La nouvelle dystopie, c'est maintenant

L'article qui suit n'est pas une traduction intégrale mais un survol aussi fidèle que possible de la conférence TED effectuée par la sociologue des technologies Zeynep Tufecki. Cette conférence intitulée : « Nous créons une dystopie simplement pour obliger les gens à cliquer sur des publicités »
(We're building a dystopia just to make people click on ads) ~~est en cours de traduction sur la plateforme Amara préconisée par TED, mais la révision n'étant pas effectuée, il faudra patienter pour en découvrir l'intégralité sous-titrée en français.~~ est maintenant traduite en français \o/

En attendant, voici 4 minutes de lecture qui s'achèvent hélas sur des perspectives assez vagues ou plutôt un peu vastes : il faut tout changer. Du côté de Framasoft, nous proposons de commencer par outiller la société de contribution avec la campagne Contributopia… car dégoogliser ne suffira pas !

Mettez un peu à jour vos contre-modèles, demande Zeynep : oubliez les références aux menaces de Terminator et du 1984 d'Orwell, ces dystopies ne sont pas adaptées à notre débutant XXI^{e} siècle.

Cliquez sur l'image pour afficher la vidéo sur le site de TED (vous pourrez afficher les sous-titres via un bouton en bas de la vidéo)

Ce qui est à craindre aujourd'hui, car c'est *déjà là*, c'est plutôt comment ceux qui détiennent le pouvoir utilisent et vont utiliser l'intelligence artificielle pour exercer sur nous des formes de contrôle nouvelles et malheureusement peu détectables. Les technologies qui menacent notre liberté et notre jardin secret (celui de notre bulle d'intimité absolue) sont développées par des entreprises-léviathans qui le font d'abord pour vendre nos données et notre attention aux GAFAM (Tristan Nitot, dans sa veille attentive, signale qu'on les appelle les *frightful five,* les 5 qui font peur, aux États-Unis). Zeynep ajoute d'ailleurs Alibaba et Tencent. D'autres à venir sont sur les rangs, peut-on facilement concevoir.

Ne pas se figurer que c'est seulement l'étape suivante qui prolonge la publicité en ligne, c'est au contraire un véritable saut vers une autre catégorie « un monde différent » à la fois exaltant par son potentiel extraordinaire mais aussi terriblement dangereux.

Voyons un peu la mécanique de la publicité. Dans le monde physique, les friandises à portée des enfants au passage en

caisse de supermarché sont un procédé d'incitation efficace, mais dont la portée est limitée. Dans le monde numérique, ce que Zeynep appelle **l'architecture de la persuasion** est à l'échelle de plusieurs milliards de consommateurs potentiels. Qui plus est, l'intelligence artificielle peut cibler chacun distinctement et envoyer sur l'écran de son smartphone (on devrait dire *spyphone*, non ?) un message incitatif qui ne sera vu que par chacun et le ciblera selon ses points faibles identifiés par algorithmes.

Prenons un exemple : quand hier l'on voulait vendre des billets d'avion pour Las Vegas, on cherchait la tranche d'âge idéale et la carte de crédit bien garnie. Aujourd'hui, les mégadonnées et l'apprentissage machine (*machine learning*) s'appuient sur tout ce que Facebook peut avoir collecté sur vous à travers messages, photos, « *likes* », même sur les textes qu'on a commencés à saisir au clavier et qu'on a ensuite effacés, etc. Tout est analysé en permanence, complété avec ce que fournissent des courtiers en données.

Les algos d'apprentissage, comme leur nom l'indique, apprennent ainsi non seulement votre profil personnel mais également, face à un nouveau compte, à quel type déjà existant on peut le rapprocher. Pour reprendre l'exemple, ils peuvent deviner très vite si telle ou telle personne est susceptible d'acheter un billet pour un séjour à Las Vegas.

Vous pensez que ce n'est pas très grave si on nous propose un billet pour Vegas.

Le problème n'est pas là.
Le problème c'est que les algorithmes complexes à l'œuvre deviennent opaques pour tout le monde, y compris les programmeurs, même s'ils ont accès aux données qui sont généralement propriétaires donc inaccessibles.

> *« Comme si nous cessions de programmer pour laisser se développer une forme d'intelligence que nous ne comprenons*

pas véritablement. Et tout cela marche seulement s'il existe une énorme quantité de données, donc ils encouragent une surveillance étendue : pour que les algos de machine learning puissent opérer. Voilà pourquoi Facebook veut absolument collecter le plus de données possible sur vous. Les algos fonctionneront bien mieux »

Que se passerait-il, continue Zeynep avec l'exemple de Las Vegas, si les algos pouvaient repérer les gens bipolaires, soumis à des phases de dépenses compulsives et donc bons clients pour Vegas, capitale du jeu d'argent ? Eh bien un chercheur qui a contacté Zeynep a démontré que les algos pouvaient détecter les profils à risques psychologiques avec les médias sociaux avant que des symptômes cliniques ne se manifestent…
Les outils de détection existent et sont accessibles, les entreprises s'en servent et les développent.

L'exemple de YouTube est également très intéressant : nous savons bien, continue Zeynep, que nous sommes incités par un algo à écouter/regarder d'autres vidéos sur la page où se trouve celle que nous avons choisie.

Eh bien en 2016, témoigne Zeynep, j'ai reçu de suggestions par YouTube : comme j'étudiais la campagne électorale en sociologue, je regardais des vidéos des meetings de Trump et YouTube m'a suggéré des vidéos de suprématistes (extrême-droite fascisante aux USA) !
Ce n'est pas seulement un problème de politique. L'algorithme construit une idée du comportement humain, en supposant que nous allons pousser toujours notre curiosité vers davantage d'extrêmes, de manière à nous faire demeurer plus longtemps sur un site pendant que Google vous sert davantage de publicités.
Pire encore, comme l'ont prouvé des expériences faites par ProPublica et BuzzFeed, que ce soit sur Facebook ou avec Google, avec un investissement minime, on peut présenter des

messages et profils violemment antisémites à des personnes qui ne sont pas mais *pourraient* (toujours suivant les algorithmes) devenir antisémites.

L'année dernière, le responsable médias de l'équipe de Trump a révélé qu'ils avaient utilisé de messages « non-publics » de Facebook pour démobiliser les électeurs, les inciter à ne pas voter, en particulier dans des villes à forte population d'Afro-américains. Qu'y avait-il dans ces messages « non-publics » ? On ne le saura pas, Twitter ne le dira pas.

Les algorithmes peuvent donc aussi influencer le comportement des électeurs.

Facebook a fait une expérience en 2010 qui a été divulguée après coup.
Certains ont vu ce message les incitant à voter. Voici la version basique :

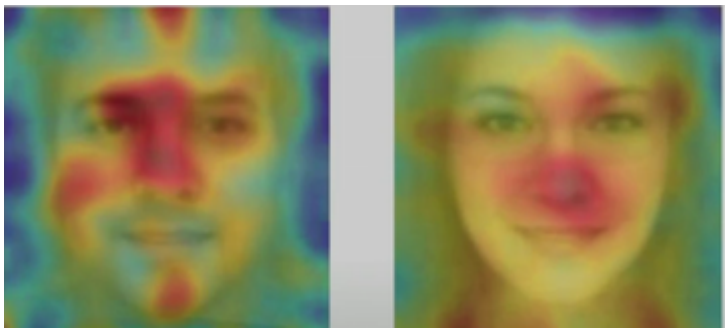
et d'autres ont vu cette version (avec les imagettes des contacts qui ont cliqué sur « j'ai voté »)

Ce message n'a été présenté qu'une fois mais **340 000 électeurs**

de plus ont voté lors de cette élection, selon cette recherche, confirmée par les listes électorales.
En 2012, même expérience, résultats comparables : 270 000 électeurs de plus.
De quoi laisser songeur quand on se souvient que l'élection présidentielle américaine de 2016 s'est décidée à environ 100 000 voix près…

> *« Si une plate-forme dotée d'un tel pouvoir décide de faire passer les partisans d'un candidat avant les autres, comment le saurions-nous ? »*

Les algorithmes peuvent facilement déduire notre appartenance à une communauté ethnique, nos opinions religieuses et politiques, nos traits de personnalité, l'intelligence, la consommation de substances addictives, la séparation parentale, l'âge et le sexe, en se fondant sur les « j'aime » de Facebook. Ces algorithmes peuvent identifier les manifestants même si leurs visages sont partiellement dissimulés, et même l'orientation sexuelle des gens à partir de leurs photos de leur profil de rencontres.
Faut-il rappeler que la Chine utilise déjà la technologie de détection des visages pour identifier et arrêter les personnes ?



Le pire, souligne Zeynep est que

> *« Nous construisons cette infrastructure de surveillance autoritaire uniquement pour inciter les gens à cliquer sur les publicités. »*

Si nous étions dans l'univers terrifiant de 1984 nous aurions peur mais nous saurions de quoi, nous détesterions et pourrions résister. Mais dans ce nouveau monde, si un état nous observe et nous juge, empêche par anticipation les potentiels fauteurs de trouble de s'opposer, manipule individus et masses avec la même facilité, nous n'en saurons rien ou très peu…

> *« Les mêmes algorithmes que ceux qui nous ont été lancés pour nous rendre plus flexibles en matière de publicité organisent également nos flux d'informations politiques, personnelles et sociales… »*

Les dirigeants de Facebook ou Google multiplient les déclarations bien intentionnées pour nous convaincre qu'ils ne nous veulent aucun mal. Mais le problème c'est le *business model* qu'ils élaborent. Ils se défendent en prétendant que leur pouvoir d'influence est limité, mais de deux choses l'une : ou bien Facebook est un énorme escroquerie et les publicités ne fonctionnent pas sur leur site (et dans ce cas pourquoi des entreprises paieraient-elles pour leur publicité sur Facebook ?), ou bien leur pouvoir d'influence est terriblement préoccupant. C'est soit l'un, soit l'autre. Même chose pour Google évidemment.

Que faire ?
C'est toute la structure et le fonctionnement de notre technologie numérique qu'il faudrait modifier…

> *« Nous devons faire face au manque de transparence créé par les algorithmes propriétaires, au défi structurel de l'opacité de l'apprentissage machine, à toutes ces données qui sont recueillies à notre sujet. Nous avons une lourde tâche devant nous. Nous devons mobiliser notre technologie, notre créativité et aussi notre pouvoir politique pour construire une intelligence artificielle qui nous soutienne dans nos objectifs humains, mais qui soit aussi limitée par*

nos valeurs humaines. »

« Nous avons besoin d'une économie numérique où nos données et notre attention ne sont pas destinées à la vente aux plus offrants autoritaires ou démagogues. »

- voir la vidéo : *We're building a dystopia just to make people click on ads*
- une autre conférence de Zeynep avec des sous-titres en français : l'intelligence artificielle rend la morale plus importante.

Des métadonnées Twitter…

S'il est de notoriété publique que nos données personnelles sont enregistrées et utilisées par les G.A.F.A.M., il est en revanche moins connu que certaines de ces données sont utilisables par tout le monde. Et c'est bien là le point faible de toute campagne de prévention : on a beau dire que nos données sont utilisées, il est peu fréquent que nos paroles soient illustrées.

x0rz publie sur son blog un billet qui illustre parfaitement ce problème. En effet, il a écrit un petit script Python (moins de 400 lignes de code) qui récupère et synthétise les métadonnées Twitter, accessible par n'importe qui.

Ce billet ouvre deux perspectives :

- Concernant le harcèlement numérique : certes ces données

sont publiques, mais il faut tout de même quelques capacités en programmation pour les exploiter, ce qui n'est pas à la portée de tout le monde. Imaginons qu'apparaissent de plus en plus de programmes grand public permettant d'accumuler et synthétiser ces données. Il deviendra alors plus facile pour un particulier d'identifier et de traquer une autre personne.
- Concernant les métadonnées en général : dans cet exemple, les données analysées restent très basiques (heure et localisation). Nous arrivons toutefois, par l'accumulation et le recoupement, à déduire des informations intéressantes de ces « méta-métadonnées », et à identifier nettement une personne. Imaginons que les métadonnées enregistrées soient plus précises et plus nombreuses, les informations obtenues seraient alors d'une importance et d'une précision inimaginables. Est-ce alors nécessaire de mentionner qu'à la fois les entreprises (ici Twitter) et les agences gouvernementales ont accès à ce genre de métadonnées ?

Article original écrit par x0rz, consultant en sécurité informatique, sur son blog.

Traduction Framalang : mo, mathis, goofy, valvin, Diane, Moriarty, Bromind et des anonymes

Vous serez surpris par tout ce que vos tweets peuvent révéler de vous et de vos habitudes

Une analyse de l'activité des comptes Twitter

J’utilise Twitter tous les jours. Pour moi qui suis consultant en cybersécurité, c’est de loin un des meilleurs outils pour rester informé des dernières actualités et pour partager des informations qu’on estime pertinentes pour d’autres. Avec la récente investiture de Donald Trump, les dingos de Twitter de la nouvelle administration et l’émergence de groupes de résistance sur Twitter, j’ai décidé de démontrer à quel point il est facile d’exposer des informations révélatrices à partir du compte de quelqu’un d’autre, sans même le pirater.

Métadonnées

Comme tous les réseaux sociaux, Twitter sait beaucoup de choses sur vous, grâce aux *métadonnées*. En effet, pour un message de 140 caractères, vous aurez un paquet de métadonnées, plus de 20 fois la taille du contenu initial que vous avez saisi ! Et vous savez quoi ? Presque toutes les métadonnées sont accessibles par l’API ouverte de Twitter.
Voici quelques exemples qui peuvent être exploités par n’importe qui (pas seulement les gouvernements) pour pister quelqu’un et en déduire son empreinte numérique :

- Fuseau horaire et langue choisie pour l’interface de twitter
- Langues détectées dans les tweets
- Sources utilisées (application pour mobile, navigateur web…)
- Géolocalisation
- Hashtags les plus utilisés, utilisateurs les plus retweetés, etc.
- Activité quotidienne/hebdomadaire

Un exemple d’analyse de tweet (2010, l’API a beaucoup changé depuis).

Tout le monde connaît les dangers des fuites de géolocalisation et à quel point elles nuisent à la confidentialité. Mais peu de gens se rendent compte que tweeter de façon régulière suffit à en dire beaucoup sur vos habitudes.
Prendre séparément un tweet unique peut révéler des métadonnées intéressantes. Prenez-en quelques milliers et vous allez commencer à voir se dessiner des lignes directrices. C’est là que ça devient amusant.

Méta-métadonnées

Une fois qu’on a collecté suffisamment de tweets d’un compte on peut par exemple identifier ceux qui relèvent d’une entreprise (émettant uniquement pendant les horaires de bureau) et même essayer de deviner combien d’utilisateurs interagissent avec ce compte.
Pour prouver ce que j’avance, j’ai développé un script en python qui récupère tous les derniers tweets de quelqu’un, extrait les métadonnées, et mesure l’activité en fonction de l’heure et du jour de la semaine.

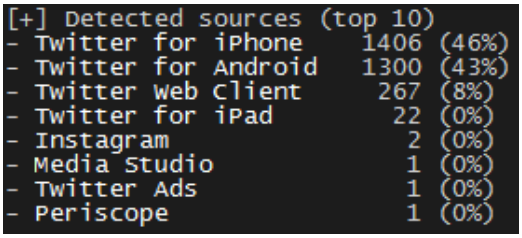
Analyse du compte de @Snowden

Snowden a posté 1682 tweets depuis septembre 2015. Comme on peut le voir ci-dessous, il est facile de déterminer son rythme de sommeil (fuseau horaire de Moscou).

Activité du compte Twitter de Snowden

Analyse du compte de @realdonaldtrump

Est-ce que le compte de Donald Trump est géré par plusieurs personnes ? Cette fois en observant le nombre de sources détectées, je vous laisse deviner…



Sources des tweets du compte de Donald Trump

Recommandations générales

Je vous recommande fortement de lire les conseils de sécurité Twitter du Grugq. En plus de ce guide, je vous conseille d'être prudents avec les fuseaux horaires et les langues que vous utilisez, et d'être également conscients que vos tweets

peuvent être analysés comme un tout : ne tweetez pas toujours à la même heure si vous ne voulez pas que les gens devinent votre fuseau horaire. Bien sûr, ces principes sont valables seulement si vous souhaitez rester anonyme, ne les appliquez pas à votre compte principal (ce serait une perte de temps) !

Code source

J'ai publié mon script sur GitHub. C'est *open source* donc n'hésitez pas à contribuer