GUIDE ESSENTIEL DE FIRST DRAFT SUR LES

Groupes fermés, applications de messagerie *et* publicités en ligne

Janvier 2020

FIRSTDRAFT

TABLE DES MATIÈRES

	Introduction	5
CHAPITRE 1	Comprendre les bibliothèques de publicités	13
CHAPITRE 2	Groupes Facebook	21
CHAPITRE 3	Application de messagerie fermée	27
CHAPITRE 4	Considérations éthiques	37
	Conclusion	43

À PROPOS DES AUTEURS

Carlotta Dotto est data journaliste senior chez First Draft, spécialisée dans les enquêtes fondées sur des données concernant le désordre informationnel international et les réseaux d'amplification coordonnés. Elle a précédemment fait partie de l'équipe chargée des données du journal *The Times* et de l'équipe du *laboratoire visuel de* La Repubblica, et a contribué à de nombreuses publications, par exemple pour *The Guardian*, la *BBC* et le *New Internationalist*.

Rory Smith est responsable de recherches chez First Draft et étudie et écrit sur les désordres informationnels. Avant de rejoindre First Draft, Rory a travaillé pour *CNN*, *Vox*, *Vice* et *Truthout*, sur des sujets variés allant de l'immigration et de la politique alimentaire à la politique et au crime organisé.

Claire Wardle supervise actuellement la direction stratégique et la recherche pour First Draft. En 2017, elle a co-rédigé le rapport fondamental intitulé Information Disorder: An interdisciplinary Framework for Research and Policy, for the Council of Europe[1]. Auparavant, elle a été doctorante au Shorenstein Center for Media, Politics and Public Policy de la Harvard's Kennedy School, directrice de recherche au Tow Center for Digital Journalism de la Columbia University Graduate School of Journalism et responsable des réseaux sociaux à l'Agence des Nations Unies pour les réfugiés. Elle a également été chef de projet pour la BBC Academy en 2009, où elle a conçu un programme complet de formation aux médias sociaux pour BBC News qui a été déployé dans toute l'organisation. Elle est titulaire d'un doctorat en communication de l'Université de Pennsylvanie.

Avec un chapitre de Victoria Kwan et une contribution d'Alastair Reid.

2e édition ; première publication en octobre 2019
Edition : Alastair Reid et Victoria Kwan
Production: Tommy Shane
Conception graphique: Imagist

Ce travail est soumis à la licence internationale Creative Commons : Usage-Non-Commercial-PasDeDérivés. Pour consulter une copie de cette licence, rendez-vous à l'adresse suivante : of this license, visit: http://creativecommons.org/licenses/by-nc-nd/4.0/

Merci

Nous remercions notre équipe de journalistes multilingues, qui a contribué à la révision des traductions dans plusieurs langues, sous la direction d'Emma Dobinson, responsable de la version préliminaire : Pedro Noel (portugais brésilien), Carlotta Dotto (italien), Marie Bohner (français), Laura Garcia (espagnol), Nadin Rabaa du GNL Berlin (allemand) et le professeur Umesh Arya de DataLEADS (hindi).

La version originale de ce guide a été publiée en anglais en octobre 2019.
La version en français a été traduite par Global Lingo et révisée par les membres de l'équipe de la version préliminaire pour en assurer l'exactitude. Cette version traduite a été publiée en juin 2020.

Tous les Guides essentiels en français

Introduction

En 2016, les réseaux sociaux, les moteurs de recherche, les rédactions et le public étaient loin d'être préparés à la mésinformation sur les élections.

Des titres proposés par les adolescents macédoniens[1] aux publicités Facebook publiées par l'Agence russe de recherche sur Internet[2], en passant par les réseaux automatisés et coordonnés par des humains qui diffusent des hashtags semant la discorde[3], tout le monde a été dupé.

Trois ans et demi plus tard, les stratagèmes utilisés en 2016 suscitent une plus grande prise de conscience, notamment grâce aux mesures mises en place par les entreprises technologiques. Google et Facebook ont modifié leur politique[4], rendant plus difficile la monétisation du contenu des sites d'informations fabriqués de toutes pièces. Facebook a créé une bibliothèque de publicités[5] afin qu'il soit plus simple de savoir qui consacre de l'argent au financement de la publicité sociale et politique sur la plateforme. Twitter a gagné en efficacité pour démanteler les réseaux automatisés[6].

> « Les entreprises technologiques ont renforcé leurs politiques et mis en place des projets comme celui de Facebook intitulé "Third Party Fact-Checking project"[7] afin de déclasser les faux contenus dans le flux d'informations, et ont investi dans des ressources techniques supplémentaires pour surveiller ces menaces. »

Il est toutefois peu probable que les mêmes tactiques observées en 2016 se reproduisent en 2020. Ceux qui

veulent promouvoir des contenus conflictuels et trompeurs sont en train de développer et de tester de nouvelles techniques qui ne seront pas affectées par les nouveaux développements de la plateforme.

S'il est impossible de savoir exactement ce qui se passera en 2020, l'une des possibilités les plus inquiétantes est que cette désinformation se propage dans des endroits plus difficiles à surveiller, notamment les groupes Facebook et les applications de messagerie fermées.

Les publicités sur Facebook posent toujours problème. L'une des caractéristiques les plus puissantes de Facebook réside dans sa gamme de produits publicitaires. Elle permet aux administrateurs d'une page Facebook de cibler un groupe très spécifique de personnes, comme les femmes âgées de 32 à 42 ans qui vivent à Raleigh-Durham, ont des enfants, sont diplômées, sont juives et aiment la page Facebook d'Elizabeth Warren, par exemple.

Facebook donne même la possibilité aux acheteurs de publicité de tester ces publicités dans des environnements qui autorisent d'enregistrer des échecs en privé. Ces « dark ads » permettent aux organisations de cibler certaines personnes, mais elles ne figurent pas sur la page Facebook principale de l'organisation, ce qui les rend difficiles à suivre. Au début de l'année, Facebook a lancé Ad Library[8], qui vous permet de consulter les types d'annonces diffusées par certains candidats ou de faire des recherches par mots clés comme « armes ». Vous trouverez dans ce guide des explications quant à l'utilisation d'Ad Library.

Une autre menace majeure sera la fuite d'informations préjudiciables ou fausses vers les rédactions à des fins politiques. Dans la période précédant l'élection présidentielle française de 2017, des soi-disant documents sur les finances personnelles du Président Macron ont fait l'objet d'une fuite 44 heures avant l'élection[9]. En France, la loi interdit les reportages sur les candidats et leurs

partisans pendant cette période et les rédactions françaises ont accepté de respecter la loi, ce qui signifie que les informations divulguées n'ont pas été amplifiées.

Toutefois, aux États-Unis, la fuite et la publication de courriers électroniques liés à Hillary Clinton[10] et au personnel du Democratic National Committee dans les semaines précédant le jour des élections ont emprunté un chemin bien différent. Selon une étude publiée dans la Columbia Journalism Review[11] « en six jours seulement, The New York Times a publié autant d'articles de couverture sur les courriers électroniques d'Hillary Clinton que sur toutes les questions politiques réunies au cours des 69 jours précédant l'élection ».

Une tribune dans le New York Times de Scott Shane de mai 2018, intitulée When Spies Hack Journalism[12], vaut la peine d'être lue. Comme l'écrit M. Shane : « Les anciennes règles stipulent que si les organismes de presse obtiennent du contenu qu'ils jugent à la fois authentique et digne d'intérêt, ils doivent le diffuser. Pourtant, ces conventions peuvent piéger les journalistes et inciter les agences d'espionnage à manipuler ce qu'ils publient, et cela comporte un danger supplémentaire : Des archives de documents authentiques truffées de faux. »

Dans l'ensemble, les menaces sont déplacées vers des emplacements plus difficiles à observer. En 2020, plusieurs pays seront amenés à tenter d'influencer les élections, pas uniquement la Russie. Et si chacun aime se concentrer sur l'ingérence étrangère, les acteurs nationaux — qu'il s'agisse d'agents de campagne, de partisans de certains candidats ou de ceux qui tentent de semer la zizanie pour le plaisir — seront également mobilisés. Il y aura un endroit où les chemins se croiseront. Les entreprises technologiques ayant pris des mesures de répression à l'encontre des entités étrangères qui paient pour des publicités, et des indices comme une adresse IP étrangère sont un signal d'alarme

potentiel, nous voyons le ciblage des acteurs et des personnes d'influence nationaux comme un moyen de pousser ou d'amplifier un message. Par conséquent, bien que cela puisse avoir un caractère national, il est possible qu'il y ait des liens qui mènent à d'autres endroits.

Si vous n'avez pas vu l'excellent documentaire du *New York Times* intitulé Operation Infektion[13] sur la similarité des pratiques actuelles en matière d'information avec celles du KGB dans les années 1980 et 1990, nous vous le recommandons vivement.

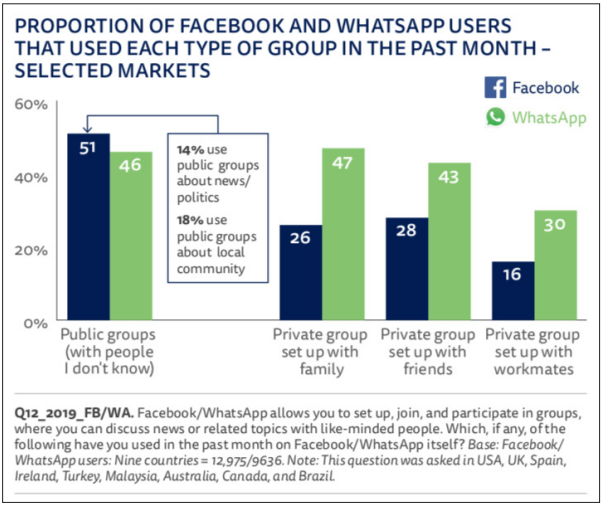
EN QUOI CES ZONES D'OMBRE SONT-ELLES SI INQUIÉTANTES ?

En mars 2019, Mark Zuckerberg a annoncé un tournant pour Facebook en matière de vie privée[14]. Cette description traduit en fait ce qui avait déjà commencé à se produire. Au cours des dernières années, les internautes ont quitté les espaces où ils pouvaient être observés et ciblés, probablement parce qu'ils ont appris le fonctionnement des publications dans les espaces publics. Les enfants grandissent et se plaignent de n'avoir jamais consenti à la publication de leurs photos de bébé sur Google. Des personnes perdent leur emploi après avoir bu ou simplement envoyé des tweets peu judicieux, ou se rendent compte que les forces de l'ordre, les experts en assurances et les agents de protection des frontières surveillent tout ce qui est publié sur le Net. Le harcèlement en ligne est une réalité alarmante, qui vise en particulier les femmes et les personnes de couleur.

Certains réagissent en rendant leur profil Instagram privé. D'autres lisent les conseils de confidentialité de Facebook et limitent les informations disponibles sur leur profil, ou s'autocensurent sur Twitter [15]. Dans certaines régions du

monde, la réglementation visant à punir ceux qui partagent de fausses informations pourrait avoir un effet dissuasif sur la liberté d'expression[16], selon des militants, ce qui inciterait encore plus à opter pour des applications fermées.

Cette transition vers un espace fermé est tout à fait compréhensible et nous pensons que les historiens considéreront les dix dernières années comme une période très étrange et unique où les populations étaient en fait heureuses de partager leurs activités et leurs opinions. Ce n'est en fait qu'un retour à la norme, où les conversations avec des groupes plus restreints de personnes, en particulier celles avec lesquelles vous avez un niveau de confiance ou d'affinité plus élevé, constituent le point pivot vers la vie privée.



Comment les utilisateurs de Facebook et de WhatsApp se fient aux groupes pour les actualités et la politique . Reuters Institute for the Study of Journalism.

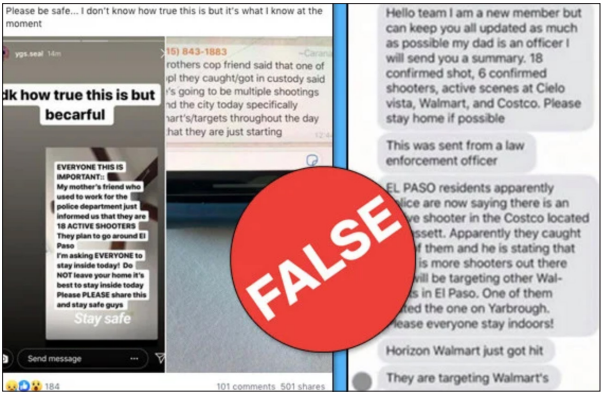
Ce graphique extrait du 2019 Reuters Institute Digital News Report[17] révèle le nombre de personnes qui dépendent actuellement des groupes sur Facebook et WhatsApp pour obtenir des informations et participer à la vie politique.

Cette évolution complique toutefois la tâche des journalistes qui tentent de comprendre, de réfuter et de ralentir la diffusion de rumeurs virales et de fausses informations.

Si les informations circulent sur des applications de messagerie fermées, qu'il s'agisse de WhatsApp, iMessage ou FB Messenger, leur provenance est inconnue. Aucune métadonnée ne peut donc être trouvée. Il est impossible de savoir d'où les rumeurs ont commencé et comment elles ont circulé sur le réseau.

Beaucoup de ces espaces sont cryptés. Il n'y a aucun moyen de les observer avec Tweetdeck ou CrowdTangle. La recherche avancée n'est pas disponible sur WhatsApp. Bien que le cryptage soit un point extrêmement positif, lorsqu'il s'agit de traquer la désinformation, en particulier la désinformation conçue pour être cachée, comme les campagnes de suppression d'électeurs, cela suscite des inquiétudes.

Jane Lytvynenko de *BuzzFeed* suit régulièrement les rumeurs et les mensonges qui circulent dans les médias. C'est en regardant les événements se dérouler lors des fusillades de masse à El Paso et Dayton à la mi-août 2019 qu'elle a vu pour la première fois des niveaux significatifs de contenu problématique circuler dans des espaces fermés, notamment les groupes FB messenger, Telegram, Snapchat et Facebook - Observations qu'elle a consignées sur Buzzfeed.[18]



La mésinformation sur les fusillades d'El Paso et de Dayton a circulé dans des espaces de messagerie fermés. Buzzfeed.

Ce changement de tactique crée un certain nombre de nouveaux défis pour les journalistes, en particulier des défis d'ordre éthique. Quels sont ces groupes ? Une fois que vous les avez trouvés, devez-vous les rejoindre ? Devez-vous faire preuve de transparence quant à votre identité lorsque vous rejoignez un groupe sur une application de messagerie fermée ? Pouvez-vous communiquer les informations que vous avez recueillies auprès de ces groupes ? Pouvez-vous automatiser le processus de collecte des commentaires issus de ces types de groupes ? Nous aborderons ces questions et bien d'autres tout au long de ce guide.

CHAPITRE 1

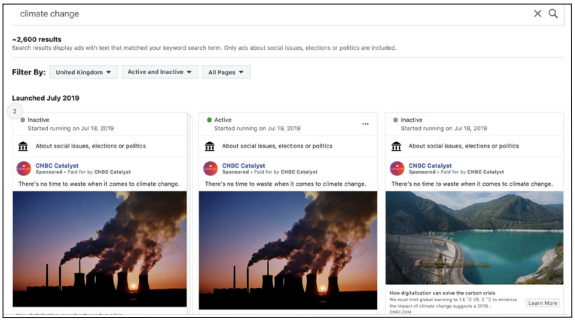
Comprendre les bibliothèques de publicités

Avec les contributions de
Alastair Reid
Rédacteur en chef numérique

Ad Library de Facebook vous permet d'enquêter sur les publicités diffusées sur les produits Facebook. La bibliothèque est accessible à tous. Il n'est pas nécessaire de créer un compte Facebook - la bibliothèque permet à tout le monde de voir des publicités actives et inactives sur n'importe quel sujet.

Pour les journalistes et les chercheurs, cet outil laisse une marge de manœuvre sans précédent pour faire de la veille et trouver des informations sur les publicités politiques dans le monde entier, y compris sur les personnes qui paient pour ces publicités.

Vous pouvez utiliser la fonction recherche pour trouver des informations portant sur la politique, les élections ou les aspects sociaux. Si vous recherchez par exemple « changement climatique », la bibliothèque affichera une liste de toutes les annonces actives et inactives qui ont été diffusées sur le sujet.

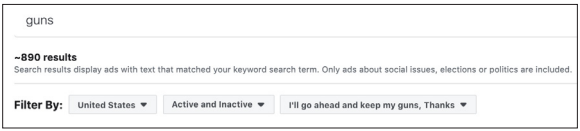


Ad Library de Facebook vous montrera une liste de toutes les publicités actives et inactives qui ont été diffusées sur un sujet particulier. Capture d'écran de l'auteur.

En cliquant sur chaque annonce, vous obtiendrez des informations plus précises, notamment le nom de la personne qui a financé l'annonce, le lieu où elle a été diffusée, la population visée et des informations essentielles sur les sommes dépensées pour l'annonce.

Vous pouvez associer votre recherche à divers filtres pour préciser si vous souhaitez consulter des annonces dans le monde entier ou dans un pays en particulier, et si vous préférez les annonces inactives ou actives, voire les deux. Vous pouvez également rechercher des mots clés et filtrer les résultats par pages Facebook spécifiques.

Par exemple, vous pouvez rechercher des armes à feu et limiter les résultats à la page « I'll go ahead and keep my guns, Thanks" » pour avoir un aperçu de sa campagne publicitaire et identifier ceux qui la financent.



Ad Library vous permet également de limiter les résultats de recherche par page. Capture d'écran de l'auteur.

Le rapport d'Ad Library de Facebook est également disponible. Vous trouverez ici un aperçu général de toutes les publicités Facebook liées aux aspects sociaux, aux élections et à la politique pour différents pays et différentes périodes. Vous pouvez télécharger ces rapports au format CSV pour les analyser ultérieurement.

Vous pouvez également accéder à l'API d'As Library de Facebook pour obtenir des données encore plus granulaires ou pour constituer votre propre base de données de publicités Facebook. Facebook a publié un guide[19] reprenant les instructions d'installation et d'utilisation.

La bibliothèque comporte toutefois des limites. Une fois qu'elles sont inactives, vous ne pouvez pas accéder aux publicités signalées comme apolitiques. L'API a été critiquée[20] pour son manque de rigueur, car elle fournit des données incomplètes qui pourraient affecter la fiabilité de vos activités de veille et de recherche.

Assurez-vous également de désactiver votre bloqueur de pubs lorsque vous utilisez la bibliothèque - cela pourrait affecter vos recherches - et méfiez-vous si votre recherche ne renvoie aucun résultat. Si vous actualisez la page et effectuez à nouveau la recherche, vous obtiendrez probablement une nouvelle liste de résultats.

GOOGLE AD TRANSPARENCY REPORT

Google a lancé son outil de transparence des publicités[21] en août 2018. Il ne dispose pas des mêmes fonctionnalités que Facebook et ne fonctionne actuellement qu'aux États-Unis, en Europe et en Inde, mais il propose des annonces sur les réseaux publicitaires de Google, YouTube et d'autres « réseaux partenaires ».

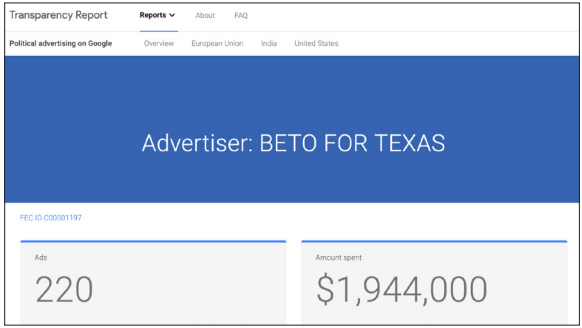
La base de données est mise à jour hebdomadairement et contient des informations sur les « dépenses consacrées aux annonces liées aux élections qui présentent un candidat à une fonction élective, un fonctionnaire en exercice ou un parti politique dans un système parlementaire », selon Google.

La première chose que vous voyez en cliquant sur l'une des trois régions est une carte qui ventile les dépenses publicitaires pour chaque circonscription électorale participante : pays de l'UE ou États des États-Unis et de l'Inde.

Si vous faites défiler la carte, vous verrez les différents annonceurs enregistrés, classés selon leurs dépenses, et une bibliothèque de toutes les annonces pour l'ensemble de la région. Les utilisateurs peuvent les explorer par date, par dépense, par impression et par format.

Plus bas, il est possible d'explorer les organisations de campagne politique qui dépensent le plus, pour voir combien d'argent elles ont dépensé et à quoi ressemblent les annonces.

Les utilisateurs peuvent également effectuer des recherches dans la bibliothèque pour chaque région par candidat ou par mot clé et télécharger les données au format CSV pour approfondir leur recherche.



Outil Ad Transparency de Google
Capture d'écran de l'auteur.

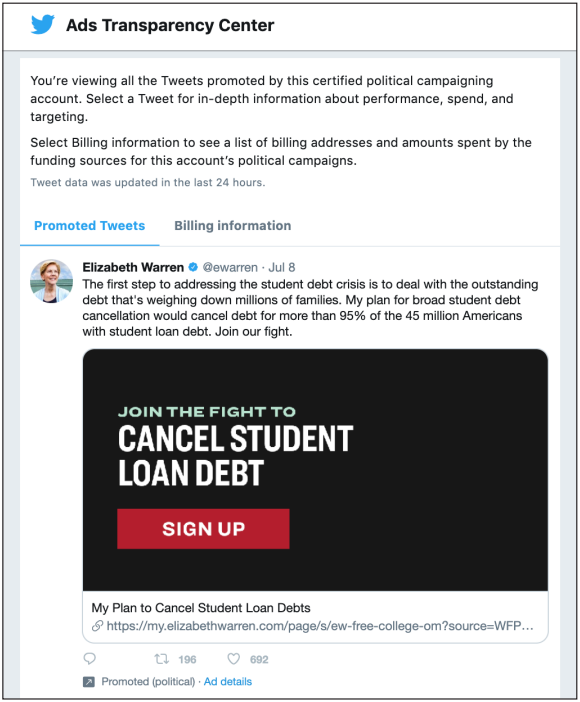
ANNONCES SUR TWITTER

Note du rédacteur : En novembre 2019, peu avant sa publication, le PDG de Twitter, Jack Dorsey, a annoncé que la plateforme restreindrait toute publicité politique dans le monde entier, notamment en interdisant aux partis politiques, aux candidats à des fonctions politiques et aux fonctionnaires élus ou nommés de diffuser la moindre publicité.[22]

Le Centre de transparence des publicités de Twitter a été lancé au cours de l'été 2018 et contient des informations sur les « annonceurs de campagnes politiques » aux États-Unis, en Europe, en Australie, en Inde et au Canada, avec des définitions juridiques distinctes pour chaque pays.

Des dizaines d'annonceurs de ce type figurent dans la base de données pour les États-Unis et une liste réservée aux États-Unis pour les « annonceurs thématiques ». Il existe entre cinq et vingt annonceurs politiques en Europe, en Inde et au Canada, et seulement trois en Australie. Le site indique que Twitter exige des annonceurs de campagnes politiques qu'ils s'identifient, il n'est donc pas évident de savoir dans quelle mesure ces listes sont complètes.

Si le compte officiel de Joe Biden est celui d'un annonceur politique enregistré, celui de Donald Trump ne l'est pas (du moins au moment de la rédaction du présent document). Par conséquent, bien que nous puissions voir tous les tweets promotionnels de Joe Biden depuis qu'il s'est inscrit comme annonceur politique sur la plateforme, nous ne pouvons voir que les tweets promotionnels de @realDonaldTrump pour les sept derniers jours. Compte tenu de la présence habituelle de M. Trump sur la plateforme et de sa position de leader du pays le plus puissant du monde, il ne devrait pas avoir à payer pour une telle campagne de promotion. Mais, dans l'état actuel des choses, il est difficile de savoir s'il l'a fait.



Outil Ad Transparency de Google Capture d'écran de l'auteur.

L'outil le plus puissant du Twitter Ads Transparency Center est dissimulé dans le coin supérieur droit du site : une barre de recherche qui permet aux utilisateurs de trouver n'importe quel compte et de voir les publicités qu'il a financées au cours des sept derniers jours.

Si l'annonceur s'est "identifié", toutes les publicités diffusées par le compte depuis l'ouverture de la base de données s'affichent, ainsi que des informations supplémentaires sur la facturation, à savoir qui a payé pour la publicité, combien, et un petit lien hypertexte marqué « Ad details » sur le tweet promu lui-même.

Il suffit de cliquer ici pour afficher un résumé particulièrement complet de la campagne, avec les données démographiques ciblées et les personnes qui ont effectivement vu une publicité, leur lieu de résidence, leur âge, leur sexe et leur langue.

ANNONCES SNAPCHAT

Il convient de mentionner Snapchat, qui semble avoir essayé de se mettre à l'abri de toute critique potentielle en faisant une bibliothèque publique de publicités politiques et de « plaidoyers ».

L'offre est basique, mais détaillée. Les utilisateurs téléchargent un CSV de toutes ces publicités pour 2018 ou 2019 et s'en donne à coeur joie pour l'exploration des données, en découvrant les organisations, l'argent dépensé, les impressions, les messages, les données démographiques, les liens et les images associés à chaque publicité.

Le tableur de 2019 ne contenait qu'environ 2 000 entrées, mais il offre des informations précises qui manquent aux autres plateformes dont il est question ici.

CHAPITRE 2

Groupes Facebook

Fin avril 2019, Facebook a annoncé se focaliser dorénavant beaucoup plus sur les groupes.

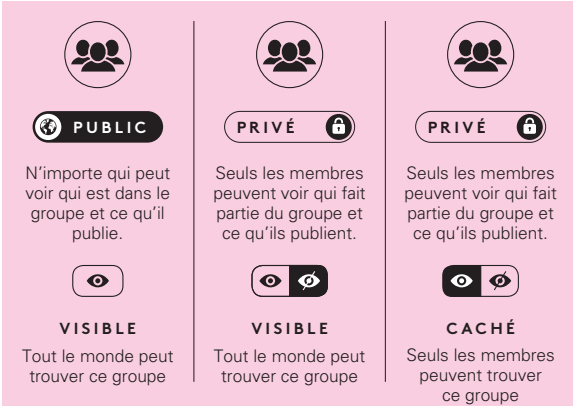
TYPES

Trois types de groupes Facebook ont été créés : Public, Privé et Caché.

L' « anti-sèches » ci-dessous permet d'expliquer les différences. Les groupes publics et privés peuvent être trouvés dans la recherche Facebook, mais, s'il s'agit d'un groupe dit « caché », vous devez en faire la demande et un administrateur du groupe vous y donnera accès le cas échéant.

Mark Zuckerberg a annoncé une réorientation des groupes Facebook en 2019. Capture d'écran de l'auteur.

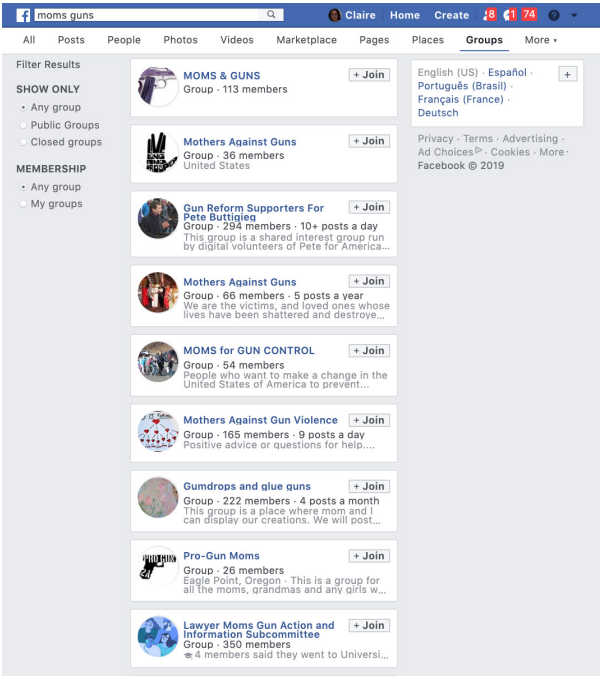
Ces groupes vous poseront parfois des questions spécifiques sur vos points de vue et opinions, et/ou vous demanderont de vous engager à respecter une certaine confidentialité ou un code de conduite. (Cela peut créer des problèmes éthiques pour les journalistes, comme nous le verrons plus loin dans ce guide.)



Les groupes Facebook : les trois types. Capture d'écran de l'auteur.

COMMENT LES RECHERCHER

Vous pouvez rechercher des groupes en utilisant la recherche sur Facebook. Vous trouverez ci-dessous une recherche simple pour les groupes liés à « Moms and Guns » (que l'on pourrait traduire par « Mamans et armes à feu »). Vous pouvez voir dans les résultats que Facebook lit « Moms » (Mamans) et en tire également des résultats qui incluent le mot « mother » (mère).



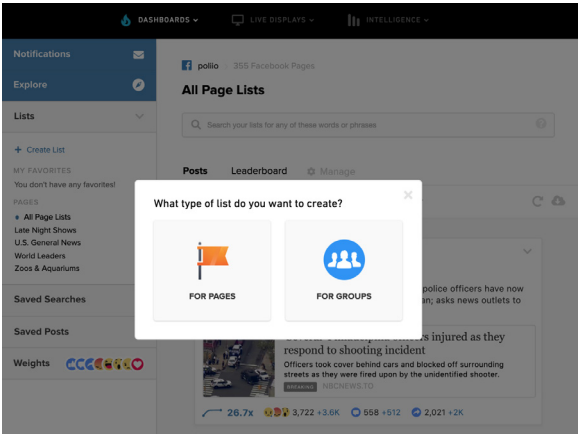
Vous pouvez utiliser la barre de recherche native de Facebook pour rechercher des groupes sur un sujet précis. Capture d'écran de l'auteur.

Si vous avez besoin d'utiliser des opérateurs de recherche plus complexes, vous pouvez effectuer une recherche dans Google en utilisant quelque chose comme « Moms AND guns » (Mères ET armes à feu) « el paso » site:facebook.com/groups

Il est difficile de faire une veille des groupes Facebook, à moins d'utiliser CrowdTangle, la plateforme que Facebook a rendue gratuite pour les journalistes en 2017.

Dans CrowdTangle, vous pouvez créer des listes de groupes Facebook publics et recevoir des mises à jour régulières sur les messages les plus populaires des groupes. CrowdTangle ne contient néanmoins aucune information privée, de sorte que les groupes privés ou cachés ne sont accessibles que sur la plateforme principale de Facebook.

Pour en savoir plus, consultez le guide essentiel de First Draft sur la collecte d'informations et la veille sur le Web social[23]



Vous pouvez utiliser CrowdTangle pour constituer des listes de groupes Facebook à observer. Capture d'écran de l'auteur.

CHAPITRE 3

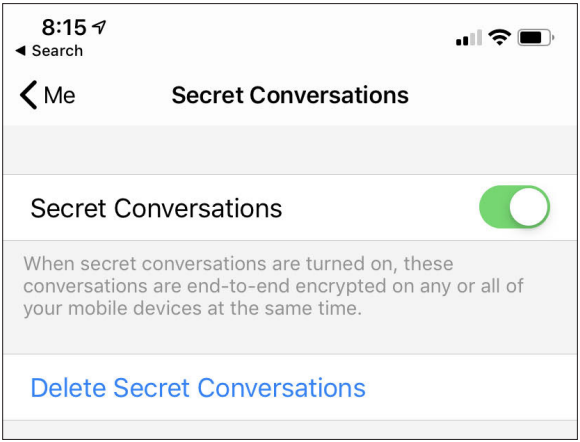
Applications de messagerie fermée

L'utilisation d'applications de messagerie fermée est significative au niveau mondial. On dénombre plus de 1,5 milliard d'utilisateurs de WhatsApp et 1,3 milliard d'utilisateurs de Facebook Messenger. Certaines applications sont natives de certains pays, comme KakaoTalk en Corée et WeChat en Chine, tandis que d'autres sont plus populaires dans certains pays, même si elles sont largement disponibles, comme Telegram en Iran, Viber au Myanmar et LINE au Japon.

Cependant, il existe des différences dans le niveau de cryptage. Par exemple, WhatsApp est crypté par défaut, tandis que Telegram offre un cryptage de bout en bout pour les appels vocaux et, en option, des chats « secrets » cryptés de bout en bout entre deux utilisateurs en ligne, mais pas encore pour les groupes ou les canaux.

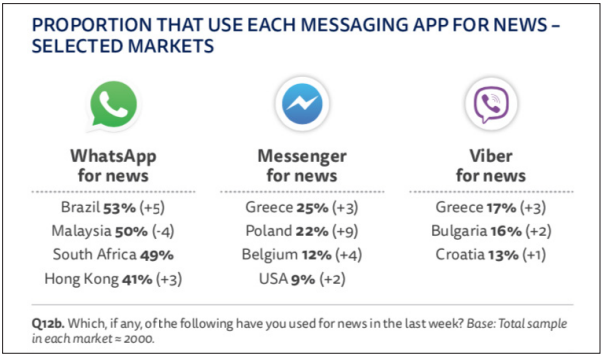
Certaines applications vous permettent de choisir librement le cryptage. Dans les paramètres de l'application Messenger de Facebook, vous pouvez accéder aux « conversations secrètes » et y activer le cryptage. C'est important si vous accédez à des sources quelconques via Facebook. Vérifiez que le cryptage est également activé avant de commencer à discuter avec elles.

Si votre objectif est vraiment de vous protéger et de protéger vos sources, Signal est l'application la plus recommandée aux journalistes par les spécialistes de la sécurité, car elle comprend le cryptage et prévoit une option d'autodestruction des messages après un certain laps de temps.



Vous pouvez crypter les conversations sur Facebook Messenger en activant « Conversations secrètes ». Capture d'écran de l'auteur.

Il est facile d'écarter les applications de messagerie fermée et de les considérer comme une autre forme de SMS, mais il est important de comprendre que ces espaces sont utilisés de manière très inégale par les différentes communautés. Par exemple, le 2019 Reuters Institute Digital News Report a révélé que près de la moitié ou plus des personnes interrogées dans des pays comme le Brésil, la Malaisie et l'Afrique du Sud utilisent WhatsApp pour accéder aux informations.



Popularité des applications de messagerie fermée dans le monde entier. Reuters Institute for the Study of Journalism.

WHATSAPP

WhatsApp est l'application de messagerie la plus populaire au monde. Avec 1,5 milliard d'utilisateurs, l'application de messagerie appartenant à Facebook est déjà la principale application de messagerie dans des pays comme l'Espagne, le Brésil et l'Inde. La fonction de chat de groupe de l'application a révolutionné la communication mobile, devenant rapidement l'un des outils les plus populaires pour échanger des informations sur les manifestations, les événements et les élections.

La nature fermée de ces groupes ainsi que le cryptage de bout en bout de WhatsApp ont empêché de nombreux journalistes et chercheurs d'observer le service de messagerie. Cependant, au cours des dernières années, plusieurs moyens de suivre de près le service ont émergé.

Vous pouvez rechercher manuellement les groupes WhatsApp publics sur diverses plateformes comme Google, Facebook, Twitter et Reddit, en utilisant le terme de recherche chat.whatsapp.com. Vous pouvez adhérer à chaque groupe et les suivre individuellement. La manière dont vous utilisez les informations recueillies auprès de ces groupes nécessite des considérations éthiques (voir ci-dessous).

Il existe un moyen d'observer ces groupes informatiquement, mais cela va à l'encontre des conditions d'utilisation de WhatsApp. Vous pouvez trouver sur le Web des groupes WhatsApp ouverts au public, liés à votre pays ou à votre région. Cette technique a été utilisée principalement par des chercheurs[24] et a suscité des débats quant à l'éthique de cette approche[25].

Les méthodes de décryptage et de récupération décrites ici soulèvent de sérieuses préoccupations éthiques, notamment en ce qui concerne les violations de la vie privée. Vous et votre organisation devez examiner ces aspects avec beaucoup de soin, de réflexion et de planification avant de recourir à ces techniques.

La façon la plus simple d'observer et de rechercher des informations spécifiques sur WhatsApp est d'établir une ligne d'informations et de signalisations sur des sujets particuliers, qui peut être connectée à un téléphone de votre rédaction. En fonction de la quantité de conseils et d'informations, vous pouvez envisager de l'intégrer à Zendesk (service payant), qui vous offre une plus grande souplesse pour organiser ces informations et signalisations.

Dans le cadre de Comprova, le projet de journalisme collaboratif de First Draft autour des élections brésiliennes de 2018[26], les organisateurs ont créé une ligne d'information et de signalisation centrale 12 semaines avant le jour du scrutin, et le projet a reçu plus de 100 000 messages du public.

TELEGRAM

Telegram présente des fonctionnalités similaires à celles de WhatsApp, en ce sens qu'il existe des groupes et des chats individuels cryptés, mais là où WhatsApp limite les groupes à 256 membres, les groupes de base de Telegram en comptent 200. Les supergroupes sur Telegram peuvent contenir 100 000 personnes par groupe.

La principale différence avec WhatsApp est que Telegram propose également une fonctionnalité appelée « channels », qui permet à une personne ou une organisation de « diffuser » à un nombre illimité d'abonnés.

Telegram s'est forgé une réputation de plateforme de messagerie privilégiée par les extrémistes. Autrefois lieu de résidence des partisans de l'État dit islamique, cette plateforme a également vu affluer ces derniers mois des extrémistes d'autres obédiences, car les grandes plateformes répriment les activités qui enfreignent les directives de leur communauté.

DISCORD

Discord est une application de messagerie en temps réel très populaire auprès des gamers. Au cours des dernières années, elle a toutefois acquis la réputation d'être un lieu de conversation privilégié pour les sujets politiques et sociaux.

Au cours de la #MacronLeak, il était possible de trouver des personnes parlant de tactiques et de techniques (comme le souligne cette publication[27] de Ben Decker et Padraic Ryan à l'époque). Il existe également des liens entre ceux qui fréquentent des forums anonymes comme Reddit et 4chan, et vous pouvez trouver sur ces derniers des liens courts vers les communautés Discord.

Le service est organisé par des serveurs, également appelés des guildes. Durant la période précédant les élections intermédiaires de 2016 aux États-Unis, il était possible de suivre des conversations où les gens coordonnaient des serveurs autour de campagnes ou de candidats particuliers.

Dans son guide de 2018 pour les journalistes effectuant des reportages dans des espaces fermés et semi-fermés[28], Mark Frankel, ancien rédacteur en chef des médias sociaux de la BBC, décrit Discord comme suit :

« Pour ceux qui sont moins à l'aise pour parler dans un forum en ligne entièrement ouvert ou public, Discord se veut une alternative. En effectuant des recherches quotidiennes sur différents serveurs, j'ai constaté que de nombreuses personnes partageaient des liens vers des documents que je n'avais pas vus sur des sites Web publics et parlaient librement d'un certain nombre de sujets, de l'attitude de l'administration Trump à l'égard des enfants migrants aux arrêts de la Cour suprême et aux campagnes locales des gouverneurs. À bien des égards, la plateforme rappelle les débuts du Web social où des groupes largement anonymes traînaient sur MySpace, AOL ou Yahoo. »

Certains serveurs sont accessibles et tout le monde peut s'y inscrire. D'autres vous demandent de « prouver » votre identité en vous connectant à d'autres profils numériques et vous poseront des questions avant de vous laisser entrer, comme c'est le cas pour certains groupes Facebook.

Une capture d'écran incluse dans le guide de Frankel vous donne un exemple de l'un de ces questionnaires de « contrôle ».

VETTING QUESTIONS

Heritage:

Nation of residence:

Ideology:

Describe Ideology:

Influential books you've read:

Username of who posted/gave you the server invite:

Name your heroes:

Opinion on Israel:

Opinion on Holocaust:

Opinion on Trump:

Opinion on Conservatives:

Opinion on Jews:

Opinion on Communism:

Opinion on Globalism:

Questions de « contrôle » sur Discord.
Capture d'écran de Mark Frankel pour Nieman Lab.

Nous recommandons aux journalistes qui souhaitent passer du temps sur Discord, de recourir à un VPN. Nous vous recommandons également de discuter à l'avance avec votre rédacteur en chef de certains des inconvénients inhérents à votre présence sur la plateforme. Bien qu'il soit possible de se cacher dans ces espaces, il est nécessaire de réfléchir aux répercussions potentielles liées à la publication d'informations provenant de ces applications fermées. Pour en savoir plus, veuillez consulter la section sur les aspects éthiques à la fin de ce document.

Deux guides peuvent vous être utiles : « Secure Your Chats »[29] de Net Alert et « Guide to ChatApps[30] de 2015 », de Trushar Barot et Eytan Oren.

CHAPITRE 4

Aspects éthiques

Rédigé par Victoria Kwan
Rédactrice en chef de l'éthique et des standards

Que vous cherchiez à comprendre les idéologies de groupes potentiellement hostiles ou à écrire un article à caractère humain sur une communauté traditionnellement secrète, le fait d'entrer dans des groupes et des applications de messagerie fermés présente différents défis éthiques, sécuritaires, voire juridiques.

Cet article d'*ABC Australia*[30] sur l'expérience d'une femme dont le commentaire dans un groupe privé sur Facebook a été amplifié par les médias vaut la peine d'être lu, car il rappelle que les petites décisions des journalistes peuvent avoir un impact considérable sur celles et ceux dont les mots sont utilisés.

Avant de commencer votre enquête, passez soigneusement en revue la politique existante de votre organisation concernant la collecte d'informations dans des espaces en ligne fermés avec votre rédacteur en chef, le bureau d'éthique et de standards et l'équipe juridique. Si votre rédaction ne dispose pas d'une telle politique, consultez vos interlocuteurs sur la meilleure façon de procéder à votre collecte d'informations.

La première question à se poser :

- Existe-t-il des moyens d'obtenir l'information que vous recherchez sans avoir à entrer dans des espaces en ligne fermés ?

VIE PRIVÉE ET INTÉRÊT PUBLIC

Si la réponse est non, nous vous recommandons de passer aux questions suivantes. Elles permettent notamment de soupeser le respect de la vie privée et les dommages potentiels par rapport à l'intérêt public, et vous encouragent à réfléchir à la proportionnalité :

- Que comptez-vous obtenir en rejoignant ce groupe - des sources, des conseils ou des connaissances de base pour nourrir vos enquêtes ? Ou est-ce que l'existence et le contenu du groupe lui-même sont au cœur de votre reportage ?
- S'agit-il d'un groupe qui s'attend à des « curieux » ? Les membres s'attendent-ils naturellement à ce que les conversations et autres contenus de ces groupes soient rendus publics ?
- Quelle est la taille de chaque groupe fermé dans lequel vous prévoyez d'entrer, et comment cela affecte-t-il les attentes en matière de respect de la vie privée pour chaque groupe ?
- Le fait d'écrire un article exposerait-il les membres du groupe à des conséquences négatives ?
- Quel est l'intérêt du public pour votre éventuel article ?
- Prévoyez-vous d'entrer dans plusieurs groupes ? Quel est le nombre minimum d'espaces fermés dans lesquels vous pouvez entrer pour trouver les informations dont vous avez besoin ?

TRANSPARENCE VS SÉCURITÉ

Demandez-vous ensuite si vous allez utiliser votre véritable identité pour entrer dans le groupe fermé et si vous allez révéler votre identité ou simplement refuser de la dissimuler.

Savoir prendre ces décisions de manière responsable nécessite à la fois une compréhension du groupe dans lequel vous entrez et une compréhension de votre propre identité par rapport au groupe, en mettant en balance la transparence et la sécurité :

- Quel est l'objectif de ce groupe ? Le groupe est-il susceptible d'être hostile, et comment les membres du groupe réagiraient-ils face à un journaliste parmi eux ? Entrer dans un groupe fermé qui prône des idéologies extrémistes, par exemple, peut aboutir à des conclusions différentes que d'entrer dans une conversation WhatsApp composée de parents locaux ou d'un groupe secret d'employés cherchant à se syndiquer.
- Votre présence au sein du groupe, en utilisant votre véritable identité, est-elle susceptible de susciter un regain d'attention imprévu ? Les journalistes femmes et de couleur, par exemple, peuvent être confrontées à des problèmes de sécurité supplémentaires lorsqu'elles entrent dans certains groupes potentiellement hostiles, ce qui peut les amener à prendre une décision différente en matière de divulgation.
- Si vous décidez d'entrer dans le groupe en utilisant votre véritable identité, à qui divulguerez-vous cette information ? Les divulguerez-vous à l'administrateur du groupe ou à l'ensemble du groupe ?
- Quand divulguerez-vous votre identité ? La divulguerez-vous lorsque vous entrerez pour la première fois dans le groupe, lorsque vous trouverez quelque chose d'utile dans le groupe que vous souhaitez inclure dans votre reportage, lorsque vous aurez terminé la collecte d'informations ou lorsque votre article sera publié ?
- Allez-vous également révéler les raisons pour lesquelles vous faites partie de ce groupe ?

- Si le groupe vous demande de répondre à certaines questions avant votre admission, y répondrez-vous honnêtement ?

CONSIDÉRATIONS SUPPLÉMENTAIRES

En outre, réfléchissez avant de vous lancer dans ce type de reportage :

- S'il existe des clauses de confidentialité explicites dans les lignes directrices communautaires des groupes.
- De quelle manière allez-vous décrire les méthodes de collecte des informations dans le reportage qui en résultera.
- Si vous prévoyez de retourner dans le groupe après la publication de votre article et de partager les informations que vous avez apprises.

Si vous utilisez votre véritable identité ou un pseudonyme, il est absolument essentiel de discuter avec vos rédacteurs en chef et de mettre en place des mesures de sécurité numérique, en particulier lorsque vous collectez des informations dans des communautés potentiellement hostiles. Les conseils de sécurité numérique du Comité pour la protection des journalistes[31] peuvent constituer un point de départ utile.

Pour un examen approfondi des questions éthiques liées à l'entrée dans des communautés non hostiles, nous recommandons l'article de MarkFrankel sur les promesses et les pièges d'un reportage dans les applications de chat et autres plateformes semi-ouvertes[32].

Conclusion

Les informations circulent dans l'obscurité. En 2020, nous nous attendons à ce que la majorité des désordres informationnels se produisent dans des espaces fermés et semi-fermés. À mesure que les capacités de veille se perfectionneront, ceux qui tenteront de diffuser de la désinformation migreront vers des espaces où leurs tactiques sont plus difficiles à trouver et à suivre.

La veille de ces espaces exigera beaucoup de travail et obligera les journalistes à passer du temps à localiser et à observer ces espaces. Il faudra également que l'ensemble du secteur débatte de l'éthique de ce type de tâches.

Les lignes de renseignements au public sont l'une des approches recommandées pour surveiller les espaces en ligne fermés. Cette méthode exige des rédactions qu'elles instaurent un climat de confiance avec leurs communautés, et plus particulièrement avec les publics qui sont plus susceptibles d'être ciblés par des campagnes coordonnées de désinformation et de suppression d'électeurs. Avant les élections, il est essentiel que les rédactions réfléchissent à des moyens de s'associer avec des groupes communautaires et de base, des groupes religieux et des bibliothèques, afin de suivre ce que ces communautés voient dans les publicités Facebook, les groupes Facebook, WhatsApp et les groupes de messagerie.

Tout comme les rédactions ont dû se préparer à l'ère des médias sociaux, où les conseils, les reportages et les sources sont soudainement devenus disponibles en temps réel, nous devons maintenant nous préparer à l'ère suivante, où les informations de mauvaise qualité - rumeurs, canulars et théories du complot - disparaitront hors-champ, loin de ceux qui peuvent les réfuter et les démystifier.

NOTES DE FIN

1. Wardle, C. & Derakshan, H. (2017, October). Information Disorder. An Interdisciplinary Framework for Research and Policy for the Council of Europe. Consulté sur https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c

2. Subramanian, S. (2017, February). Inside the Macedonian Fake-News Complex. Wired. Consulté sur https://www.wired.com/2017/02/veles-macedonia-fake-news/

3. Lapowsky, I. (2018, May). House Democrats Release 3,500 Russia-linked Facebook Ads. Wired. Consulté sur https://www.wired.com/story/house-democrats-release-3500-russia-linked-facebook-ads/

4. Bernstein, J. (2017, April). Never Mind the Russians, Meet The Bot King Who Helps Trump Win Twitter. BuzzFeed. Consulté sur https://www.buzzfeednews.com/article/josephbernstein/from-utah-with-love

5. Wingfield, N., Isaac, M. and Benner, K. (2016, November). Google and Facebook Take Aim at Fake News Sites. New York Times. Consulté sur https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html

6. Shukla, S. (2019, March). A Better Way to Learn About Ads on Facebook. Facebook Newsroom. Consulté sur https://newsroom.fb.com/news/2019/03/a-better-way-to-learn-about-ads/

7. Roth, Y. and Harvey, D. (2018, June). How Twitter is fighting spam and malicious automation. Twitter. Consulté sur https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html

8. How is Facebook addressing false news through third-party fact-checkers? Consulté le 30 octobre 2019. Consulté sur https://www.facebook.com/help/1952307158131536

9. Facebook Ad Library. Consulté le 30 octobre 2019. Consulté sur https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=GB&impression_search_field=has_impressions_lifetime

10. Mohan, M. (2017, May). Macron leaks: the anatomy of a hack. BBC. Consulté sur https://www.bbc.co.uk/news/blogs-trending-39845105

11. Conger, K. (2017, February). John Podesta talks email hack, fake news and Russia. TechCrunch. Consulté sur https://techcrunch.com /2017/02/08/john-podesta-talks-email-hack-fake-news-and-russia/

12. Watts, D. and Rothschild, D. (2017, December). Don't blame the election on fake news. Blame it on the media. Columbia Journalism Review. Consulté sur https://www.cjr.org/analysis/fake-news-media-election-trump.php

13. Shane, S. (2018, May). When Spies Hack Journalism. New York Times. Consulté sur https://www.nytimes.com/2018/05/12/sunday-review/when-spies-hack-journalism.html

14. Ellick, A. and Westbrook, A. (2018, November). Operation Infektion. New York Times. Consulté sur https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html

15. Lapowsky, I. (2019, March). Facebook's Pivot to Privacy is Missing Something Crucial. Wired. Consulté sur https://www.wired.com/story/facebook-zuckerberg-privacy-pivot/

16. Toxic Twitter—The Silencing Effect. Amnesty International. Consulté le 30 octobre 2019. Consulté sur https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-5/#topanchor

17. Priday, R. (2018, April). Fake news laws are threatening free speech on a global scale. Wired. Consulté sur https://www.wired.co.uk/article/malaysia-fake-news-law-uk-india-free-speech

18. Reuters Institute Digital News Report 2019. Consulté le 30 octobre 2019. Consulté sur http://www.digitalnewsreport.org/

19. Lytvynenko, J. (2019, August). The El Paso And Dayton Shootings Show How Disinformation Spreads On Messaging Apps. BuzzFeed. Consulté sur https://www.buzzfeednews.com/article/janelytvynenko/telegram-disinformation-fake-news

20. Facebook Ad Library API. Consulté le 31 octobre 2019. Consulté sur https://www.facebook.com/ads/library/api/?source=archive-landing-page

21. Methods—EU Ad Transparency Report. Consulté le 31 octobre 2019. Consulté sur https://adtransparency.mozilla.org/eu/methods/

22. Google Transparency Report. Consulté le 31 octobre 2019. Consulté sur https://transparencyreport.google.com/political-ads/region/US

23. Twitter. Prohibited Content Policies: Policitical Content. Consulté le 5 décembre 2019. Consulté sur https://business.twitter.com/en/help/ad-policies/prohibited-content-policies/political content.html

24. Dotto, C. and Smith, R. (2019). Guide essentiel de First Draft pour la collecte d'informations et la veille sur le Web social , Londres: First Draft. Consulté sur https://fr.firstdraftnews.org/wp-content/uploads/sites/3/2020/03/FD_NM_French.pdf?x80787

25. Garimella, K. and Tyson, G. (2018, April). WhatsApp, Doc? A First Look at WhatsApp Public Group Data. Cornwell University. Consulté sur https://arxiv.org/abs/1804.01473

26. Wadhwa, V. (2018, April). WhatsApp public groups can leave user data vulnerable to scraping. VentureBeat. Consulté sur https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/

27. Burgos, P. Conter, G. Dias, N. Pimenta, A. and Wardle, C. (2019, June). An Evaluation of the Impact of a Collaborative Journalism Project on Brazilian Journalists and Audiences. First Draft. Consulté sur https://firstdraftnews.org/wp-content/uploads/2019/07/comprova_ING_web_OK_v5.pdf?x19860

28. Storyful Team (2017, May). Online 'Alt-Right' Attempts to Influence France's Electorate. Storyful. Consulté sur https://storyful.com/blog/online-alt-right-wants-influence-frances-electorate-meme-wars-working/

29. Frankel, M. (2018, July). The promises and pitfalls of reporting within chat apps and other semi-open platforms: A journalist's guide. The Nieman Foundation for Journalism. Consulté sur https://www.niemanlaborg/2018/07/a-journalists-guide-to-the-promises-and-pitfalls-of-reporting-within-open-and-closed-and-semi-open-platforms/

30. Open Effect, The Citizen Lab and Crandall, J. (2017, November). Secure your Chats! Net Alert. Consulté sur https://netalert.me/encrypted-messaging.html

31. Barot, T. and Oren, E. (2015, November). Guide to Chat Apps. Tow Center for Digital Journalism. Columbia Journalism Review. Consulté sur https://www.cjr.org/tow_center_reports/guide_to_chat_apps.php

32. De Poloni, G. (2019, August). How Perth vegan Zoe Callis got caught in viral media storm after a Facebook post. ABC News. Consulté sur https://www.abc.net.au/news/2019-08-11/what-it-feels-like-to-be-caught-in-a-viral-media-storm/11385410?pfmredir=sm

33. Committee to Protect Journalists (2019, July). Digital safety kit. Consulté sur https://cpj.org/2019/07/digital-safety-kit-journalists.php

34. Frankel, M. (2018, July). The promises and pitfalls of reporting within chat apps and other semi-open platforms: A journalist's guide. The Nieman Foundation for Journalism. Consulté sur https://www.niemanlab.org/2018/07/a-journalists-guide-to-the-promises-and-pitfalls-of-reporting-within-open-and-closed-and-semi-open-platforms/

NOTES

NOTES

À PROPOS DE FIRST DRAFT

First Draft est une organisation internationale, à but non lucratif et non-partisane qui a pour but d'accompagner les journalistes sur le terrain. Nous proposons des conseils pratiques et des formations qui s'appuient sur des recherches continues. Nos compétences, outils et recommandations sont continuellement testés et révisés en collaboration avec des partenaires du monde entier.

FIRSTDRAFT

Avec le soutien de

Google News Initiative

@firstdraftnews

Pour en savoir plus, consultez le site firstdraftnews.org/resources