Brésil et CrossCheck au Nigeria.[93] Cette approche a été utilisée pour collecter des données sur des événements politiques, la diffusion de fausses informations et de discours haineux et d'autres objectifs de recherche. International Fact-Checking Network a également développé une collaboration avec WhatsApp qui permet l'accès à l'API pour certains types de recherche

Google

Les fiches info de Google sont des boîtes d'informations qui apparaissent lorsque les utilisateurs recherchent des personnes, des lieux, des objets et des organisations figurant dans le Knowledge Graph, la base de données de faits de Google.[94] Ces boîtes d'information générées automatiquement, illustrées ci-dessous, fournissent un instantané des informations sur un sujet particulier. Les fiches info ont été créés pour fournir des informations et remédier à la manipulation des informations, mais elles ont tout de même été à l'origine de l'amplification de certaines désinformations.[95]



[90] Nathaniel Gleicher, "Labeling State-Controlled Media on Facebook" (Facebook, 4 june, 2020), https://about.fb.com/news/2020/06/labeling-state-controlled-media/.

[91] Colin Crowell et @misskaul, « Protecting the Integrity of the Election Conversation in India » (Twitter, 21 février 2019), https://blog.twitter.com/en_in/topics/events/2019/election-integrity.

[92] Sarah Perez, « Twitter Partners with AP and Reuters to Address Misinformation on Its Platform », TechCrunch, 2 août 2021, https://techcrunch.com/2021/08/02/twitter-partners-with-ap-and-reuters-to-address-misinformation-on-its-platform/.

[93] « Zendesk Introduces WhatsApp for Zendesk » (Zendesk, 16 août 2019), https://www.zendesk.com/company/press/zendesk-introduces-whatsapp-zendesk/; First Draft, « Introducing the First Draft Coalition » (First Draft, 18 juin 2015), https://medium.com/1st-draft/introducing-the-first-draft-coalition-e557fdacd1a6;First Draft, « Comprova » (First Draft, s.d.), https://firstdraftnews.org/tackling/comprova/; First Draft, « CrossCheck Nigeria » (First Draft, s.d.), https://firstdraftnews.org/tackling/crosscheck-nigeria/

[94] Aide Fiche info, « À propos des fiches info » (Google, s.d.), https://support.google.com/knowledgepanel/answer/9163198?hl=fr ; Aide Fiche info, « Fonctionnement du Knowledge Graph de Google » (Google, s.d.), https://support.google.com/knowledgepanel/answer/9787176?hl=fr.

[95] Barry Schwartz, « Google adds new knowledge panel to provide information about news publishers », Search Engine Lab (7 novembre 2017), https://searchengineland.com/google-adds-new-knowledge-graph-learn-news-publishers-286394; Lora Kelley, « The Google Feature Magnifying Disinformation », *Atlantic* (23 septembre 2019, https://www.theatlantic.com/technology/archive/2019/09/googles-knowledge-panels-are-magnifying-disinformation/598474/.

YouTube

Afin de fournir aux utilisateurs des informations précises, YouTube propose les fonctions Actualités et Top des actualités, qui mettent en avant des informations provenant de sources d'information vérifiées.[96] Dans le cadre des efforts continus de la société, YouTube a indiqué qu'elle développait l'utilisation de panneaux d'information pour fournir aux utilisateurs un contexte supplémentaire provenant de vérificateurs d'informations.[97]

Le silence stratégique

Comme nous l'avons mentionné plus haut dans ce guide, toute manipulation d'informations ne nécessite pas une réponse. Même si les compétences liées au repérage des fausses informations s'améliorent, il est essentiel, lorsque l'on décide de démystifier une contre-vérité, d'éviter d'amplifier le message même que l'on tente de corriger. Décider activement de ne pas démentir une fausse allégation est un silence stratégique. Pour déterminer si une incertitude justifie ou non une réponse, évaluez les éléments suivants :

- Quel est le niveau de risque associé à l'allégation ? Peut-elle conduire à la violence ou à des dommages physiques ? Menace-t-elle de compromettre de manière significative les élections et/ou la confiance des électeurs dans le processus ou les résultats ?
- Quels sont les niveaux d'adhésion ?
- Quelle est la portée de l'attention ?
- Qui a créé l'incertitude ? S'agit-il d'une voix établie qui peut être considérée comme crédible ? Quelle influence a-t-elle ?
- L'inexactitude a-t-elle déjà eu un effet démontré

Si les niveaux d'adhésion à l'égard de l'allégation sont faibles, si l'attention n'est pas généralisée, s'il n'y a pas d'effet démontré ou si l'allégation n'a pas ou peu d'impact sur le comportement et les croyances des électeurs, il est peu probable que l'allégation nécessite une intervention. Si l'allégation ne nécessite pas encore de réponse, nous vous recommandons d'enregistrer l'incident et de l'ajouter à tout schéma de surveillance existant en cas de pertinence ou d'adhésion accrue. Bien qu'il puisse sembler contre-intuitif de laisser une fausse information non vérifiée, le fait de contrer une allégation qui n'a pas suscité beaucoup d'attention ni obtenu beaucoup d'influence peut avoir l'effet d'amplifier ou de renforcer involontairement une inexactitude simplement en la répétant.

Réflexion sur les délais

WIl n'existe pas de délai précis pour la durée du silence que vous ou votre organisation devez maintenir, vous devrez maintenir une surveillance continue du ou des faux récits ou des informations manipulées identifiés pour déterminer le moment où la communication est nécessaire. Si un récit ou un contenu faux ou trompeur commence à gagner du terrain, que ce soit en l'espace de quelques jours ou de quelques semaines, il peut s'avérer prudent, voire nécessaire, d'ajuster votre stratégie pour faire face à ce faux récit.

[96] Aide YouTube, « Sections "Actualités" et "Top des actualités" sur YouTube » (YouTube, s.d.), https://support.google.com/youtube/answer/9057101?hl=fr.

[97] PTI, « Fighting fake news: YouTube to show 'information panels' on news-related videos », The Economic Times (7 mars 2019), https://economictimes.indiatimes.com/magazines/panache/fighting-fake-news-youtube-to-show-information-panels-on-news-related-videos/articleshow/68302365.cms.

Ressources pour répondre à la désinformation

Une fois que vous avez identifié la désinformation, les outils et ressources énumérés ci-dessous peuvent vous aider à la contrer ou à y répondre.

- **Demtech/Comprop Navigator *(Liste de ressources)*** : Dans le cadre du projet sur la propagande informatique *Computational Propaganda*, l'Oxford Internet Institute a mis au point le Demtech Navigator, un guide en ligne destiné aux organisations de la société civile qui fournit des outils, des informations et des ressources provenant de diverses sources et proposant des stratégies pour aborder la désinformation, les fake news, la cybersécurité et le harcèlement en ligne.[98]
- **Base de données de RAND Corporation d'outils de lutte contre la désinformation *(Liste de ressources)*** : La RAND Corporation a compilé une base de données d'outils développés par des organisations à but non lucratif aux États-Unis pour lutter contre la désinformation, notamment sur les réseaux sociaux. Il s'agit d'outils liés aux produits ou aux ressources, plutôt que de ressources fournissant des informations générales. La base de données comprend des outils de fact-checking, des traqueurs de bots et des instruments de vérification d'images.[99]
- **Guide de lutte contre la désinformation du CEPPS *(Guide)***: Commandé par l'USAID, le Consortium pour le renforcement des élections et des processus politiques (CEPPS) - composé du National Democratic Institute, de l'International Republican Institute et de l'International Foundation for Electoral Systems - a développé le Guide de lutte contre la désinformation du CEPPS comme une ressource pour les organisations de la société civile, les gouvernements et les organismes de gestion des élections. Le guide propose des recherches sur la lutte contre la désinformation et une base de données consultable sur les initiatives prises par des organisations de la société civile et d'autres parties prenantes du monde entier pour lutter contre la désinformation.[100]
- **Digital Sherlocks *(Réseau)***: Digital Sherlocks est un programme lancé par l'Atlantic Council visant à former un réseau d'individus à des outils open-source pour contrer la désinformation. À ce jour, l'Atlantic Council a formé plus de 1,500 personnes dans le cadre de 50 ateliers sur six continents afin de soutenir la résilience numérique mondiale.[101]

[98] DemTech Navigator (Programme on Democracy and the Internet, Oxford University Institute, s.d.), https://navigator.oii.ox.ac.uk.

[99] « Tools That Fight Disinformation Online » (RAND Corporation, s.d.), https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html.

[100] International Foundation for Electoral Systems, International Republican Institute, National Democratic Institute. "Database of Informational Interventions" (Consortium for Elections and Political Process Strengthening, 2021). https://counteringdisinformation.org/index.php/interventions.

[101] 360/Digital Sherlocks (Atlantic Council, Digital Forensic Research Lab, s.d.), https://www.digitalsherlocks.org.

Étape 3 Renforcement de la résilience

Afin de construire un environnement de l'information dynamique et robuste, les démocraties existantes et naissantes doivent donner la priorité à la mise en place de processus démocratiques résistants aux troubles de l'information, notamment la manipulation de l'information. Dans ce guide, ce que nous entendons par résilience *est la capacité des citoyens à participer et à contribuer aux processus démocratiques tels que les élections*. Les citoyens doivent avoir les compétences nécessaires pour trouver, identifier, réfléchir de manière critique et évaluer les informations relatives aux élections qu'ils consomment en ligne et hors ligne, tandis que les institutions publiques, privées et de la société civile doivent veiller à ce que les citoyens aient accès à des ressources et à des informations crédibles. Si les communications stratégiques sont nécessaires avant et pendant les élections, pour une résilience à long terme, il est également essentiel de poursuivre les efforts entre les périodes électorales.

Une approche de résilience pansociale

Pour construire une société résiliente, il faut comprendre les réponses et les interventions de lutte contre la manipulation de l'information de l'ensemble de la société au niveau mondial, régional et national, comme l'illustrent les exemples ci-dessous. Si les gouvernements, les plateformes numériques, le secteur privé, le monde universitaire et la société civile ont chacun leur propre approche d'atténuation, aucun secteur ne peut relever seul ces défis.

Mondial 	**Appel de Paris pour la confiance et la sécurité dans le cyberespace**	L'Appel de Paris consiste en un groupe de 79 pays, 35 autorités publiques, 391 organisations et 705 entreprises qui se sont réunis pour s'aligner sur un ensemble de neuf principes visant à créer un cyberespace ouvert, sûr, sécurisé et pacifique. L'Appel de Paris réaffirme l'engagement de ces pays à l'égard du droit international humanitaire et du droit international coutumier afin d'offrir aux citoyens les mêmes protections en ligne que celles que ces lois offrent hors ligne. En créant cette initiative, les gouvernements, la société civile et le secteur privé, y compris les entreprises de réseaux sociaux, adhèrent à l'idée d'assurer la sûreté, la stabilité et la sécurité dans le cyberespace et de renforcer la confiance et la transparence pour les citoyens. L'Appel a créé un processus de forum multi-acteurs permettant aux organisations et aux pays de se réunir pour accroître le partage d'informations et la collaboration.[102]
Régional (Europe) 	**Le Code de bonnes pratiques contre la désinformation de l'Union européenne**	Le Code de bonnes pratique contre la désinformation de l'UE[103] est l'une des initiatives régionales les plus multinationales et les mieux dotées en ressources, puisqu'elle bénéficie du soutien de l'ensemble du bloc européen et comprend des signataires de Facebook, Google, Twitter et Mozilla, ainsi que des annonceurs et une partie du secteur de la publicité. Le Code repose sur cinq piliers : améliorer la transparence des informations en ligne ; promouvoir l'éducation aux médias et à l'information pour lutter contre la désinformation ; développer des outils permettant aux utilisateurs et aux journalistes de lutter contre la désinformation ; préserver la diversité et la durabilité de l'écosystème européen des médias d'information ; et promouvoir la recherche continue sur l'impact de la désinformation en Europe afin d'évaluer et d'ajuster les mesures de réponse.

[102] Appel de Paris Pour la confiance et la sécurité dans le cyberespace (12 novembre 2018), https://pariscall.international/en/.

[103] Shaping Europe's digital future, "Code of Practice on Disinformation," (European Commission, s.d.) https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

Régional (Latin America) 	**Fundamedios**	Fondée en 2007, Fundamedios est une organisation qui se consacre à la promotion de la liberté d'expression, à la défense des droits humains et à la surveillance des agressions et des risques encourus par les journalistes en Amérique latine. Fundamedios a travaillé activement à la mise en place d'un réseau - couvrant l'Équateur, la Bolivie, l'Argentine, le Honduras et les États-Unis - de la société civile, des médias et des organisations internationales pour observer et former les journalistes et autres acteurs de la société civile afin de mieux identifier, comprendre et combattre la désinformation. Il existe d'autres collaborations régionales, notamment de plaidoyer auprès des gouvernements pour améliorer l'accès à l'information, ainsi que la création de médias pour diffuser des contenus véridiques.[104]
National (Nigeria) 	**Accord d'Abuja**	Avant les élections générales de 2015 au Nigeria, de multiples parties prenantes ont affirmé leur engagement en faveur d'un processus électoral pacifique en signant un accord en cinq points, l'Accord d'Abuja. Les signataires - comprenant les candidats à la présidence, les représentants de l'OGE et les agences de sécurité - se sont engagés à renforcer la sécurité des élections au Nigeria, notamment en acceptant de prendre des mesures proactives pour prévenir la violence électorale, en s'engageant à respecter pleinement les règlements définis par le cadre juridique des élections au Nigeria et en plaçant l'intérêt national au-dessus des préoccupations partisanes, entre autres engagements.[105]
National (Argentina) 	**Engagement numérique éthique**	En 2019, la Chambre nationale électorale (CNE: Cámara Nacional Electoral) d'Argentine a lancé une initiative visant à inciter les parties prenantes de tous types - y compris les partis politiques ainsi que les représentants des entreprises de technologie et de réseaux sociaux - à signer un Engagement numérique éthique. L'objectif de cet engagement était de prévenir la diffusion de fake news et de tout autre mécanisme de manipulation de l'information susceptible d'avoir un impact négatif sur les élections. L'engagement prévoyait une collaboration entre les différents secteurs de la société, puisque les signataires comprenaient des personnes issues de divers partis politiques, des représentants de Google, Facebook, Twitter et WhatsApp, ainsi que des directeurs de l'Association des organes de presse numérique (ADEPA), entre autres.[106]

[104] Fundamedios (Fundamedios, s.d.), https://www.fundamedios.org.

[105] "Abuja Accord on the Prevention of Violence and Acceptance of Election Results by Presidential Candidates and Chairpersons of Political Parties Contesting the 2015 General Elections" (Nigeria, 2015), https://www.idea.int/sites/default/files/codesofconduct/Abuja%20Accord%20January%202015.pdf.

[106] « Engagement numérique éthique » (Argentine : Chambre nationale électorale, 30 mai 2019), https://www.electoral.gob.ar/nuevo/paginas/pdf/CompromisoEticoDigital.pdf.

Campagnes de sensibilisation du public

Si les communications stratégiques sont nécessaires avant et pendant les élections, pour une résilience à long terme, il est également essentiel de poursuivre les efforts entre les périodes électorales. Les campagnes de sensibilisation du public aident les citoyens à comprendre que l'environnement de l'information est manipulé d'une manière qui pourrait nuire à leur capacité à exercer leurs droits démocratiques. Il est important de permettre à votre public cible de réfléchir de manière critique aux informations qu'il consomme et de lui donner les moyens de communiquer et de s'engager auprès de ses réseaux de confiance (amis, famille et collègues), afin qu'il puisse à son tour partager son appréciation. Dans vos efforts de sensibilisation à la menace de manipulation de l'information, tenez compte des étapes ci-dessous.

Avant votre campagne:

- Identifiez le segment de la population et le public que vous souhaitez atteindre aux niveaux national, sous-national et local.
- Identifiez d'autres organisations de la société civile et partenaires à inclure activement dans votre campagne de sensibilisation ou groupes qui peuvent vous aider à amplifier vos messages.
- Déterminez comment vous allez mener votre campagne de sensibilisation et quels canaux vous allez utiliser pour dissiper les inexactitudes et les informations manipulées. Par exemple, vous pouvez utiliser des annonces de service public, des communiqués de presse, les réseaux sociaux, la télévision, la radio et le bouche à oreille.

Pendant votre campagne:

- Adoptez une communication proactive pour identifier les risques potentiels de manipulation de l'information et ses conséquences pendant et entre les cycles électoraux.
- Sensibilisez vos électeurs et vos partenaires aux types de manipulation de l'information qu'ils peuvent subir et voir en ligne et hors ligne (inexactitudes, « demi-vérités », discours haineux, propagande d'État, etc.)
- Faites savoir à votre population cible et à vos électeurs où trouver les compétences, les ressources et les programmes d'éducation numérique, de cyberprotection et les moyens de réagir à la manipulation de l'information.
- Partagez des idées sur le moment où il faut garder le silence pour éviter de diffuser des informations manipulées.

Après la campagne:

- Réunissez-vous avec votre équipe pour déterminer les leçons apprises et les mesures à prendre pour améliorer les cas suivants.
- Reproduisez les campagnes de sensibilisation réussies auprès de segments de population différents (populations âgées, communautés marginalisées, etc.).

Le tableau ci-dessous présente des exemples de campagnes de sensibilisation du public qui ont réussi à améliorer les connaissances des citoyens ciblés. Bien que certains de ces exemples se concentrent sur la sensibilisation à COVID-19, les tactiques utilisées sont également transférables à des contextes électoraux.

Acteur de la démocratie	Exemples
Gouvernement	« **Stop the Spread** » est une campagne mondiale visant à sensibiliser aux risques de mésinformation autour de COVID-19, en encourageant le public à vérifier les informations auprès de sources fiables telles que l'OMS et les autorités sanitaires nationales.[107]
Gouvernement	Au Timor-Leste, des représentants du gouvernement se sont associés à l'IRI pour mettre en relation les citoyens et les membres du parlement par le biais d'un talk-show intitulé « **Koalia Ba Hau/Talk to Me!**" » Les responsables gouvernementaux sont en mesure de partager de manière proactive des informations véridiques sur des sujets tels que le COVID-19, et les citoyens peuvent participer en posant des questions et en faisant des commentaires. Koalia Ba Hau est diffusé sur la télévision nationale avec une audience de 9 500 téléspectateurs, ainsi que sur des stations de radio dans tout le pays. Cette forme de communication proactive s'est avérée avoir une meilleure portée que les traditionnelles assemblées publiques et tables rondes.
OGE	En 2020, le Tribunal supérieur électoral (TSE) du Brésil a renforcé ses stratégies traditionnelles de sensibilisation du public en créant « **e-Título**," » une application mobile qui aide les électeurs à identifier leurs bureaux de vote et facilite la communication directe entre les électeurs et le TSE.[108]
OGE	Le Conseil électoral national d'Éthiopie (NEBE) a créé la campagne **#AskNebe campaign**[109] sur Twitter pour que les électeurs puissent communiquer directement avec le Conseil et poser des questions sur le processus électoral et sur la manière d'obtenir des informations crédibles.
CSO	Matsda2sh ("do not believe") (« ne pas croire ») est une OSC égyptienne de fact-checking qui a utilisé Facebook pour atteindre plus de 500 000 abonnés avec des **vidéos de sensibilisation** aux dangers de la désinformation.[110]

[107] Organisation mondiale de la santé, « Countering Misinformation about COVID-19: A Joint Campaign with the Government of the United Kingdom » (mis à jour le 13 mai 2020), https://www.who.int/news-room/feature-stories/detail/countering-misinformation-about-covid-19.

[108] Tribunal supérieur électoral du Brésil, « e-Título » (app), https://apps.apple.com/us/app/e-t%C3%ADtulo/id1320338088.

[109] #AskNebe campaign (Twitter Campaign), https://twitter.com/nebethiopia/status/1357311115257143298?lang=en.

[110] Matsda2sh (Facebook Page), https://www.facebook.com/matsda2sh/.

L'importance du plaidoyer

Les organisations de la société civile peuvent constituer une voix forte et plaider pour une plus grande transparence de la part des gouvernements locaux, des partis politiques et des OGE afin de faire pression pour des changements réglementaires et juridiques pour mieux protéger les futures élections et garantir des engagements plus forts, des mesures de vérifiabilité et de responsabilité de la part des réseaux sociaux et autres entreprises de technologie. Ces appels à la transparence, à la responsabilité et à la réforme exigeront souvent des OSC qu'elles conçoivent une campagne de plaidoyer proactive.

Lorsque vous élaborez une campagne de plaidoyer destinée au gouvernement, tenez compte des meilleures pratiques énumérées ci-dessous.

- Effectuez une analyse de la situation et du paysage pour déterminer pourquoi la campagne de plaidoyer est justifiée : Quelles sont les lois et réglementations actuelles sur la manipulation de l'information, la haine en ligne, le harcèlement et la liberté d'expression au sein de la société ?
- Identifiez les parties prenantes et créez une coalition : Quelles sont les parties prenantes avec lesquelles vous devez collaborer parmi les autorités locales, vos partenaires et les experts juridiques et techniques, pour former une coalition et lancer une campagne de plaidoyer réussie ? Étant donné que la manipulation de l'information, la haine en ligne et le harcèlement touchent souvent des communautés marginalisées, veillez à inclure ces voix et opinions dans toute leur diversité.
- Réfléchissez à la question centrale ou à l'ensemble des questions autour desquelles vous allez construire votre campagne de plaidoyer politique, et assurez-vous que la question soit cohérente à travers votre écosystème de parties prenantes.
- Créez des stratégies de communication de messages. Cela peut inclure l'élaboration de contenu, un site web et une présence sur les réseaux sociaux et dans les médias traditionnels. Identifiez les acteurs qui peuvent valider et amplifier le message de votre campagne.
- Identifiez les acteurs gouvernementaux auprès desquels vous souhaitez plaider et les meilleures tactiques de plaidoyer auprès du gouvernement. Il peut s'agir de communiquer directement avec des gouvernements, d'écrire des lettres, de soumettre des recommandations et de s'associer à des alliés internes qui peuvent faire passer le message.

Des informations supplémentaires sont disponibles dans le guide de plaidoyer Advocacy Playbook de Open Internet for Democracy.[111]

[111] Open Internet for Democracy, *Advocacy Playbook: Strategies to Build Coalitions & Tactics* (OID, s.d.), https://openinternet.global/sites/default/files/2020-10/Open%20Internet%20for%20Democracy%20Playbook%20%283April2019%20Release%29.pdf.

Éducation à la culture numérique

Les initiatives d'éducation numérique visent à renforcer la capacité des citoyens à fonctionner dans un monde hautement numérisé. Bien que les programmes d'éducation à la culture numérique doivent être adaptés à leur public, ils consistent généralement à aider les gens à apprendre à discerner rapidement les faits de la fiction et à comprendre comment les informations se propagent en ligne. Dans le cadre d'une initiative d'éducation numérique, vos partenaires, employés et citoyens peuvent apprendre ces compétences essentielles:

- Comment réfléchir de manière critique aux informations qu'ils consomment tant sur les réseaux sociaux que par le biais des médias traditionnels.
- Les fonctions des réseaux sociaux et médias grand public, notamment la manière dont les informations sont sélectionnées et diffusées.
- Comment identifier un contenu crédible (c'est-à-dire, peut-il être vérifié par plusieurs sources crédibles, a-t-il été vérifié par des organismes de vérification des informations crédibles, le titre fait-il du sensationnel, etc.)
- Comment vérifier les images et les vidéos à l'aide de programmes tels que Recherche Google Images, Reverse Image Search, et fake video news debunker. [112]
- Comment éviter de contribuer à la désinformation en ne partageant ou en ne commentant pas sur des contenus non vérifiés.[113]
- Comment signaler aux plateformes de réseaux sociaux des contenus faux ou préjudiciables dans les réseaux ouverts et fermés.
- Reconnaître comment les préjugés, la « pensée unique » et les normes culturelles, religieuses et sociales affectent la capacité d'identifier et d'évaluer un contenu crédible.

Toute initiative d'éducation numérique destinée aux citoyens, aux partenaires et à votre propre organisation devrait également inclure des leçons de cyberprotection.

- Utiliser des mots de passe forts et une authentification à double facteur.
- Utiliser une messagerie cryptée pour communiquer des informations sensibles.
- Utiliser un réseau privé virtuel (VPN) pour établir des connexions réseau privées afin de communiquer et de mener les activités de votre organisation en toute sécurité.[114]
- Vérifier les paramètres de confidentialité et de sécurité de vos comptes de réseaux sociaux.

Le programme complet Learn to Discern (L2D) de l'IREX propose de nombreuses ressources pour la mise en place d'un programme d'éducation à la culture numérique sur sa page Resources for Learning & Impact.[115] La page des ressources de l'UNESCO sur l'éducation aux médias et à l'information énumère également plusieurs ressources utiles.[116]

Conseil: Il est particulièrement important d'adapter les programmes d'éducation numérique aux groupes marginalisés, car la manipulation de l'information se répand souvent dans ces communautés et cible fréquemment les femmes et les filles.

[112] Google Images (Google, s.d.), https://www.google.com/imghp?hl=en; Squobble.com, « RevEye Reverse Image Search » (app), https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf?hl=en; InVID et WeVerifyFake, « News Debunker » (app), https://chrome.google.com/webstore/detail/fake-news-debunker-by-inv/mhccpoafgdgbhnjfhkcmgknndkeenfhe?hl=en.

[113] ReFrame et PEN America, *Disinfo Defense Toolkit for Organizers and Advocates* (ReFrame et PEN America, s.d.), https://pen.org/wp-content/uploads/2020/12/disinfo-defense-toolkit-v2-compressed.pdf.

[114] Techopedia, « What is a Virtual Private Network (VPN)? » (Techopedia, mis à jour le 14 novembre 2016), https://www.techopedia.com/definition/4806/virtual-private-network-vpn.

[115] Learn to Discern, « Media Literacy Training » (IREX, s.d.), https://www.irex.org/project/learn-discern-l2d-media-literacy-training.

[116] « Éducation aux médias et à l'information - Ressources » (UNESCO, s.d.), https://en.unesco.org/themes/media-and-information-literacy/resources.

Conseil: N'oubliez pas les médias traditionnels

Souvenez-vous que l'éducation numérique doit également permettre de comprendre comment l'information se diffuse hors ligne par le biais de sources d'information plus traditionnelles (journaux, radio, etc.). Veillez à rappeler aux participants que les mêmes compétences en matière de culture numérique s'appliquent lorsqu'il s'agit d'identifier des informations crédibles dans les journaux et à la radio et que les informations peuvent circuler entre les médias traditionnels hors ligne et les réseaux de confiance en ligne.

« Apprendre à discerner par le jeu »

Votre initiative d'éducation numérique peut intégrer des approches d'apprentissage uniques. Les jeux peuvent montrer comment les fake news se propagent et comment identifier et discerner les informations crédibles et démystifier les faux récits ou les inexactitudes. Par exemple, des psychologues de l'université de Cambridge se sont associés au collectif médiatique néerlandais DROG pour créer le jeu Bad News, qui vise à renforcer la résilience psychologique face à la désinformation.[117] Le jeu consiste en un apprentissage actif par l'expérience en demandant aux joueurs de créer un faux personnage, d'attirer des adeptes et d'asseoir leur crédibilité en tant que site de fake news. En d'autres termes, le jeu permet aux joueurs de se familiariser avec l'état d'esprit des acteurs de la menace qui cherchent à diffuser la désinformation. Les joueurs renforcent leur résistance face à la désinformation en comprenant mieux les acteurs de la menace et leurs tactiques, notamment l'usurpation d'identité, l'émotion, la polarisation, les théories du complot, le discrédit des faits et le trolling. La capture d'écran ci-dessous illustre l'expérience du joueur.

Des jeux similaires existent pour des publics mondiaux, régionaux et nationaux. Parmi les jeux qui pourraient être utilisés à l'échelle mondiale, citons PolitiTruth, Be Internet Awesome, Factitious et Fakey.[118] D'autres jeux, tels que Harmony Square et Fake It to Make It, ont été créés spécifiquement pour les contextes nationaux des États-Unis et des Pays-Bas, respectivement.[119] Passez en revue ces outils existants pour voir si l'un d'entre eux pourrait être utile dans vos efforts d'éducation numérique. Nombre de ces jeux peuvent servir de point de départ utile pour concevoir un jeu adapté au contexte de votre pays. L'utilisation de jeux existants nécessitera probablement une traduction, une contextualisation et d'autres ajustements pour qu'ils soient adaptés au contexte de votre pays.

[117] DROG, « Bad News Game » (jeu en ligne), https://www.getbadnews.com/#intro.

[118] PolitiFact, « PolitiTruth » (app) https://www.cinqmarsmedia.com/politifact/index.html; Be Internet Awesome, « Interland » (jeu en ligne), https://beinternetawesome.withgoogle.com/en_us/interland/landing/tower-of-treasure; AU Game Lab et JoLT, « Factitious 2020 » (jeu en ligne), http://factitious-pandemic.augamestudio.com/#/; Observatory on Social Media,« Fakey » (jeu en ligne), https://fakey.osome.iu.edu.

[119] Global Engagement Center (GEC), Cybersecurity and Infrastructure Security Agency (CISA), DROG and University of Cambridge, "Harmony Square" (online game), https://harmonysquare.game/en; Amanda Warner, "Fake It to Make It" (online game), https://www.fakeittomakeitgame.com.

Initiatives d'éducation numérique des plateformes de réseaux sociaux

Les plateformes de réseaux sociaux et d'autres partenaires du secteur privé ont investi dans le renforcement des efforts de résilience à l'échelle mondiale par le biais de partenariats privés-publics-civiques. La plupart des programmes qui en résultent - détaillés ci-dessous - sont disponibles en plusieurs langues et pourraient constituer des ressources utiles dans le cadre de vos efforts pour développer la culture numérique de votre organisation et de vos communautés.

- **Facebook** et des experts de la région Asie-Pacifique ont collaboré au programme « We Think Digital », qui encourage la culture numérique dans la région par la création de guides publics des actions des utilisateurs, de modules d'apprentissage numérique, de vidéos et d'autres ressources pédagogiques.[120]

- **Twitter** s'est associé à l'UNESCO pour créer Teaching and Learning with Twitter un guide qui aide les éducateurs du monde entier à permettre aux jeunes de réfléchir de manière critique aux informations qu'ils consomment.[121]

- **Google** et **YouTube** ont beaucoup investi dans la responsabilité numérique et l'éducation aux médias afin de développer la résilience des citoyens et des jeunes.[122] Plus récemment, Google a investi 25 millions d'euros pour aider à lancer le Fonds européen pour les médias et l'information.[123] Cet effort a pour but d'éduquer, de former et d'aider les citoyens à renforcer leurs compétences en matière d'éducation aux médias, de soutenir et de développer le travail des vérificateurs d'information et de renforcer l'expertise et la recherche sur la manipulation de l'information sous toutes ses formes.

- **Microsoft** a également établi des partenariats avec des instituts de recherche et des OSC dans le monde entier, notamment l'université de Washington, Sensity et USA Today, dans le cadre de son programme Defending Democracy Program, Ce programme vise à renforcer la résilience et à promouvoir l'éducation aux médias et aux technologies numériques, afin d'aider le public à décrypter les inexactitudes, les demi-vérités et les faits.[124] L'objectif ultime de cette initiative a conduit à un plus grand engaged citizenry.[125]

[120] Facebook, "We Think Digital" (Facebook, s.d.), https://wethinkdigital.fb.com.

[121] Twitter, "Teaching and Learning with Twitter" (Twitter, s.d.), https://about.twitter.com/content/dam/about-twitter/en/tfg/download/teaching-learning-with-twitter-unesco.pdf.

[122] Jacqueline Fuller, « Bringing Digital and Media Literacy Education to More Schools in Korea » (Google.org, 28 mars 2019), https://www.blog.google/outreach-initiatives/google-org/digital-and-media-literacy-education-korea/.

[123] Matt Briton, « Google's €25 million Contribution to Media Literacy », *The Keyword* (Google blog), 21 mars 2021, https://blog.google/around-the-globe/google-europe/googles-25-million-contribution-to-media-literacy/; « European Media and Information Fun », Fondation Calouste Gulbenkian, https://gulbenkian.pt/en/european-media-and-information-fund/.

[124] Sensity, https://sensity.ai; Tom Burt, Tom Burt, « Announcing the Defending Democracy Program », *Microsoft on the Issues* (blog), 13 avril 2018, https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program/.

[125] Tom Burt, « New Steps to Combat Disinformation » Microsoft on the Issues (blog), 1er septembre 2020, https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/.

Conseils clés pour lutter contre la manipulation de l'information

Vous trouverez ci-dessous des conseils essentiels pour permettre à votre organisation d'identifier la manipulation des informations, d'y répondre et de renforcer sa résilience.

Mettez en place un plan

N'attendez pas d'avoir vécu ou d'être témoin de récits de manipulation de l'information électorale dans votre écosystème local d'information en ligne pour commencer à identifier les meilleures approches et stratégies pour les contrer. Préparez-vous de manière proactive.

Tous les gouvernements n'ont pas de bonnes intentions

Faites preuve de prudence si et quand vous décidez de signaler la manipulation d'informations liées aux élections aux gouvernements, car beaucoup ne respectent pas les normes démocratiques ou ne sont pas impartiaux. Examinez les ressources et les mesures prises par le passé par les gouvernements pour éviter de causer davantage de dommages.

Trouvez des partenaires pour obtenir de meilleurs résultats

Contactez et collaborez avec un ensemble diversifié d'entités travaillant autour des élections, comme les OGE et les OSC orientées sur l'éducation des électeurs, les dirigeants communautaires et religieux qui sont des sources d'information de confiance dans leurs communautés, les plateformes de réseaux sociaux, les journalistes et les vérificateurs d'information, etc.

Adaptez vos attentes quant au comportement et aux actions des plateformes de réseaux sociaux

La manipulation des informations électorales est monnaie courante sur les plateformes de réseaux sociaux. Familiarisez-vous avec les politiques et les normes communautaires des plateformes et comprenez que de nombreuses plateformes ne sont pas immédiatement réactives aux signalements des utilisateurs ou préparées à aborder l'environnement de l'information électorale d'un pays sur leurs sites.

Combinez, associez et adaptez vos approches

La réponse à la manipulation de l'information électorale nécessite une combinaison d'approches pour garantir des résultats positifs, et l'efficacité de ces approches variera selon les contextes nationaux.

Réponse rapide et résilience à long terme vont de pair

Les réponses à court terme à la manipulation de l'information électorale doivent être complétées par un renforcement de la résilience à long terme dans des domaines tels que l'éducation numérique, les campagnes de sensibilisation du public et une approche pansociale pour créer un public bien informé.

Parlez si vous voyez ou entendez quelque chose

Si vous voyez ou entendez des informations manipulées visant votre organisation, des organisations partenaires et/ou des segments de la population avec lesquels vous travaillez, signalez-les aux autorités gouvernementales, aux plateformes de réseaux sociaux et aux médias pour qu'ils enquêtent en cas de besoin.

La culture numérique renforce l'esprit critique

Sensibilisez vos citoyens, votre organisation, vos partenaires et vos réseaux de confiance à l'identification des faux récits et contenus. Encouragez-les à rester vigilants et à porter un regard critique sur les informations consommées en ligne et hors ligne.

Annexes

Annexe A : Études de cas

Étude de cas du Mexique

Historique et contexte politique

Au Mexique, la manipulation de l'information s'opère dans un environnement caractérisé par des taux de pénétration d'Internet relativement élevés - environ deux tiers du pays connecté - et un haut niveau d'utilisation des réseaux sociaux. La plupart des gens (86 %) s'informent à partir de sources en ligne, Facebook (70 %), YouTube (44 %) et WhatsApp (39 %) étant les trois principales plateformes d'information en ligne. Malgré les taux élevés d'utilisation des réseaux sociaux et médias en ligne, 60 % des Mexicains sont préoccupés par l'écosystème de l'information en ligne et la diffusion de fausses informations en ligne.[126]

Cette tendance est encore exacerbée par le fait que l'environnement numérique mexicain n'est que « partiellement libre », ce qui, combiné à la polarisation croissante et aux politiques identitaires, a créé des conditions propices à la diffusion de fausses informations en ligne. Le gouvernement a également entrepris des mesures pour entraver la liberté d'expression, la liberté de la presse, les pratiques démocratiques et d'autres droits humains fondamentaux par le biais de la surveillance, de lois restrictives et de la manipulation de l'information.[127]

Manipulation de l'information au Mexique

Dans ces circonstances politiques et ce contexte en ligne, le Mexique a une longue histoire de manipulation de l'information par une variété d'acteurs malveillants, notamment les candidats politiques, le secteur de l'influence et d'autres acteurs locaux qui ont utilisé les réseaux sociaux pour diffuser de la désinformation sur la politique. Ces campagnes se caractérisent souvent par l'utilisation de comptes hautement automatisés - parfois appelés « bots politiques » - qui jouent un rôle important dans l'amplification de la désinformation en ligne. L'utilisation de bots a d'abord été portée à l'attention du public lors des élections présidentielles de 2012 au Mexique, des chercheurs ont alors identifié l'utilisation de « Peñabots » par le Parti révolutionnaire institutionnel (PRI)[128] pour soutenir la campagne du candidat de l'époque, Enrique Peña Nieto. Depuis lors, des études universitaires et des enquêtes journalistiques ont mis en évidence l'utilisation continue de bots pour perturber la communication en ligne, le discours politique et les activités de protestation au Mexique.[129]

Les élections générales de 2018 ont été marquées par des défis sans précédent pour l'écosystème de l'information en ligne. S'agissant de la plus grande élection de l'histoire du Mexique - avec plus de 3 400 sièges à pourvoir aux niveaux local, étatique et fédéral - les réseaux sociaux sont devenus l'un des principaux fronts de manipulation de l'information. Alors que l'on craignait que ce soit les campagnes d'information russes qui polluent l'écosystème de l'information, la plupart de la désinformation provenait du Mexique. À l'approche du vote, des comptes robots ont généré des hashtags viraux pour exacerber les clivages politiques et amplifier les conspirations autour de la fraude et de la corruption.[130] Les diffuseurs de fausses nouvelles et les faux sondeurs ont mêlé la réalité à la fiction pour miner la crédibilité des organismes d'information professionnels et entraver la capacité des citoyens à accéder à des informations exactes sur l'élection, les candidats et leurs campagnes.[131] Les enquêteurs

[126] Nic Newman, et al., *Reuters Institute Digital News Report 2020* (Reuters Institute for the Study of Journalism, 2020), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf.

[127] Freedom House, « Mexico: Freedom on the Net 2020 Country Report », Freedom House (2020), https://freedomhouse.org/country/mexico/freedom-net/2020.

[128] Luis Daniel, « Rise of the Peñabots », *Data and Society: Points* (blog), Data and Society Research Institute (24 février 2016), https://points.datasociety.net/rise-of-the-peñabots-d35f9fe12d67.

[129] Luiza Bandeira et al., *Disinformation in Democracies: Strengthening Digital Resilience in Latin America* (Atlantic Council Digital Forensic Research Lab, mars 2019), https://www.atlanticcouncil.org/in-depth-research-reports/report/disinformation-democracies-strengthening-digital-resilience-latin-america/; Samantha Bradshaw, Hannah Bailey, et Philip Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project (Oxford Internet Institute, 13 janvier 2021), https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf; Pablo Suárez-Serrato et al., « On the Influence of Social Bots in Online Protests. Preliminary Findings of a Mexican Case Study », dans E. Spiro et YY Ahn (éd.) « Social Informatics. SocInfo 2016 », *Lecture Notes in Computer Science*, vol. 10047(Springer, Cham), https://doi.org/10.1007/978-3-319-47874-6_19.

[130] Luiza Bandeira et al., *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*; Monika Glowacki et al., « News and Political Information Consumption in Mexico: Mapping the 2018 Mexican Presidential Election on Twitter and Facebook » (Computational Propaganda Project, 2018), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/06/Mexico2018.pdf.

[131] Jorge Buendia, *Fake Polls as Fake News: The Challenge for Mexico's Elections* (Wilson Center, 2018), https://www.wilsoncenter.org/publication/fake-polls-fake-news-the-challenge-for-mexicos-elections.

ont découvert que nombre de ces activités étaient alimentées par des sociétés commerciales engagées par des politiciens et des entreprises pour déformer l'écosystème de l'information en leur faveur.[132]

Les élections générales de 2018 au Mexique ont également été caractérisées par des niveaux élevés de violence politique, avec plus de 100 personnalités politiques tuées pendant la période précédant le vote.[133] Nombre de ces meurtres ont été associés au crime organisé et à la lutte contre la drogue, mais la violence politique a également été exacerbée à cause de la manipulation de l'information. Lors d'une course au poste de gouverneur dans la province de Puebla, le Atlantic Council a découvert des comptes automatisés amplifiant des hashtags concurrents qui revendiquaient prématurément la victoire des candidats adverses.[134] La province de Puebla a signalé des niveaux élevés de violence, avec des citoyens assassinés et des bulletins de vote volés ou incendiés.

Au Mexique, la manipulation de l'information ne survient pas seulement pendant les élections. En 2019, une enquête de Signa_Lab a permis d'identifier un réseau de comptes Twitter qui s'en prenaient aux journalistes et aux organes de presse qui critiquaient le nouveau président.[135] La manipulation de l'information entraine de nombreux défis pour la liberté d'expression et la liberté de la presse au Mexique : les journalistes, les activistes et les opposants politiques sont victimes de manière disproportionnée de harcèlement, de menaces, de rumeurs et de calomnies sur les réseaux sociaux.[136] Comme dans de nombreux autres pays, les femmes sont particulièrement la cible de campagnes de dénigrement en ligne, où de faux comptes ont partagé des vidéos et des images manipulées pour sexualiser, mettre en doute et saper la crédibilité et la légitimité de femmes à des postes de responsabilité.[137] Bien que le Mexique ait adopté des règles de parité entre les sexes pour les partis politiques, les femmes politiques sont toujours confrontées à un nombre disproportionné de harcèlements en ligne.

Interventions

Afin d'identifier, de répondre et de renforcer la résilience face à la manipulation de l'information lors des élections présidentielles de 2018, l'Institut national électoral (INE) du Mexique a collaboré avec des plateformes de réseaux sociaux et des OSC pour renforcer l'intégrité de l'information dans tout le pays.

Les trois principales sociétés de réseaux sociaux (Facebook, Twitter et Google) ont travaillé directement avec l'INE pour rendre les informations sur l'élection plus facilement accessibles aux citoyens.[138] Étant donné que plus de 60 millions de citoyens mexicains utilisent Internet - dont un grand nombre pour la recherche et la conservation des informations - les trois plateformes ont diffusé en direct les débats présidentiels mexicains et les annonces officielles des élections pour la première fois. Twitter a organisé des discussions formelles par hashtag autour des débats présidentiels, ce qui a créé un forum de commentaires professionnels et journalistiques en temps réel sur les sujets débattus. Facebook et Google ont également collaboré avec l'INE pour mettre en place des boutons interactifs qui dirigeraient les utilisateurs vers le centre électoral de l'INE, les aideraient à trouver des bureaux de vote et diffuseraient des messages pour inciter les électeurs à voter. Dans l'ensemble, ces collaborations entre plateformes ont aidé les citoyens à trouver et à accéder à des informations précises sur les candidats ainsi que sur les procédures et les informations électorales.[139]

En plus de travailler avec les plateformes, les organisations de la société civile se sont également coordonnées avec l'INE pour aider à identifier, répondre et renforcer la résilience face à la manipulation de l'information lors des élections de 2018. L'une

[132] Ben Nimmo et al., "#ElectionWatch: Trending Beyond Borders in Mexico," Medium, 28 juin 2018, https://medium.com/dfrlab/electionwatch-trending-beyond-borders-in-mexico-2a195ecc78f4.

[133] Natasha Turak, "More than 100 Politicians Have Been Murdered in Mexico Ahead of Sunday's Election," CNBC, 26 juin, 2018, https://www.cnbc.com/2018/06/26/more-than-100-politicians-murdered-in-mexico-ahead-of-election.html.

[134] Bandeira et al., *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*.

[135] Signa_Lab, « Democracia, Libertad de Expresión y Esfera Digital. Análisis de Tendencias y Topologías En Twitter. El Caso de La #RedAMLOVE » (2019), https://signalab.iteso.mx/informes/informe_redamlove.html.

[136] ARTICLE 19, « Mexico: Report shows silencing of journalists and media freedom » (ARTICLE 19: 17 avril 2019), https://www.article19.org/resources/mexico-report-shows-silencing-of-journalists-and-media-freedom/.

[137] Freedom House, « Mexico: Freedom on the Net 2020 Country Report ». https://freedomhouse.org/country/mexico/freedom-net/2020.

[138] Commission Kofi Annan sur les élections et la démocratie, « Protéger l'intégrité électorale à l'ère du numérique » (janvier 2020), https://www.kofiannan-foundation.org/our-work/kofi-annan-commission/the-kacedda-94nfyd3mjqo9phewncbtfd5tcgitolhz/.

[139] Commission Kofi Annan sur les élections et la démocratie, « Protéger l'intégrité électorale à l'ère du numérique » https://www.kofiannanfoundation.org/app/uploads/2020/05/85ef4e5d-kaf-kacedda-report_2020_english.pdf.

des interventions les plus notables a été Verificado 2018, qui a rassemblé plus de 80 partenaires pour identifier et répondre à la manipulation de l'information en temps réel.[140] Verificado a créé un centre de ressources électorales et produit des vidéos d'information - qui ont enregistré 5,4 millions de visites - pour aider les citoyens à comprendre le processus électoral.[141] Ils ont également mis en place une série de processus permettant aux utilisateurs de vérifier la véracité du contenu des plateformes de réseaux sociaux et de recevoir des réponses fiables et rapides de la part des vérificateurs d'informations. Sur Twitter et Facebook, les comptes de Verificado comptaient plus de deux cent mille abonnés. Verificado a également mis en place un groupe WhatsApp où les utilisateurs pouvaient envoyer des demandes de vérification des informations. Au cours de la première semaine de fonctionnement, le groupe a reçu plus de 18 000 messages, dont 13 800 ont été traités par quatre membres du personnel de Verificado. Au total, le groupe de Verificado comptait plus de 9 600 abonnements et plus de 60 000 interactions.

Leçons du Mexique pour une réponse de la société civile à la manipulation de l'information

Établir des relations de collaboration avec les plateformes et les acteurs de la société civile.

Les réseaux sociaux deviennent de plus en plus une source de nouvelles et d'informations. Collaborer avec des partenaires des plateformes pour aider à rationaliser l'accès aux informations électorales officielles peut donc contribuer à renforcer la confiance dans les élections. En diffusant en continu des débats qui n'étaient traditionnellement diffusés qu'à la télévision, l'INE et les entreprises de réseaux sociaux ont aidé les utilisateurs à trouver et à regarder les débats par le biais de moyens de communication utilisés par des millions de citoyens. Les discussions formelles avec hashtags qui ont mis en évidence des commentaires journalistiques et professionnels ont contribué à exposer les citoyens à des informations et des opinions supplémentaires sur les débats, afin qu'ils puissent formuler leurs propres idées et opinions. Les centres de vote et les informations sur comment et où voter ont contribué à encourager les citoyens à aller voter le jour de l'élection. En fournissant des informations précises sur les processus de vote et les candidats, ces relations de collaboration avec les plateformes peuvent contribuer à renforcer la résilience face aux campagnes de manipulation de l'information.

Le timing est important : Augmentez la vitesse et l'échelle de la vérification des informations.

Il est extrêmement important de pouvoir s'attaquer à la manipulation de l'information en temps réel et avant que les récits ne deviennent viraux, afin de lutter contre la propagation de més/désinformation nuisible. Si Verificado a connu un tel succès, c'est en grande partie grâce à la vitesse et à l'échelle auxquelles il a fonctionné. En travaillant avec plusieurs partenaires de confiance, le personnel a pu identifier les manipulations d'informations dès leur apparition sur les réseaux sociaux et répondre rapidement et facilement aux demandes des utilisateurs concernant la véracité du contenu. Ils ont également opéré sur des plateformes en ligne où se propageait de la més/désinformation afin de communiquer au public des informations corrigées et des contre-messages. À l'approche des élections, le groupe Twitter, Facebook et WhatsApp de Verificado a touché des centaines de milliers d'électeurs en répondant à des demandes individuelles concernant la véracité du contenu. Le développement de ces canaux de confiance capables de répondre avec rapidité et précision et sur des plateformes où les utilisateurs trouvaient des informations erronées a permis à Verificado de démentir les rumeurs et de renforcer la confiance des citoyens et des électeurs, ce qui a contribué au succès global de l'initiative.

Créez une marque claire et cohérente pour les informations professionnelles vérifiées.

Ce qui a contribué à la réussite de l'intervention de Verificado, c'est non seulement son approche en temps réel face aux récits de més/désinformation au fur et à mesure de leur apparition, mais aussi la manière dont l'initiative a établi une marque claire et centrale promouvant un contenu journalistique précis, fiable et professionnel sur l'élection. Bien que travaillant avec plus de 80 partenaires de confiance, Verificado a permis à différentes organisations de prêter leurs ressources et leur expertise sous une seule marque de confiance qui a gagné la reconnaissance des utilisateurs et des citoyens. Les vérifications et les informations de Verificado ont également été reprises et diffusées sur les chaînes de télévision locales et dans la presse écrite, en plus de son travail en ligne. La marque de confiance a également aidé Verificado à s'imposer comme une source neutre et professionnelle d'informations factuelles dans un environnement caractérisé par une désinformation nationale très polarisée.

[140] Bandeira et al., "Disinformation in Democracies: Strengthening Digital Resilience in Latin America." https://www.atlanticcouncil.org/in-depth-research-reports/report/disinformation-democracies-strengthening-digital-resilience-latin-america/.

[141] Bandeira et al., « Disinformation in Democracies: Strengthening Digital Resilience in Latin America ».

Étude de cas de Taiwan

Historique et contexte politique

Taïwan a été pris au dépourvu par la désinformation lors des élections et référendums locaux de 2018. Au cours des deux années suivantes, le pays a élaboré une réponse pansociale pour renforcer la cohésion sociale, contrer la désinformation et assurer la réussite de l'élection présidentielle de 2020. En 2018, le gouvernement taïwanais répondait principalement aux campagnes de désinformation de manière unilatérale, sans aucune coordination avec des vérificateurs d'informations tiers ou des entreprises de réseaux sociaux. À cette époque, il n'existait pas encore de relations avec les entreprises de réseaux sociaux et les vérificateurs d'informations tiers qui pouvaient collaborer avec le gouvernement pour mettre en évidence les récits crédibles.[142] Pourtant, en moins de deux ans, Taiwan a établi des relations, des canaux de communication et de coordination entre le gouvernement, la société civile, les plateformes de réseaux sociaux et des vérificateurs d'informations indépendants. Cette coordination a permis à Taïwan d'identifier la désinformation et d'y répondre avec rapidité et efficacité lors des élections de 2020 et d'établir les bases d'une résilience à long terme face à la désinformation (voir ce rapport).[143]

La réponse pansociale de Taïwan aux campagnes de désinformation

Vous trouverez ci-dessous les grandes lignes des principales interventions mises en œuvre par Taïwan pour établir une réponse pansociale à la manipulation de l'information autour des élections présidentielles de 2020.

Gouvernement	Plateformes de réseaux sociaux	Organisations de la société civile
Réponse: Le bureau en charge de la guerre politique du ministère de la Défense nationale a mis en place une « équipe de traitement rapide » chargée d'identifier et de répondre rapidement à la désinformation provenant de la Chine et des sources et individus nationaux prochinois, d'utiliser le big data pour analyser les campagnes de désinformation du PCC et de mettre en évidence du contenu vérifié sur les réseaux sociaux et via les points de presse.[144]	**Partenariat:** LINE a établi un partenariat privé-public-civique avec le Yuan exécutif de Taiwan et le FactCheck Center, Cofacts, MyGoPen, Doublethink Lab et d'autres dans le cadre du Digital Accountability Project (DAP).[145] Grâce à ce partenariat, LINE a intégré la vérification des informations dans son service et a développé un chatbot pour sensibiliser les utilisateurs aux campagnes de désinformation, leur permettre de soumettre du contenu à l'analyse d'organisations de vérification d'informations réputées et leur fournir du contenu provenant de sources d'information crédibles.	**Activisme local :** Les organisations de la société civile ont développé des réseaux de confiance avec des vérificateurs d'informations indépendants tels que Cofacts, le FactCheck Center de Taïwan et d'autres, ainsi qu'avec des plateformes de réseaux sociaux afin d'identifier les campagnes de désinformation, d'y répondre et de renforcer la résilience à l'approche des élections de 2020, à travers des group chats fermés et des groupes physiques de voisinage et religieux. Cette approche s'est avérée particulièrement efficace, car les représentants des OSC ont pu collaborer et partager des informations avec des réseaux fiables pour favoriser la confiance.[146]

[142] Représentant du Consejo Nacional Electoral (CNE) de l'Équateur en discussion avec l'auteur, mars 2020.

[143] Aaron Huang, *Combatting and Defending Chinese Propaganda and Disinformation: A Case Study of Taiwan's 2020 Elections* (Belfer Center for Science and International Affairs, 2020), https://www.belfercenter.org/sites/default/files/files/publication/Combating%20Chinese%20Propaganda%20and%20Disinformation%20-%20Huang.pdf.

[144] Jude Blanchett, et al., *Protecting Democracy in an Age of Disinformation: Lessons from Taiwan* (Center for Strategic & International Studies, janvier 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210127_Blanchette_Age_Disinformation.pdf.

[145] Elizabeth Lange et Doowan Lee, « How One Social Media App is Beating Disinformation », Foreign Policy (23 novembre 2020), https://foreignpolicy.com/2020/11/23/line-taiwan-disinformation-social-media-public-private-united-states/.

[146] Contributeur de la communauté g0v en discussion avec l'auteur, décembre 2020

Gouvernement	Plateformes de réseaux sociaux	Organisations de la société civile
Amplification: Le gouvernement a créé des équipes de « conception de mèmes » au sein de chaque agence gouvernementale afin d'utiliser des campagnes humoristiques pour répondre à la désinformation de manière attrayante.[147]	**Réponse:** À la suite du plaidoyer et des contacts continus avec le gouvernement et des OSC, Facebook a lancé sa « war room en temps réel pour préparer les élections de 2020 à Taïwan, permettre à sa famille d'apps de démonter les comportements trompeurs et les faux contenus en temps réel, et de renforcer considérablement l'environnement de l'information par rapport aux élections de 2018.[148]	**Résilience:** Les OSC ont lancé des campagnes de culture numérique, de sensibilisation du public et d'éducation pour renforcer l'esprit critique et donner aux citoyens des informations crédibles tout en évitant l'excès de partisannerie et la politisation de contenu.[149] Ces campagnes consistaient à: ● Briser les chambres d'écho médiatique en favorisant les dialogues intergénérationnels avec les personnes âgées. ● L'initiative « Reprenez la télécommande de la télé », dans le cadre de laquelle les étudiants ont refusé de regarder la télévision qui couvrait de manière disproportionnée des sujets prochinois.[150]
Résilience: Le gouvernement a établi un programme d'enseignement de la culture numérique pour les élèves et a demandé au comité d'éducation aux médias de veiller à ce que le programme d'enseignement de la culture numérique soit correctement mis en œuvre.[151]	**Résilience:** Facebook a organisé des événements d'éducation numérique en partenariat avec des organisations tierces de vérification d'informations, telles que Taiwan FactCheck Center, Cofacts, MyGoPen et Doublethink Lab, afin d'apprendre aux citoyens à distinguer les informations crédibles des faux contenus.	

[147] Anne Quito, « Taiwan is Using Humor as a Tool Against Coronavirus Hoaxes », Quartz (5 juin 2020), https://qz.com/1863931/taiwan-is-using-humor-to-quash-coronavirus-fake-news/.

[148] Tzu-ti Huang, « Facebook Releases Report on Fight Against Disinformation in Run-Up to Taiwan Elections », *Taiwan News* (6 octobre 2020), https://www.taiwannews.com.tw/en/news/4024275.

[149] Contributeur de la communauté g0v en discussion avec l'auteur, décembre 2020.

[150] Olivia Yang, « Defending Democracy through Media Literacy », Taiwan Democracy Bulletin 3, n° 6 (9 octobre 2019), https://bulletin.tfd.org.tw/tag/fake-news-cleaner/.

[151] Nicola Smith, « Schoolkids in Taiwan Will Now Be Taught How to Identify Fake News », *TIME* (7 avril 2017) https://time.com/4730440/taiwan-fake-news-education/; Sam Robbins, "Taiwan's Push for Media Literacy - Is it All Fake News?" *Taiwan Insight* (27 mars 2020), https://taiwaninsight.org/2020/03/27/taiwans-push-for-media-literacy-is-it-all-fake-news/.

Gouvernement		
Au niveau juridique : Le gouvernement a promulgué des réglementations, notamment des sanctions pour la diffusion de désinformation ou de rumeurs et l'ingérence dans les élections locales, comme l'amendement de la loi sur les la nomination et la révocation des présidents et vice-présidents[152] ien mai 2020 et l'adoption de la loi contre l'infiltration.[153]		

Leçons de Taïwan pour une réponse pansociale à la manipulation de l'information

Alors que d'autres organisations de la société civile, gouvernements et citoyens réfléchissent à la manière de contrer la manipulation de l'information pendant les élections et les troubles civils, l'approche pansociale taïwanaise fournit des bonnes pratiques qui peuvent être reproduites dans d'autres pays et régions.

La collaboration et les partenariats privé-public-civique sont essentiels.

L'approche de Taïwan était axée sur la mise en place rapide de partenariats solides entre le secteur privé, le secteur public et le secteur civique, afin de permettre d'identifier et de répondre rapidement et de développer la résilience face à la manipulation de l'information. Si le lancement d'initiatives telles que l'alphabétisation numérique peut prendre du temps, d'autres, comme la formation de partenariats avec des organisations de vérification des informations et des entreprises de médias sociaux, peuvent être mises en place rapidement afin de perturber la manipulation externe et interne de l'information et de démystifier les contenus et les récits erronés.

Connaissez votre public et communiquez avec empathie.

Taïwan a montré qu'une approche unique ne permet pas de lutter contre la manipulation de l'information et de renforcer la résilience. La société civile et le gouvernement taïwanais ont lancé des campagnes de sensibilisation du public et déployé des efforts d'adaptation pour éduquer les différents segments de la population, toutes générations confondues. La clé de ces efforts est l'empathie, la compassion et la suppression des barrières sociétales qui diminuent souvent la cohésion interne.

La créativité et l'innovation sont essentielles à la réussite.

Taiwan a montré que la créativité et l'innovation sont essentielles pour identifier la manipulation de l'information, y répondre et s'y adapter. L'utilisation des mèmes indique que l'humour est un outil créatif et puissant pour démystifier les faux récits et mettre en évidence les contenus crédibles. Les mèmes sont peu coûteux et très efficaces et ils peuvent être reproduits par d'autres acteurs de la société civile et par les gouvernements.

[152] Loi sur l'élection et la révocation des présidents et vice-présidents, amendée le 6 mai 2020, ministère de l'Intérieur de la République de Chine (Taiwan), https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=D0020053.

[153] Conseil des affaires continentales, République de Chine (Taïwan), « Legislative Yuan Passes Anti-Infiltration Bill to Strengthen Defense for Democracy and Preserve Stable and Orderly Cross-Strait Exchanges » (communiqué de presse), 31 décembre 2019, https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&s=88E5E1EF1343B1B8. Il est important de noter que si Taïwan a adopté un certain nombre de lois et de règlements pour contrer la désinformation et empêcher l'ingérence étrangère dans les élections, les voies légales doivent être examinées attentivement pour s'assurer qu'elles sont conformes aux principes démocratiques et aux droits de l'homme.

Annexe B : Informations complémentaires sur les plateformes de réseaux sociaux

Aperçu des politiques des plateformes de réseaux sociaux

Le tableau ci-dessous présente les liens et les points marquants des politiques des principales plateformes de réseaux sociaux concernant leurs efforts pour limiter la diffusion de més/désinformation liée aux élections.

Plateforme	Points marquants
Standards de la communauté de Facebook[154]	Les Standards de la communauté de Facebook n'interdisent pas à l'heure actuelle la més/désinformation en général, mais interdisent les contenus qui présentent de manière erronée des informations sur le vote ou les élections, incitent à la violence et qui promeuvent des discours haineux. En outre, les standards de la communauté interdisent les comportements trompeurs organisés qui se traduit par une interdiction générale des activités caractéristiques d'opérations d'information à grande échelle sur la plateforme.[155] L'entreprise a également la responsabilité de réduire la propagation de « fausses informations ». Pour rendre cela opérationnel, Facebook s'engage à réduire algorithmiquement (ou à afficher plus bas) la diffusion de ce type de contenu, en plus de prendre d'autres mesures pour atténuer son impact et dissuader sa diffusion. L'entreprise a également développé une politique de suppression de certaines catégories de médias manipulés susceptibles d'induire les utilisateurs en erreur; toutefois, cette politique a une portée limitée. Elle s'étend uniquement aux médias qui sont le produit de l'intelligence artificielle ou de machine learning et inclut une tolérance pour tout média considéré comme un contenu satirique ou un contenu qui modifie, omet ou change l'ordre des mots qui ont été réellement prononcés.[156] En mai 2021, Facebook a lancé un nouveau Centre de transparence qui contient des ressources sur ses efforts d'intégrité et de transparence à l'intention des utilisateurs. Cette nouvelle initiative montre comment Facebook détecte les violations à l'aide de la technologie et des équipes de révision, et explique l'approche en trois parties de Facebook en matière d'application des contenus : supprimer, réduire et informer.[157]

[154] Facebook, « Standards de la communauté » (Facebook, s.d), https://www.facebook.com/communitystandards/.

[155] Facebook, « Standards de la communauté : Coordination de préjudice ou promotion d'actions criminelles » (Facebook, s.d.), https://www.facebook.com/communitystandards/coordinating_harm_publicizing_crime; Facebook, « Standards de la communauté : Violence et provocation » (Facebook, s.d.), https://www.facebook.com/communitystandards/credible_violence; Facebook, « Standards de la communauté : Discours incitant à la haine » (Facebook, s.d.), https://www.facebook.com/communitystandards/hate_speech; Facebook, « Standards de la communauté : Comportement trompeur », https://www.facebook.com/communitystandards/inauthentic_behavior/.

[156] Facebook, « Standards de la communauté : Fausses informations » (Facebook, s.d.), https://www.facebook.com/communitystandards/false_news; Facebook, "Community Standards: Manipulated Media" (Facebook, n.d), https://www.facebook.com/communitystandards/manipulated_media.

[157] Centre de transparence de Facebook (Facebook, s.d.), https://transparency.fb.com; Centre de transparence de Facebook, « How We Enforce Our Policies » (Facebook, s.d.), https://transparency.fb.com/enforcement/.

Plateforme	Points marquants
Règles[158] **de Twitter**	Bien qu'il n'existe pas de politique générale en matière de mésinformation, les Règles de Twitter comprennent plusieurs dispositions relatives aux contenus et comportements mensongers ou trompeurs dans des contextes spécifiques. Les politiques de Twitter interdisent la désinformation et tout autre contenu susceptible de supprimer la participation ou d'induire les gens en erreur sur le moment, le lieu ou la manière de participer à un processus civique et les contenus comprenant des discours haineux ou incitant à la violence ou au harcèlement. Twitter interdit également les comportements trompeurs et le spam. En ce qui concerne la désinformation, Twitter a mis à jour sa politique relative aux comportements haineux afin d'interdire les propos qui déshumanisent les personnes sur la base de leur race, de leur origine ethnique ou nationale.[159] Les politiques de Twitter en matière d'élections interdisent explicitement les informations trompeuses sur le processus de vote. Toutefois, les déclarations inexactes concernant un élu ou officiel nommé, un candidat ou un parti politique sont exclues de cette politique.[160] En vertu de ces règles, Twitter a supprimé les publications contenant des informations erronées sur les processus électoraux, telles que la promotion d'un jour de vote erroné ou de fausses informations sur les bureaux de vote - des contenus que les observateurs électoraux de l'OGE et d'autres s'efforcent de surveiller et de signaler.

[158] Twitter, « Les Règles de Twitter » (Twitter, s.d.), https://help.twitter.com/en/rules-and-policies/twitter-rules.

[159] Centre d'assistance de Twitter, « Politique en matière d'intégrité civique » (Twitter, s.d.), https://help.twitter.com/en/rules-and-policies/election-integrity-policy; Centre d'assistance de Twitter, « Politique en matière de manipulation de la plateforme et de spam » (Twitter, s.d.), https://help.twitter.com/en/rules-and-policies/platform-manipulation.

[160] Centre d'assistance de Twitter, « Politique en matière d'intégrité civique »

Plateforme	Points marquants
Règlement de la communauté[161] **YouTube**	YouTube applique une politique en trois temps qui entraîne la suspension ou la suppression des comptes en infraction liés à la désinformation. Le Règlement de la communauté YouTube comprend plusieurs dispositions relatives à la désinformation dans des contextes particuliers, notamment les contenus visant à tromper les électeurs sur le moment, le lieu, les moyens ou les conditions d'admissibilité pour voter ou participer à un recensement; qui avance de fausses affirmations liées aux conditions d'éligibilité des candidats politiques et des représentants élus du gouvernement ; ou qui incite à la violence, à la haine ou au harcèlement à l'encontre d'individus ou de groupes en fonction de leurs caractéristiques intrinsèques. En outre, YouTube a également étendu sa politique de lutte contre le harcèlement, qui interdit aux créateurs de vidéos d'utiliser des discours haineux et des insultes fondés sur le sexe, l'orientation sexuelle ou la race.[162] YouTube a également élaboré une politique concernant les médias manipulés qui interdit les contenus qui ont été techniquement manipulés ou trafiqués d'une manière qui induit les utilisateurs en erreur (au-delà des clips sortis de leur contexte) et qui peuvent présenter un risque de préjudice grave. Afin de réduire davantage les risques de manipulation ou de campagnes de désinformation, YouTube dispose également de politiques qui interdisent l'usurpation d'identité les fausses déclarations sur le pays d'origine d'une personne ou la dissimulation d'une association avec un acteur gouvernemental. Ces politiques interdisent également d'augmenter artificiellement les taux de certaines métriques par l'utilisation de systèmes automatisés ou par la diffusion de vidéos auprès de spectateurs non avertis.[163]
Règles communautaires[164] **TikTok**	En août 2020, TikTok a mis à jour ses règles communautaires interdisant les contenus induisant en erreur les membres de la communauté sur les élections ou autres actes civiques, les contenus diffusés par des campagnes de désinformation et toute désinformation susceptible de nuire à la santé d'autrui.[165] TikTok a ajouté une politique qui « interdit les médias synthétiques ou médias manipulés qui induisent les utilisateurs en erreur en déformant la vérité et qui portent atteinte ». Cela inclut l'interdiction des «deepfakes» afin d'empêcher la propagation de la désinformation. TikTok a également augmenté la transparence de sa politique concernant les comportements trompeurs organisés.[166]

[161] Aide YouTube, « Règlement de la communauté YouTube » (YouTube, s.d.), https://support.google.com/youtube/answer/9288567.

[162] Aide YouTube, « Règles concernant le spam, les pratiques trompeuses et les escroqueries » (YouTube, s.d.), https://support.google.com/youtube/answer/2801973?hl=fr ; Aide YouTube, « Règles concernant l'incitation à la haine » (YouTube, s.d.), https://support.google.com/youtube/answer/2801939?hl=en&ref_topic=9282436.

[163] Aide YouTube, « Règles concernant le spam, les pratiques trompeuses et les escroqueries »; Aide YouTube, « Règles concernant l'usurpation d'identité » (YouTube, s.d.), https://support.google.com/youtube/answer/2801947?hl=fr; YouTube Help, « Règles concernant les interactions artificielles » (YouTube, s.d.), https://support.google.com/youtube/answer/3399767?hl=fr.

[164] "TikTok Community Guidelines" (TikTok, s.d.), https://www.tiktok.com/community-guidelines?lang=en#37.

[165] Vanessa Pappas, « Combating Misinformation and Election Interference on TikTok », (TikTok, 5 août 2020), https://newsroom.tiktok.com/en-us/combating-misinformation-and-election-interference-on-tiktok.

[166] Nick Statt, « TikTok is Banning Deepfakes to Better Protect Against Misinformation », The Verge, (5 août 2020), https://www.theverge.com/2020/8/5/21354829/tiktok-deepfakes-ban-misinformation-us-2020-election-interference; Vanessa Pappas, « Combating Misinformation and Election Interference on TikTok »

Plateforme	Points marquants
Règles communautaire[167] **Snapchat** 	En janvier 2017, Snapchat a créé pour la première fois des politiques visant à lutter contre la propagation de la désinformation. Snapchat a mis en place des politiques pour ses fournisseurs d'informations sur la section Découvrir de la plateforme afin de lutter contre la désinformation et de réguler les informations considérées comme inappropriées pour les mineurs. Ces nouvelles directives exigent que les médias vérifier les informations de leurs articles avant qu'ils ne puissent être affichés dans la section « Découvrir » de la plateforme.[168] Dans un éditorial, le PDG de Snapchat, Evan Spiegel, a décrit la plateforme comme étant différente des autres types de réseaux sociaux et de nombreuses autres plateformes, affirmant que « le contenu conçu pour communiquer avec des amis n'est pas nécessairement un contenu conçu pour fournir des informations exactes ». Il n'y a pas de flux d'informations provenant des utilisateurs sur Snapchat comme c'est le cas sur de nombreuses autres plateformes de réseaux sociaux - une distinction qui rend Snapchat plus comparable à une app de messagerie. Avec les mises à jour de Snapchat, la plateforme fait appel à des rédacteurs humains qui surveillent et régulent ce qui est mis en avant dans la section Découvrir pour empêcher la diffusion de fausses informations.[169]

Aperçu des fonctionnalités des produits et des interventions des plateformes de réseaux sociaux

Type de plateforme	Exemple clé des efforts de la plateforme par le biais de fonctionnalités de produit et intervention technique/humaine
Plateformes traditionnelles de réseaux sociaux	**Facebook** utilise des stratégies algorithmiques pour déclasser les informations fausses ou contestées, ce qui réduit la visibilité de ces contenus dans le fil d'actualité ; la plateforme applique des limites de diffusion aux pages et aux sites web des contrevenants récidivistes et envoie des notifications aux utilisateurs qui ont utilisé de la més/désinformation. **Twitter** utilise des messages automatiques mettant en garde les utilisateurs contre le partage de liens qu'ils n'ont pas ouverts, dans le but de « promouvoir une discussion mieux informée » et d'encourager les utilisateurs à évaluer les informations avant de les partager. Cela fait suite à l'introduction d'étiquettes de contenu et d'avertissements, que la plateforme a apposés sur les tweets qui ne sont pas susceptibles d'être supprimés en vertu des politiques de la plateforme (ou de l'exception « d'intérêt public » de la société) mais qui peuvent néanmoins contenir des informations erronées ou des médias manipulés.[170]

[167] Snap Inc., « Règles communautaires de Snapchat » (Snap Inc., s.d.), https://www.snap.com/en-US/community-guidelines.

[168] Zameena Mejia, « Snapchat Wants to Make on its Platform Disappear, Too », Quartz (23 janvier 2017), https://qz.com/892774/snapchat-quietly-updates-its-guidelines-to-prevent-fake-news-on-its-discover-platform/.

[169] Evan Spiegel, « How Snapchat is Separating Social from Media », Axios, (29 novembre 2017), https://www.axios.com/how-snapchat-is-separating-social-from-media-2513315946.html; Jamie Condliffe, « Snapchat Has a Plan to Fight Fake News: Ripping the 'Social' from 'Media' », *MIT Technology Review* (29 novembre 2017), https://www.technologyreview.com/2017/11/29/147413/snapchat-has-a-plan-to-fight-fake-news-ripping-the-social-from-the-media/; Daniel Funke, « Here's Why Snapchat's Latest Update Further Insulates it from Fake News » (Poynter, 1er décembre 2017), https://www.poynter.org/fact-checking/2017/heres-why-snapchats-latest-update-further-insulates-it-from-fake-news/.

[170] Yoel Roth et Nick Pickles, « Updating our Approach to Misleading Information », *Produit Twitter* (blog), 11 mai 2020, https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.

Type de plateforme	Exemple clé des efforts de la plateforme par le biais de fonctionnalités de produit et intervention technique/humaine
Plateformes traditionnelles de réseaux sociaux	**Instagram** supprime le contenu identifié comme étant de la désinformation des hashtags et de sa page Explorer et rend les comptes qui publient de façon répétée de la désinformation plus difficiles à trouver en filtrant le contenu de ce compte des pages consultables.[171] **TikTok** utilise la technologie pour renforcer ses pratiques de modération de contenu, notamment pour aider à identifier les comportements non authentiques, les modèles et les comptes destinés à diffuser du contenu trompeur ou du spam. L'entreprise indique que ses outils servent à faire respecter ses règles et rendent plus difficile la découverte de contenus préjudiciables, comme la désinformation et les théories du complot, dans les recommandations ou les fonctions de recherche de la plateforme. **YouTube** utilise également la technologie, en particulier le machine learning, pour renforcer ses actions.[172] Comme l'indique l'entreprise dans ses politiques, le machine learning (apprentissage automatique) est bien adapté à la détection de modèles, ce qui nous aide à trouver des contenus similaires à d'autres contenus que nous avons déjà supprimés, avant même qu'ils ne soient visionnés.
Applications de messagerie	**WhatsApp** a introduit des limites sur le transfert de messages en 2018 - ce qui empêchent les utilisateurs de transférer un message à plus de cinq personnes - ainsi que des marques visuelles pour s'assurer que les utilisateurs peuvent distinguer les messages transférés du contenu original. Dans le contexte de la pandémie de COVID-19, WhatsApp a limité davantage le transfert en annonçant que les messages qui ont été transférés plus de cinq fois ne peuvent plus être partagés qu'avec un seul utilisateur à la fois. WhatsApp a également développé des systèmes permettant d'identifier et de supprimer les comptes automatisés qui envoient de gros volumes de messages. WhatsApp expérimente actuellement des méthodes permettant de détecter des modèles dans les messages grâce à des pratiques d'évaluation par chiffrement homomorphe.[173] Ces stratégies peuvent contribuer à éclairer l'analyse et les interventions techniques liées aux campagnes de désinformation à l'avenir.

[171] Guy Rosen et al, « Helping to Protect the 2020 US Elections », (Facebook, mis à jour le 27 janvier 2020), https://about.fb.com/news/2019/10/update-on-election-integrity-efforts/.

[172] Aide YouTube, « Règlement de la communauaté YouTube ».

[173] Himanshu Gupta et Harsh Taneja, « WhatsApp has a fake news problem-that can be fixed without breaking encryption », *Columbia Journalism Review*, 23 août 2018), "https://www.cjr.org/tow_center/whatsapp-doesnt-have-to-break-encryption-to-beat-fake-news.php.

Type de plateforme	Exemple clé des efforts de la plateforme par le biais de fonctionnalités de produit et intervention technique/humaine
Moteurs de recherche	**Google** a modifié son algorithme de recherche pour lutter contre la diffusion de fake news et les théories du complot. Dans un article de blog, Ben Gomes, vice-président de Google chargé de l'ingénierie, a écrit que l'entreprise allait aider à faire apparaître des pages faisant davantage autorité et à faire apparaitre plus bas le contenu de faible qualité » dans les recherches.[174] Dans le but de fournir de meilleures orientations de recherche, Google fait appel à de vraies personnes pour agir en tant qu'évaluateurs afin d'examiner la qualité des résultats de recherche de Google et faire part de leurs commentaires sur les expériences de Google. [175] Google fournira également des « outils de rétroaction directe » pour permettre aux utilisateurs de signaler les contenus inutiles, sensibles ou inappropriés qui apparaissent dans leurs recherches.

Annexe C : Ressources supplémentaires

De nombreuses ressources sont disponibles pour aider à l'identification, à la réponse et au renforcement de la résilience face à la désinformation. Veuillez consulter ce classeur pour accéder à une liste d'outils et de ressources régulièrement alimentée et mise à jour:

Annexe de ressources sur la manipulation de l'information

Concevoir : Arra Design Consultants

[174] Le mot-clé, "Nos dernières améliorations de la qualité pour la recherche" (Google, 25 avril 2017) https://blog.google/products/search/our-latest-quality-improvements-search/.

[175] Ben Gomes, « Our Latest Quality Improvements for Search », *The Keyword* (blog), Google (25 avril 2017), https://blog.google/products/search/our-latest-quality-improvements-search/.

NDI
NATIONAL DEMOCRATIC INSTITUTE

IRI
INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

Stanford | Internet Observatory
Cyber Policy Center