Social Bots

Ils ont fait parler d'eux pendant la campagne présidentielle aux États-Unis : les "social bots", ou "robots sociaux" en français, ainsi que les fausses informations, auraient influencé l'élection. Mais que se cache-t-il exactement derrière ces programmes que l'on retrouve sur les réseaux sociaux ? Ce dossier donne un aperçu de l'univers des bots et tente d'évaluer la situation.

Qu'est-ce que les social bots ?

Le terme "bot" est une abréviation de "robot". De manière générale, les bots sont des programmes qui exécutent automatiquement des tâches répétitives, sans intervention humaine. On utilise aussi souvent le terme de "botnets" lorsque l'on parle d'ordinateurs infectés de malware, qui sont par exemple utilisés pour envoyer des spams. Il n'existe pas de définition exacte pour désigner un programme de "bot" – il s'agit ici de conventions linguistiques qui se sont instaurées avec le temps. Les social bots sont des bots actifs sur les réseaux sociaux. Le phénomène touche particulièrement le réseau social de microblogage Twitter. En effet, ses caractéristiques techniques et l'ouverture des interfaces de programmation (API) permettent de mettre en place assez facilement des bots. Aussi, du fait qu'il n'existe qu'un seul type de compte et que la longueur des messages est limitée à 140 caractères, Twitter se prête idéalement aux bots - en effet, d'un point de vue technique, créer un profil Facebook entièrement automatisé est beaucoup plus complexe, tandis que pour Twitter, des connaissances de base en programmation suffisent. On estime que 7 pourcent de tous les comptes Twitter sont des bots - bien que l'estimation se révèle particulièrement difficile. Fin janvier 2017, des scientifiques de University College London ont découvert un botnet composé de plus de 350 000 comptes qui tweetaient tous des citations de films "Star Wars" à une fréquence inhabituelle. Ce botnet semble actuellement être en veille, mais, en théorie, il pourrait être réactivé à tout moment par ses créateurs. Sur Facebook Messenger, certaines sociétés proposent déjà des chatbots qui s'occupent d'un service clients rudimentaire, par exemple pour informer les clients sur le retard d'un vol. Des projets similaires existent sur WhatsApp. Le service de messagerie Telegram propose une interface de programmation pour les bots.

Sur les réseaux sociaux, le comportement des bots ressemble souvent à celui des êtres humains. Ainsi, le risque de confusion est très grand et il n'est pas toujours facile de savoir si l'interlocuteur est une personne ou une machine. Comme le développement dans le secteur de l'intelligence artificielle ne cesse de progresser, nous verrons à l'avenir encore plus de bots, notamment dans le secteur des services (p.ex. messagerie de support).

Les bots sont-ils dangereux ?

La plupart des bots connus ne sont pas dangereux – ceux qui proposent des services sur Facebook Messenger ou d'autres réseaux sociaux sont notamment clairement identifiés en tant que bots. Ainsi, impossible de les confondre avec des êtres humains. Sur Twitter aussi, il existe de nombreux bots qui sont identifiables en tant que tels à première vue. Cependant, ces petits projets de programmation n'ont souvent aucun intérêt et agacent la plupart des utilisateurs : il existe par exemple des bots Twitter qui sont à l'affût des fautes d'orthographe et qui font ensuite la leçon aux auteurs des tweets. D'autres bots Twitter sont plutôt des projets artistiques et génèrent d'une liste préétablie d'éléments de structure de phrase des petites histoires sous forme de tweets d'une phrase. D'autres programmes retweetent des tweets qui contiennent certains termes - reste à savoir si de tels comptes ont vraiment une utilité pratique.

Bien évidemment, il existe également de nombreux bots aux objectifs douteux : des comptes créés en masse, qui semblent authentiques à première vue, peuvent être achetés en tant que followers. Les bots sont également utilisés à des fins publicitaires, souvent de manière cachée et sans être identifiés en tant que tels. Un exemple bien connu est le compte d'une jeune femme séduisante qui s'intéresse à un sujet bien précis (p.ex. camping) et qui tweete et retweete uniquement sur ce sujet. On simule de cette manière un intérêt et un savoir d'expert "humains" pour un sujet. Lorsque le compte a un certain nombre de followers, des liens vers des boutiques en ligne sont utilisés pour faire dépenser les utilisateurs. Bien que de tels bots ne soient pas dangereux en soi, ils dupent et trompent toutefois les utilisateurs non experts, puisqu'il ne s'agit pas d'une recommandation humaine, mais d'une publicité qui n'est pas identifiée en tant que telle.

Le type de bots qui a suscité beaucoup l'attention ces derniers temps est celui qui tente d'exercer une influence politique et auquel l'on reproche de manipuler les résultats d'élections. Nous allons d'ailleurs nous intéresser de plus près à ce type de bots dans les lignes qui suivent.

Influence politique

Il existe différentes méthodes pour utiliser les social bots à des fins politiques. D'une part, les bots permettent assez facilement d'augmenter le nombre de followers ou de J'aime d'un compte. Utilisés en masse, les bots qui aiment chaque tweet d'un candidat et le retweetent assurent des chiffres impressionnants. D'autre part, il est possible de faire réagir les bots à certains mots-clés. Les contestataires du réchauffement climatique aux États-Unis, par exemple, ont programmé un bot qui a réagi aux tweets sur le changement climatique. Il se peut que quelques utilisateurs se laissent convaincre par une seule phrase suivie d'un lien vers un article. Contrairement aux bots, les êtres humains se fatiguent, sont incapables d'écrire en même temps à des centaines d'utilisateurs et ne peuvent pas passer tout leur temps sur les réseaux sociaux. Aussi, impossible pour l'opposition de convaincre les bots, qui, comparés à d'autres formes publicitaires, sont très bon marché - la tentation de les utiliser pendant une campagne électorale est donc très grande.

Il ne faut toutefois pas surestimer les possibilités des social bots : il est très facile de programmer un bot qui réagit à certains mots-clés ou comptes et aime, retweete ou écrit automatiquement une réponse (prédéfinie). Les bots capables de mener

des discussions politiques exigent un niveau de développement très élevé et sont donc coûteux. Ainsi, la plupart du temps, on utilise des bots "bêtes" pour manipuler les tendances sur Twitter. A une époque où chaque tweet d'une personne politique est considéré comme un message potentiel, il va de soi que les journalistes scrutent Twitter de très près. Les social bots ont donc le potentiel de manipuler la situation médiatique et générer de gros titres, lorsque les journalistes écrivent sur l'ambiance prétendue sur Twitter. Bien évidemment, les bots se prêtent également idéalement à diffuser des fausses informations sur Internet.

États-Unis

Pendant l'élection présidentielle aux États-Unis, les Républicains et les Démocrates ont utilisé des bots sur Twitter pour mettre un coup de projecteur sur leur candidat(e). Après le premier débat télévisé entre Hillary Clinton et Donald Trump, l'université d'Oxford a examiné les tweets publiés sur cet événement. L'université a conclu - avec surprise - que plus d'un tiers des tweets en faveur de Trump étaient émis par des bots. Chez Clinton, le taux de bots était d'environ 22 pourcent. Ces bots donnent l'impression qu'il existe beaucoup d'activistes qui tweetent pour soutenir leurs candidats, capables de manipuler les tendances sur Twitter en utilisant de manière ciblée des hashtags précis. Bien que les deux partis aient utilisé des social bots comme publicité, il est fort probable que Trump doit son succès électoral à l'utilisation de bots.

Brexit

Le référendum sur le maintien du Royaume-Uni dans l'Union européenne était un sujet vivement débattu sur Twitter où les bots ont également joué un rôle important. Du moins lorsque l'on regarde le nombre de tweets. L'université d'Oxford a examiné 1,5 millions de tweets en rapport avec le Brexit et a constaté qu'un tiers - donc un demi-million - de ces tweets ont été écrits de moins d'un pourcent de tous les comptes. Aucun être humain peut rédiger autant de tweets, rien que le nombre élevé de tweets fait supposer une certaine automatisation. Les deux comptes les plus actifs étaient également des bots. Malheureusement, on ignore la réparation exacte des bots concernant les partisans et les opposants du Brexit.

Allemagne

Après l'élection présidentielle aux États-Unis, plusieurs personnes politiques en Allemagne ont exprimé leur inquiétude concernant les social bots, la chancelière Angela Merkel proposait même que tous les partis devraient se mettre d'accord sur le fait de ne pas utiliser de social bots pendant la prochaine campagne électorale. Le projet "botswatch" examine les activités de bots lors d'événements politiques en Allemagne, par exemple pendant les émissions de débats télévisées. Il s'est avéré qu'il existe déjà des social bots en langue allemande, dont certains font dix pourcent des comptes concernés.

Luxembourg

Au Luxembourg, il n'existe encore aucun rapport sur les social bots. Rien d'étonnant, car le nombre des utilisateurs actifs de Twitter est relativement faible au Grand-Duché. Mis à part quelques journalistes et personnes politiques, rares sont les personnes qui utilisent régulièrement le réseau social de microblogage. Il ne serait donc actuellement pas très intéressant d'utiliser des social bots comme mesure de campagne électorale. Puisque l'utilisation de bots sur Facebook est beaucoup plus complexe, la campagne électorale se fera encore, pour le moment, de manière manuelle sur ce réseau social. Au vu du succès de Trump et co., des personnes politiques luxembourgeoises pourraient toutefois aussi prendre goût à Twitter - les social bots seraient donc l'étape suivante.

Dangers

Les dangers des social bots, utilisés pour exercer une influence politique, sont bien évidemment la manipulation d'électeurs potentiels. Nous devons toutefois ne pas oublier que les moyens traditionnels d'une campagne électorale, à savoir les affiches, les flyers, les spots publicitaires, les goodies, sont également une forme de "manipulation". Nous nous sommes tout simplement habitués à voir de la publicité politique pendant les campagnes électorales et nous avons appris à les gérer. Le danger des social bots consiste notamment à ce que nous considérons ces comptes comme des comptes gérés par des personnes et à ce que nous évaluions mal la diffusion de points de vue. Une situation particulièrement dangereuse lorsqu'il s'agit de hate speech (discours haineux), car nous avons moins de scrupules lorsque nous avons le sentiment que "tous" pensent de la sorte. Les social bots restent pour le moment relativement rudimentaires – si les programmes évoluent et s'il devient possible de discuter avec des utilisateurs comme le feraient deux personnes, le danger quant à l'influence peut être beaucoup plus grand.

De la même manière dont nous avons développé la compétence médiatique pour les publicités électorales traditionnelles, nous devons désormais également apprendre pour les social bots à les reconnaître et à gérer les informations qu'ils diffusent.

Comment reconnaître les social bots ?

De manière générale, une analyse critique de chaque compte Twitter permet d'évaluer les informations publiées par le compte en question. Les étapes suivantes sont non seulement pratiques lorsque l'on pense avoir à faire à un social bot, elles permettent aussi d'évaluer le sérieux d'un compte Twitter de manière générale.

1. Le compte est-il fiable ?

Lisez quelques tweets du compte et jugez-les : s'agit-il de positions extrêmes, peut-on y lire un certain jargon, s'agit-il d'un discours haineux ? Regardez également si vous connaissez des followers de ce compte - bien qu'il n'existe aucune sécurité à cent pourcent, cela vous donne tout de même un indice.

2. Quel est le profil ?

Les bots ont souvent pas d'avatar ou utilisent une photo de profil volée sur Internet – un moteur de recherche d'images permet de savoir où l'image est également utilisée. La description de profil peut aussi donner des indices à la question de savoir si le compte est authentique ou s'il s'agit d'une machine. Les bots indiquent des lieux choisis au hasard dans leur profil - cela aussi peut être un indice !

3. Quelle est l'activité du compte ?

Les bots sont souvent très actifs et publient de nombreux tweets par jour, pour des projets comme "botswatch", il s'agit de 50 tweets minimum par jour. Il existe bien sûr aussi des personnes qui sont très actives sur les réseaux sociaux, mais elles sont l'exception. Si le compte n'est pas très vieux et présente un grand nombre de tweets, cela peut être un indice qu'il s'agit d'un bot. Les bots ont également souvent un nombre élevé de retweets et de J'aime, qui sont tous les deux vérifiables.

4. Comment le compte écrit-il ?

Les comptes qui ne font que retweeter sont très vraisemblablement des bots. Cependant, c'est souvent leur style linguistique qui trahit les bots - la grammaire laisse à désirer ? les mêmes termes et tournures de phrase reviennent constamment ? et le compte répond-il très vite ? Il s'agit alors très probablement d'un bot !

Outre votre intuition, il existe désormais également des services que vous pouvez utiliser pour reconnaître des bots : le projet Bot or Not? de l'université d'Indiana examine plusieurs facteurs d'un compte Twitter et tente d'évaluer si le compte est un bot ou un être humain. Bien sûr, cette évaluation n'est pas toujours très précise (Donald Trump serait p.ex. à 52 pourcent un bot), mais elle peut donner un premier indice.

Conclusion

Les dangers et le degré d'influence des social bots ne devraient pas être surestimés. La responsabilité incombe aux exploitants des réseaux sociaux - ils devraient exclure les faux comptes ou les comptes qui font miroiter de fausses informations. Malheureusement, tous les réseaux sociaux, de part leurs modèles commerciaux, ont un grand intérêt à obtenir un grand nombre d'utilisateurs, ce qui va à l'encontre de la lutte contre les faux comptes. Les possibilités politiques d'intervenir en imposant une réglementation sont plutôt faibles et les experts considèrent de tels projets comme une atteinte à la liberté d'expression. Kevin Munger de l'Université de New York a eu une idée intéressante. Le chercheur a développé quatre bots qui faisaient remarquer aux utilisateurs qu'ils utilisaient un langage raciste. Conséquence : les commentaires racistes reculaient de 27 pourcent par jour. Cependant, on peut se demander combien de personnes sont prêtes à se faire réprimander par un bot - et s'interroger sur l'éthique de l'utilisation, lorsque les bots "bienveillants" prétendent être des personnes.

Si vous ne souhaitez pas être manipulé par des social bots, essayez de les démasquer, faites preuve de bon sens et vérifiez les informations et leurs sources.

Sources :

- Heinrich Böll Stiftung sur les social bots : https://www.boell.de/de/2017/02/09/social-bots
- Botswatch : http://botswatch.de/
- Blog du WDR sur les social bots pendant l'élection présidentielle aux États-Unis : https://blog.wdr.de/digitalistan/usa-wahlkampf-mit-propaganda-bots-gefaehrdet-demokratie/
- The Rise of social bots : http://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext
- Forbes : Do evil – The Business of social media bots: http://www.forbes.com/sites/lutzfinger/2015/02/17/do-evil-the-business-of-social-media-bots/#6080c2b91104
- tagesschau : seule l'AfD veut utiliser des "robots d'opinion" : https://www.tagesschau.de/inland/social-bots-afd-101.html
- Bots Brexit : https://qz.com/713980/watch-out-for-the-brexit-bots/
- Bot or Not? http://truthy.indiana.edu/botornot/
- Botnet Star Wars : https://www.heise.de/newsticker/meldung/Forscher-entdecken-riesiges-Twitter-Botnetz-Star-Wars-3604196.html
- Bots Facebook Messenger : https://blog.hubspot.com/marketing/facebook-bots-guide
- Bots "bienveillants" : https://www.heise.de/tr/blog/artikel/Die-guten-Chatbots-3492352.html

Pour toute question au sujet de l'arnaque en ligne ou sur l'utilisation d'Internet en général, contactez la BEE SECURE Helpline:

BEE SECURE HELPLINE CONSEIL
Tél: 8002 1234

Editeur: BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.lu www.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union Connecting Europe Facility