Note numéro 37
mars 2019

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Réseaux sociaux : paradoxes et convergence technologique

Par M. Philippe AUBERT-COUTURIER, en stage Master 2 au CREOGN

Synthèse d'une publication de M. Daniel GUINIER[1], Docteur ès sciences, expert en cybercriminalité et crimes financiers auprès de la Cour pénale internationale de La Haye

En 2018, Internet totalisait quelque 4,2 milliards d'internautes (soit 55 % de la population mondiale) dont 3,4 milliards étaient des utilisateurs de réseaux sociaux (*Facebook*, *Twitter*, *LinkedIn*, *Whatsapp*, etc.) Parallèlement au poids croissant qu'ils prennent, les réseaux sociaux présentent de multiples facettes : espace de partage et d'échanges, ils s'avèrent être également des lieux d'influence voire de manipulation. De nouvelles formes de menaces et de vulnérabilités y sont ainsi apparues, notamment en lien avec la manipulation de l'opinion publique. Le recours aux *bots*[2] et aux *trolls*[3] a, en outre, permis d'industrialiser le partage de fausses informations.

1. Les multiples enjeux des réseaux sociaux

Un vecteur d'échanges sujet à de nombreuses dérives

Les réseaux sociaux se sont progressivement affirmés comme un lieu d'échange de connaissances et d'informations. À la frontière entre vie privée et vie publique, la loi s'y applique dans le respect des droits de chacun et ce, malgré le sentiment d'impunité qui peut parfois y prévaloir.

La prudence s'impose toutefois sur les réseaux sociaux, qui sont régulièrement utilisés à des fins de manipulation ou de discréditation. Toute information diffusée peut ainsi être instantanément vue, utilisée et retransmise, y compris par des personnes qui n'en étaient pas nécessairement les destinataires premiers. Cette instantanéité explique le phénomène croissant de propagation de rumeurs ou de fausses informations (*fake news*). Il est donc plus que jamais nécessaire de mesurer le risque inhérent aux réseaux sociaux afin de mieux les utiliser.

Un espace de construction et de vulnérabilités pour les internautes

Les réseaux sociaux ont contribué à démocratiser l'accès à l'expression publique auprès de populations qui n'y avaient auparavant pas accès. Les utilisateurs s'en servent aujourd'hui pour révéler de nombreuses

1 GUINIER, Daniel. Réseaux sociaux, paradoxes et convergence technologique. *Expertises*, n° 444, mars 2019.

2 Un « *bot* » est un logiciel informatique opérant de manière autonome, dont la principale mission consiste à effectuer des tâches de façon répétée. Abonnements automatisés, robots conversationnels et interactifs (*chatbot*), etc., le bot s'appuie sur des bases de données pour répondre aux demandes de l'internaute.

3 Les « *trolls* » sont des comptes d'internautes qui déclenchent volontairement des polémiques sur les sites de réseaux sociaux, les forums de discussion ou les blogs, dans le but de provoquer ou de générer des réactions en retour, à travers des contributions excessives, injurieuses ou de nature publicitaire.

informations sur eux-mêmes, mais également sur d'autres personnes. Chaque internaute construit ainsi sur les réseaux sociaux sa propre image, sous la forme d'un portrait numérique qu'il tend à valoriser comme il le souhaite.

Cette propension des utilisateurs à se dévoiler sur les réseaux sociaux est parfois en décalage avec la proximité qu'ils entretiennent avec les autres utilisateurs et qui n'est pas toujours maîtrisée. Nombreux sont ceux qui se montrent peu soucieux de la confidentialité des informations qu'ils publient ainsi que des paramétrages d'accès à leurs comptes et publications. De même, les informations sont régulièrement traitées trop légèrement et sont perçues et retransmises sans véritable contrôle de leur validité. En outre, beaucoup d'informations sont reprises de réseaux sociaux en réseaux sociaux, passant par exemple de *Facebook* à *Twitter,* ce qui amplifie leur portée.

Les enjeux du numérique pour les entreprises

Les réseaux sociaux constituent pour les entreprises une sphère récente de communication et d'influence. Les formes d'échanges qu'ils induisent ont progressivement fait émerger l'enjeu de l'influence numérique. La nécessité de s'engager activement dans les médias sociaux est aujourd'hui pour les entreprises le gage d'un jeu à armes égales avec la concurrence. À l'inverse, dédaigner la sphère numérique équivaut d'une certaine façon à céder aux adversaires une part non négligeable de notoriété et de réputation.

Cela est d'autant plus lourd de conséquences que l'immédiateté de la diffusion des informations rend plus que jamais nécessaire une veille, afin d'assurer à l'entreprise une réaction rapide et adaptée, dans un contexte croissant d'atteinte à la réputation. De fait, cette dernière est aujourd'hui perçue comme un risque majeur[4], au regard des larges possibilités d'audience apportées par Internet. Une bonne – ou une mauvaise – réputation peut ainsi se répandre auprès de centaines de millions de personnes, dans un délai très court.

Les entreprises tentent donc de contrôler leur identité numérique à travers leur représentation sur les réseaux sociaux, sans toutefois pouvoir garantir une maîtrise totale de leur e-réputation qui peut être mise à mal par certains grands influenceurs. De fait, les réseaux sociaux ont vu l'émergence de nouvelles formes de vulnérabilités et de menaces pour les différents acteurs qui y évoluent.

2. Nouvelles menaces et vulnérabilités

L'écosystème d'influence en ligne

L'écosystème d'influence en ligne se compose de plusieurs sphères qui se superposent et sont partagées entre internautes humains et robots. Au sein de cet écosystème, certains grands influenceurs se démarquent : experts de renom, personnalités médiatiques, groupes militants, etc. Ces « gourous » modernes sont suivis par une foule de « disciples » qui leur font écho en relayant leurs messages.

Le système de modération des réseaux sociaux, fondé sur des algorithmes, offre de nouvelles possibilités à ces influenceurs, qu'ils soient humains ou robotisés.

Un système algorithmique complexe

La modération des réseaux sociaux relève essentiellement d'algorithmes dont l'action sur la notoriété et donc l'influence des contenus est déterminante, à l'exemple de *Twitter* qui affiche en priorité les *tweets* jugés les plus pertinents. Cette sélection algorithmique a des conséquences immédiatement visibles : augmentation du nombre de vues, de *likes*, de *retweets*, etc.

Plusieurs interrogations se posent quant au fonctionnement de ces algorithmes : premièrement, sur quels critères opérer la sélection entre ce qui est pertinent et ce qui ne l'est pas ? De même, sur quels fondements décider de la suppression d'un contenu ou de la suspension d'un compte ? Un premier enjeu réside ainsi dans

4 Rapport Aon 2017 et étude Deloitte.

la qualification juridique du contenu. Une deuxième difficulté concerne la capacité à réagir et à traiter l'énorme flux de données. À ce titre, ce sont près de 10 millions de *tweets* qui sont publiés chaque minute à travers le monde. Enfin, un autre enjeu majeur réside dans la vulnérabilité des algorithmes face à de possibles attaques, qu'il s'agisse de contournements ou des modifications malveillantes. De plus, cette menace est accentuée par la possibilité d'erreurs dues à la complexité des algorithmes[5].

De nouvelles vulnérabilités : *bots* et *trolls*

Le développement des réseaux sociaux a ainsi sa part d'ombre. Leur essor a permis de nouvelles formes de manipulations, notamment à travers la propagation mondiale d'informations fausses ou trompeuses, que l'usage des *trolls* et des *bots* est venu amplifier. Les *trolls*, comptes de réseaux sociaux créés par des humains, constituent en effet un vecteur majeur de propagation de contenus orientés. Leur usage vise aujourd'hui essentiellement à créer des polémiques autour de sujets ciblés. De façon similaire, les *bots* sociaux sont des programmes destinés à tromper les internautes en simulant le comportement humain, à travers des interactions automatisées sur les réseaux sociaux. En se faisant passer pour de véritables personnes, ils sont capables d'infiltrer les réseaux sociaux et d'acquérir la confiance des utilisateurs, à des fins parfois malveillantes. Ils sont par ailleurs appuyés par des *bots* classiques, liés, quant à eux, à une machine et permettant d'amplifier la viralité des informations ciblées. *Bots* et *trolls* constituent des relais de diffusion majeurs pour certains influenceurs, en faisant office de véritables caisses de résonance auprès des utilisateurs de réseaux sociaux. Les profils impactés se comptent ainsi par millions.

Le cas de la campagne présidentielle française de 2017

Ces opérations de désinformation se sont illustrées à grande échelle au cours de la campagne présidentielle française de 2017. E. Ferrara a ainsi mis en lumière une vaste opération de manipulation de l'opinion publique[6], en analysant 17 millions de *tweets* relatifs à la période électorale, postés entre le 27 avril et le 7 mai 2017. Au total, ce sont quelque 18 324 *bots* sociaux qui auraient participé à cette campagne de désinformation visant notamment le candidat Emmanuel Macron, avec un pic de *tweets* attribués à des *bots* le 7 mai 2017, date des élections. Il est toutefois démontré que ces cascades de désinformations sont d'abord attribuées à des *tweets* humains, qui sont par la suite amplifiés par un phénomène de résonance.

Cette nouvelle menace que peuvent représenter *bots* et *trolls* prend aujourd'hui une ampleur particulière, dynamisée par les nouvelles opportunités offertes par la convergence technologique.

3. Les possibilités induites par la convergence technologique

Un perfectionnement des outils d'information

La convergence technologique, initialement limitée aux technologies de l'informatique, désigne aujourd'hui plus largement l'intégration de plusieurs appareils, services et réseaux au sein d'un système ou d'un appareil unique. Phénomène omniprésent, il s'agit ainsi de combiner les technologies de plusieurs domaines tels que le multimédia ou les télécommunications.

En matière informatique, les progrès de l'intelligence artificielle ont permis un développement poussé des *bots*, leur permettant de simuler plus que jamais de véritables internautes, pour les rendre indétectables. Cette manipulation est accentuée par le mélange des fausses informations avec des contenus exacts et vérifiables. Ces stratégies d'influence prennent la forme de véritables opérations de déstabilisation, visant les fondements mêmes de la démocratie[7].

5 GUINIER, David. Sur la place des algorithmes et les exigences face à la complexité. *Revue Experts,* n° 139, juillet 2018, p. 40-44.
6 FERRARA, Emilio. *Disinformation and social bot operations in the run up to the 2017 French presidential election*, University of Southern California, Information Sciences Institute, Vol. 22, n° 8.
7 JEANGÈNE-VILMER, Jean-Baptiste, ESCORCIA, Alexandre, GUILLAUME, Marine, HERRERA, Janaina. *Les manipulations de l'information : un défi pour nos démocraties.* Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM), août 2018, p. 210.

Les limites de la convergence technologique

Ces progrès sont toutefois à relativiser, comme en témoigne l'expérience *Tay* menée par Microsoft en mars 2018. Robot conversationnel (*chatbot*) doté d'une intelligence artificielle, *Tay* a pris le profil d'une adolescente pour dialoguer sur les réseaux sociaux, en fondant ses propos sur des réponses pré-rédigées ou sur des bases de données publiques. L'expérience a rapidement pris de l'ampleur, *Tay* ayant séduit 23 000 abonnés en moins d'une journée, grâce à l'envoi de quelque 100 000 *tweets*. Des limites aux capacités d'apprentissage et d'échanges du *chatbot* sont cependant vite apparues, après que le robot a tenu des propos inappropriés ou racistes, *Tay* ayant par ailleurs rapidement été la cible d'insultes et de remarques sexistes. Microsoft a donc finalement mis fin à cette expérience.

Quelle réponse des acteurs du numérique ?

En opposition avec la vocation première des réseaux sociaux comme lieu de partage de connaissances, la convergence technologique, en combinant Internet, réseaux sociaux, *bots*, intelligence artificielle et *big data*, est amenée à représenter un atout croissant pour les opérations de déstabilisation ou de manipulation de l'opinion publique. L'enjeu pour les plateformes de réseaux sociaux sera de conserver une éthique rigoureuse garante de la bonne utilisation des réseaux sociaux, sous le contrôle des États et des institutions. Ces derniers ont pu mesurer l'ampleur des risques de manipulation, les amenant à renforcer la concertation entre les différents acteurs concernés : pouvoirs publics, opérateurs, utilisateurs de réseaux sociaux, etc. Une évolution de la législation mérite également un examen approfondi, afin de trancher la question de l'équilibre entre liberté d'expression et contrôle de l'authenticité et de la véracité des propos mis en ligne sur les réseaux sociaux. Il s'agit ainsi de répondre définitivement aux récurrentes accusations de remise en cause des libertés publiques sur le Net, notamment en matière de liberté d'expression. À ce titre, un regard particulier est à porter sur la loi 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information[8], notamment à l'occasion du processus électoral européen.

Conclusion

Les réseaux sociaux constituent une seule réalité, mais perçue sous plusieurs angles différents, selon la nature des acteurs concernés : internautes, entreprises, opérateurs de réseaux sociaux, etc. De fait, l'écosystème d'influence en ligne révèle des intérêts divergents entre ces différents acteurs, constitués d'êtres humains mais également « d'entités algorithmiques », aux capacités d'action croissante et auxquels la convergence technologique a conféré de nouvelles possibilités. Les réseaux sociaux ont donc une nature paradoxale à prendre en compte afin d'éviter certaines dérives, dont l'une des manifestations sont les opérations de manipulation de l'opinion publique. *Fake news* et messages provocateurs constituent en effet une sérieuse menace pour l'ensemble des acteurs du web, qu'il convient d'appréhender et de réguler, que ce soit au moyen d'outils juridiques ou à travers un processus de coopération global.

8 Général d'armée (2s) WATIN-AUGOUARD, Marc. La loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. *Note du CREOGN* [en ligne], n° 36, janvier 2019. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/La-loi-n-2018-1202-du-22-decembre-2018-relative-a-la-lutte-contre-la-manipulation-de-l-information