

« Refroidissement social » ou « Social Cooling » : telle est la conséquence majeure de notre mise sous surveillance par les millions d'algorithmes qui s'activent online, dénonce l'activiste néerlandais Tijmen Schep. Comment alors pourrions-nous reconquérir notre vie privée ?

Des propos recueillis par Aurélie Jean

Malgré leur rigueur mathématique, les algorithmes possèdent des biais introduits consciemment ou pas par ceux qui les développent. Comment éliminer ces biais ?

TIJMEN SCHEP : Malheureusement ces biais ne peuvent pas être entièrement éliminés. Certes, les hommes aussi font des erreurs de jugement. **Un banquier par exemple peut inconsciemment proposer un prêt moins important à une personne de couleur.** Le recours à des algorithmes devrait nous amener à nous poser toujours ces questions : les algorithmes peuvent-ils « mieux faire » en moyenne que les hommes ? Quel niveau d'erreur sommes-nous prêts à accepter ? Quelles conséquences sommes-nous prêts à subir ?

En quoi ces biais exercent-ils un pouvoir sur notre société ?

T.S. : Je dis souvent que la technologie renforce l'idéologie. Prenons l'exemple d'une banque qui utilise un système pour estimer votre « valeur » à partir de votre présence sur les réseaux sociaux. **Les algorithmes utilisés déterminent un poids pour chaque mot que vous utilisez et analysent les sentiments associés** (neutre, positif ou négatif). Utiliser régulièrement le mot « IKEA » dans vos tweets peut-il être un indicateur de la confiance que l'on peut avoir en vous ? Que dire du mot « Allah » ? Les développeurs endossent un rôle de plus en plus important et complexe. Ils vont devoir prendre conscience de leur impact, et auront besoin d'être davantage formés à des règles éthiques. Mais n'oublions pas qu'ils travaillent sur des sujets financés par des entités dont on doit aussi comprendre les motivations.

Vous parlez de « refroidissement social », le « social cooling », pour évoquer le risque de nous voir adapter nos comportements pour conserver une réputation numérique décente.

T.S. : Gilles Deleuze, dans sa contribution « Post-scriptum sur les sociétés de contrôle », évoque deux systèmes de contrôle. Le premier est le système judiciaire. L'idée ici est que vous êtes libre mais si vous commettez un crime, un juge mesure le poids de vos actes, et vous envoie éventuellement en prison. Nous comprenons ce système. C'est une institution démocratique que nous avons construite sur des siècles. **Mais Gilles Deleuze insiste sur une couche supérieure, un système informel au-dessus de la couche judiciaire. La morale et les normes exercent une pression sociale sur les individus, et modifient leurs comportements. Ce système a toujours existé.** Mais là où notre réputation se faisait connaître par le bouche à oreille, elle est à présent mesurée et se propage à grande vitesse via des outils digitaux. Cette couche est très puissante, plus que la punition judiciaire, car elle utilise la menace d'exclusion d'un groupe, voire de la société. Les individus sont bien plus sensibles à de telles menaces. **Désormais, cette couche supérieure est active en continu, vous êtes constamment chassé. Par exemple, conduire sans se soucier du coût financier n'est pas un crime, néanmoins des systèmes d'évaluation vont mesurer vos habitudes de**

conduite et développer une pression subtile pour vous imposer de changer votre **comportement**. Vous pouvez être amené à payer plus cher une **assurance** automobile si votre conduite ne suit pas des règles implicitement définies. **En ce xxi^e siècle, la pression sociale digitale est un moyen de contrôler les individus**. Alors que la police applique la loi, votre envie d'une vie sociale et d'une carrière va développer une pression sur votre entourage et vous-même afin de « mieux » vous comporter. Certaines personnes peuvent penser qu'un peu de contrôle social serait bon pour notre société. Mais dans ce cas, il faut également reconnaître que nous ne vérifions pas que cette deuxième couche est en accord avec nos principes démocratiques. Par exemple, **Facebook développe actuellement des algorithmes pour chasser les fake news**. Il faut réaliser que le groupe d'individus qui écrit et implémente ces algorithmes a un pouvoir réel sur la notion de **censure**.

Quel est le vrai danger moral et sociétal de ces algorithmes qui décident pour nous ?

T.S. : Il y en a tellement... 1. On ne vérifie pas que le nouveau système mis en place est en accord avec nos principes démocratiques. 2. **Notre présomption d'innocence est mise en danger quand nous commençons à prédire les crimes par la data**. 3. La **liberté d'expression** est sous pression à mesure que les gens s'autocensurent afin d'obtenir une meilleure réputation sociale. 4. **À plus long terme, je m'inquiète d'une montée en puissance de la pression des réseaux sociaux qui vont créer une société plus conformiste, moins diversifiée**. 5. Et pour finir, je ne peux pas imaginer ce qu'il adviendrait si un nouvel **Hitler** venait au pouvoir.

or il se trouve que tout donne à penser qu'une telle revenance est des plus probables.

Voulez-vous dire que les hommes devraient davantage s'engager dans une meilleure compréhension des technologies qu'ils utilisent au quotidien ?

T. S. : Non, car **je ne veux pas suivre cette vision néolibérale qui place la responsabilité sur chaque citoyen et consommateur**. Lire entièrement les conditions d'utilisation à chaque fois que nous cochons la case « J'accepte » nous prendrait des années. Mais oui, **les individus doivent mieux comprendre les technologies. Ne pas le faire reviendrait à refuser d'apprendre à lire dans un monde où les écrits sont partout**.

Dans votre livre Design My Privacy: 8 Principles for Better Privacy Design, vous écrivez qu'il faut réfléchir comme un hacker. En pratique, comment faire ?

T. S. : **Les hackers sont intéressants car ils croient en l'idée que les technologies peuvent apporter beaucoup (sans s'aveugler comme le font les utopistes de la Silicon Valley), mais ils ont conscience que les technologies ne sont jamais parfaites. Penser comme un hacker implique de dédier à part égale un temps de réflexion aux bénéfices et aux dangers des technologies.**

mais cela suppose une nouvelle ère, post-hacker, c'est à dire ayant critiqué le hacking tel qu'il a servi le programme libertarien et anti-démocratique cf Morozov

Vous soulignez aussi la nécessité d'actions étatiques.

ie d'une nelle puissance publique

T. S. : Le problème est si complexe que les gouvernements ne peuvent pas agir seuls. Les designers, les entreprises, les journalistes, la société civile et les citoyens ont aussi beaucoup de travail. Aujourd'hui, le marché des données est immense et très immoral. Mais la plupart des gens ne possèdent pas les connaissances pour comprendre le problème en profondeur. J'espère pouvoir contribuer à changer cela mais le chemin est long. **De la même manière que les textes de lois sont transparents et libres d'accès, les algorithmes devraient être mis à la disponibilité de tous.** Lawrence Lessig résume très bien cette idée de transparence dans son article « Le code fait loi ». Rendre les algorithmes et le code transparents serait un moyen de les améliorer à partir du retour et des avis des individus. Ils pourraient alors évoluer au même titre que les lois pour suivre les normes sociétales. **Peut-être qu'en 2050 nous achèterons des systèmes de protection d'intimité sociale, et des systèmes de régulation nous protégeront des algorithmes abusifs.** Notre société aura une compréhension plus large et plus approfondie des biais, et des limites des mathématiques et des technologies. La technologie n'est pas une force de la nature, nous avons le contrôle.

Enfin, selon vous, l'ère numérique annonce un chaos incontrôlable ou une harmonie collaborative ?

T. S. : C'est un chaos collaboratif qui pourrait mener à une incontrôlable harmonie.

PARCOURS DE TIJMEN SCHEP

Consultant, auteur, il a inventé le concept de « refroidissement social » (social cooling), qui souligne la façon dont la société de l'information a des effets sur la liberté d'expression. Il a cofondé SETUP, une ONG néerlandaise qui utilise l'humour pour expliquer les problèmes posés par l'utilisation des données personnelles au grand public. Dans le projet DIY NSA par exemple, l'association a hacké une base de données sourçant l'ensemble des profils des Néerlandais qu'elle a mis en ligne sous la forme d'un National Birthday Calendar.

À LIRE

Tijmen Schep, Design My Privacy: 8 Principles for Better Privacy Design, BIS Publishers, 2016.