

En pratique, nous avons estimé en 2017 que près de 15% des comptes Twitter actifs étaient des bots, et qu'ils avaient joué un rôle clé dans la diffusion de la désinformation durant la campagne présidentielle américaine de 2016. Dans les secondes qui suivaient la publication d'une fausse nouvelle – par exemple l'implication d'Hillary Clinton dans des rituels occultes –, cette «information» était retweetée par de nombreux bots, puis par des humains, séduits par l'apparente popularité du tweet.

Il suffit à un bot de suivre un compte, de cliquer sur des boutons «J'aime» ou de retweeter des posts pour infiltrer une communauté en ligne et influencer ses membres. Dans un modèle conçu à l'OSoMe, les agents sont des bots qui produisent des posts de qualité médiocre, de type «pièges à clics», et ne se retweetent que les uns les autres. Le modèle prend aussi en compte des agents authentiques, susceptibles de suivre ces bots.

Nous avons montré qu'en infiltrant seulement une petite fraction du réseau, ces bots peuvent réduire à néant la qualité de l'information du réseau entier. En suggérant aux agents authentiques de suivre d'autres comptes automatisés (technique dite de «follow trains»), ils accélèrent également la formation de chambres d'écho.

Certains manipulateurs agissent dans deux camps opposés, à des fins de polarisation politique ou pour gagner de l'argent. Nous avons ainsi démasqué un réseau de faux profils sur Twitter, tous coordonnés par une même entité. Certains affichaient leur soutien à la campagne en faveur de Donald Trump, tandis que d'autres se posaient en anti-Trump. Tous faisaient appel aux dons...

FREINER LA MANIPULATION EN LIGNE

En comprenant mieux nos biais cognitifs et la façon dont les bots les exploitent, nous pouvons nous protéger des manipulations. Notre laboratoire a mis au point des outils pour ce faire, par exemple Fakey, une application dont l'objectif est d'apprendre à repérer les fausses informations. Il s'agit d'un jeu qui simule le fil d'actualité d'un réseau social, affichant des articles réels issus de sources plus ou moins fiables. Les utilisateurs doivent décider lesquels vérifier, partager, etc. Notre analyse des données de Fakey confirme le comportement grégaire des utilisateurs: peu importe la crédibilité des informations, ils partagent plus facilement celles qu'ils croient largement diffusées.

Un autre outil, Hoaxy, également public, montre comment un post se répand sur Twitter. Les nœuds représentent des comptes Twitter réels et les arêtes qui les connectent indiquent la propagation du tweet de compte en compte. Chaque nœud a une couleur représentative du score qu'il a obtenu à Botometer, ce qui permet

BIBLIOGRAPHIE

G. Bronner, **Apocalypse cognitive**, PUF, 2021.

H. Y. Yan et al., **Asymmetrical perceptions of partisan political bots**, *New Media & Society*, publié en ligne le 16 juillet 2020.

N. Grinberg et al., **Fake news on Twitter during the 2016 U.S. presidential election**, *Science*, vol. 363, pp. 374-378, 2019.

D. Robert et al., **Bad news has wings: dread risk mediates social amplification in risk communication**, *Risk Analysis*, vol. 38, pp. 2193-2207, 2018.

X. Qiu et al., **Limited individual attention and online virality of low-quality information**, *Nature Human Behaviour*, vol. 1, article 0132, 2017.

B. Mønsted et al., **Evidence of complex contagion of information in social media: an experiment using Twitter bots**, *Plos One*, vol. 12(9), article e0184148, 2017.

aux utilisateurs de vérifier si des bots interviennent dans la diffusion. Des journalistes ont déjà utilisé ces outils pour rechercher les origines de campagnes de désinformation et repérer des opérations menées par des bots, comme celle visant à dissuader des électeurs de voter lors des élections de mi-mandat de 2018 aux États-Unis. Cependant, les manipulations sont de plus en plus difficiles à détecter, car les algorithmes deviennent très performants dans leur imitation du comportement humain.

Pour repérer des campagnes de désinformation lancées, par exemple, pour détourner l'attention du public, nous avons développé un outil appelé BotSlayer. Il suit les tweets, extrait des hashtags, évalue la probabilité des comptes d'être de faux profils, afin de signaler des thèmes qui se diffusent rapidement suspectés d'être amplifiés par des bots ou des comptes coordonnés. L'objectif est de permettre aux journalistes, aux associations et aux candidats politiques de repérer et de suivre en temps réel les campagnes d'influence insidieuse.

Ces outils sont utiles mais restent insuffisants pour limiter la prolifération de fausses nouvelles. L'éducation est certes un atout, mais elle ne peut aborder tous les sujets sur lesquels les gens sont susceptibles d'être bernés. Certains gouvernements et médias sociaux veulent agir pour réprimer la désinformation en ligne. Mais qui établit ce qui est faux, manipulateur et ce qui ne l'est pas? On pourrait accompagner certaines publications de messages d'avertissements, comme Facebook et Twitter ont commencé à le faire. Mais peut-on faire confiance aux personnes qui les émettent? En outre, le risque de nuire à la liberté d'expression existe. La portée mondiale de certains médias sociaux et leurs liens avec les gouvernements compliquent encore les choses.

Pour combattre la désinformation, une solution serait de rendre la création et le partage de l'information plus difficiles. Pour cela, il faudrait que l'accès à l'information ait un coût, par exemple en temps, en travail mental (faire un puzzle) ou en argent (en facturant des frais minimes). Certaines plateformes utilisent déjà les captchas ou la confirmation téléphonique comme sésames pour accéder aux comptes. Ces efforts pourraient être étendus afin de remplacer les incitations au partage à tout-va par des informations véritablement enrichissantes.

L'information prétendue gratuite ne l'est jamais réellement. En diminuant son coût, nous avons diminué sa valeur et ouvert la porte à sa falsification. Pour restaurer la santé de notre écosystème de l'information, nous devons restaurer une économie de l'information saine, qui nous protège des manipulations. ■

QUELQUES OUTILS

Modèle EchoDemo :
<https://osome.iuni.iu.edu/demos/echo>

Botometer :
<https://botometer.osome.iu.edu>

Fakey :
<https://fakey.iuni.iu.edu>

Hoaxy :
<https://hoaxy.osome.iu.edu>

BotSlayer :
<https://osome.iuni.iu.edu/tools/botslayer>